Strasbourg, 18 February 2014

T-PD(2013)11

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD)

RECOMMENDATION R (87) 15 – TWENTY–FIVE YEARS DOWN THE LINE

by Professor Joseph A. Cannataci and Dr. Mireille M. Caruana

DG I – Human Rights and Rule of Law

Executive Summary

Between the period 2011-2012, within the framework of the PUPIE project, the authors carried out a survey of the state of legislation in 30 out of the Council of Europe's 47 member States in an effort to determine the impact of the Council of Europe's Recommendation R(87)15 on data protection in the police sector over the 25 years since the adoption of the Recommendation in 1987. This final report from the PUPIE project finds that by and large the Recommendation has been widely adopted across Europe to an extent that many European states *prima facie* already regulate police use of personal data in a way comparable but not necessarily identical to that envisaged in the current draft of the European Commission's proposal 25.1.2012 COM(2012) 10 final 2012/0010 (COD) for a "Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data". This general finding in no way obviates the need for urgent action on this sector. The Report identifies two overall findings and thirty-one provision-specific findings in relation to the provisions of R(87)15 and places these in the context of eight realities as at September 2013. In response to the overall findings of disparity of provisions and lack of harmonisation, the Report advocates that the time has come for a binding legal instrument which is capable of being deployed across sectors which have hitherto often been parallel worlds: that of law enforcement agencies (LEAs) and the other of Security & Intelligence Agencies (SIS). The Report takes into account the available evidence of utility of the EU's 2006 Data Retention Directive as well as the significance of the Snowden revelations for privacy & data protection. These considerations reinforce the Report's recommendations that the Council of Europe offers the right forum for one or more of at least three options which could produce a suitable new binding legal instrument: (1) an entirely new multi-lateral treaty or Convention which would contain mandatory provisions applicable to the LEA and SIS handling of personal data; (2) an additional protocol to the CoE's Data Protection Convention (ETS 108) encapsulating the provisions envisaged in Option 1 and/or (3) an additional protocol to the CoE's Cybercrime Convention (ETS 185) incorporating some of the provisions envisaged in Options 1 and 2. The Report finds that the urgency for and the onus upon the Council of Europe to take immediate action to produce a new binding instrument is compounded by the Snowden revelations and the possible chronic inadequacy of EU responses in the sphere of national security on account of exclusions of competence by Art 4 Section 2 of the EU Treaty.

25th September 2013

Table of Contents

Report: Recommendation R (87) 15 – Twenty–five years down the line:

By
Prof Joseph A. Cannataci
Chair in European Information Policy & Technology Law, Co-Director STeP - Security, Technology & e-Privacy Research Group, Department of European and Economic Law, Faculty of Law, University of Groningen, The Netherlands
Head of Department of Information Policy and Governance, Faculty of Media and Knowledge Sciences, University of Malta,
Adjunct Professor, Security Research Centre, School for Computer & Security Science at Edith Cowan University, Australia,
Associate, Cyber Security Center, Longwood University, USA
&
Dr Mireille M. Caruana,
Centre for IT & Law, University of Bristol
Department of Information Policy & Governance, University of Malta.

CoE Recommendation No. R(87)15 regulating the use of Personal Data in the Police Sector (R(87)15) was developed by the CoE's Project Group on Data Protection (CJ-PD) in Strasbourg between 1984 – 1986. CJ-PD was characterised by the strong leadership of Germany's Spiros Simitis, later involved in incorporating data protection into the EU Charter of Fundamental Rights: he was succeeded by Peter Hustinx, today EU Data Protection Commissioner ("EDPS"). The *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108) had created ambiguity by including an exclusion from its provisions for security purposes.[1] R(87)15 resolved this by explicitly subjecting police data to the same data protection regime as other personal data.

R(87)15 was also a significant victory for a key principle of data protection: "purpose specification", in other words, that data controllers should process data according to legitimate, specified and explicit purposes announced at the time of collection, and only use these data for purposes compatible with the original purposes of the collection.[2] This key principle was not easily won. Many CJ-PD members were accompanied by national police and/or security forces representatives who were seeking "general purpose" collection, rather than the CJ-PD's preferred option of "purpose specification" (*per* Convention 108). Only as a result of strenuous negotiations was a consensual basis for the eventual text arrived at. The drafters of R(87)15 thus succeeded in entrenching the notion of requiring a distinct purpose for collection and processing of data, even for police use.

Although R(87)15 was never popular with the police in Western Europe, it was greeted as a model for democratic policing and often cited, especially during the 1989 – 1992 period, in Central and Eastern Europe. In that post-1989 'democratic surge', the Recommendation was referred to in two international agreements: Art.115, para.1, Schengen Agreement[3] states that control by the supervisory authority should take account of the Recommendation; the Treaty of

1 CETS No.: 108, Art.9.

2 Convention 108, in particular Art.5b; R(87)15 – in particular Principle 2.1, 2.3, 2.4 and 3.1.

3 OJ 2000, L 239/19.

Amsterdam incorporated the Schengen Agreement into the EU Treaty. Likewise, Art.14, para.1, Europol Convention[4] provides that processing of police data should take account of Recommendation R(87)15. These two references mean that legally R(87)15 cannot be avoided. Meanwhile, in its *Recommendation 1181 (1992) 1 on police co-operation and protection of personal data in the police sector*, the CoE Parliamentary Assembly recommended that the Committee of Ministers draw up a convention enshrining the principles laid down in R(87)15.

In 1993 the CoE Committee of Ministers requested that the CJ-PD evaluate the relevance of R(87)15 notably whether its text required revision, especially its scope and Principle 5.4 (international communication), and considering the principles set out in Assembly Recommendation 1181 (1992). The CJ-PD completed its first evaluation in 1994,[5] determining that R(87)15 provided adequate protection for personal data used for police purposes and there was no present need to revise it. It felt that Principle 5.4, R(87)15, read together with paras.56–80, Explanatory Memorandum, was sufficiently flexible to address the foreseeable requirements of international agreements on the exchanges of data for police purposes. Several experts suggested "that the provisions of the Recommendation constitute an inalterable necessary minimum" (CJ-PD (93) 48). The number of requests for serious revision of the text, whether to strengthen or to weaken the provisions, was considered insufficient to merit re-opening discussion of R(87)15 as a priority. However, the CJ-PD suggested that R(87)15 should be subject to periodic rather than *ad hoc* review, with a review being carried out and report provided by December 1998, and thereafter on a four-yearly basis.

In 1998, the second evaluation concluded no serious problems had arisen necessitating changes to the Recommendation. The report suggested the Committee of Ministers recommend that national legislators explicitly deal with certain questions of data protection, via national data protection legislation, national codes of criminal procedure, or national or regional police law. It proposed that the Committee of Ministers include in the periodic evaluation an assessment of whether any additional international instrument should be developed.

The third evaluation of R(87)15 was completed in 2002. The CJ-PD agreed that "its principles are still relevant, continue to provide a basis for the elaboration of regulations on this issue and serve as a point of reference for any activities in this field and considered that it is not necessary to revise them at present. Furthermore, this Recommendation is referred to in other international instruments such as the Schengen Agreement and the Europol Convention". The CJ-PD recommended neither revision of R(87)15, nor the preparation of a new recommendation in the police field. Its report did recommend that the third evaluation should be the final periodic evaluation, but that as use of personal data in the police sector remained a concern, further evaluations of specific issues arising out of new techniques of processing police data could be commissioned where necessary.

[4] OJ 1995, C 316/2.

[5] CJ-PD (94) 7.

Most recently, in 2010, a consultant was appointed by the CoE to undertake a study of R(87)15 and to suggest proposals for its revision.[6] This report noted the background of R(87)15 and examined the risks prevalent in 2010. It summarized 20 key changes that had occurred between 1987–2010. Considering these changes, the report suggested that while the R(87)15 Principles remained valid and useful, they were formulated in a non-binding, sometimes insufficiently detailed, manner which significantly inhibits its usefulness. The major societal and sectorial changes outlined suggest that the amount of personal data collected, and the risks of its abuse have increased significantly, and that Convention 108 and R(87)15 are no longer a proportionate response to current levels of risk. Increased risks require binding legislative measures for European states, sufficiently detailed to be meaningful to relevant practitioners. The report identified several procedural and substantive weaknesses in Convention 108 and R(87)15, emphasising that they do not provide an attractive platform/basis for developing an international consensus on data protection in policing matters, especially vis-à-vis non-European states. The report concluded with four priority options for follow-up action by the CoE which would address the weaknesses outlined.

The history of the PUPIE project

In 2010, the principal investigator of this present study was commissioned by the Council of Europe to review the relevance of Recommendation R(87)15 in the present context and provide suggestions for its up-dating. The results of that report were submitted and published on-line in autumn 2010.[7]

During that exercise it became abundantly clear that there did not exist to date any evidence-based analysis of the extent to which R(87)15 had actually been implemented across Europe. This was pointed out by the author to the T-PD Bureau which took up the idea to survey the use by the police of personal data across Europe. This is how the PUPIE project was born. PUPIE – (Role of Law in) Police Uses of Personal Information across Europe is a project conceived and designed by Professor Joseph A. Cannataci, Chair in European Information Policy & Technology Law, Department of European and Economic Law, Faculty of Law, University of Groningen and Head of Department of Information Policy and Governance (IPG), Faculty of Media and Knowledge Sciences, University of Malta, together with Dr Mireille M. Caruana then of the Centre for IT & Law, University of Bristol, now a Research Associate at IPG. The team undertook a section-by-section analysis of R(87)15 and its Explanatory Memorandum and this served as the basis of the design of the primary research instrument employed in the project: a questionnaire (here reproduced as Appendix A) which was intended to be distributed to all the member states represented at the T-PD. This design and development work commenced in late 2010 and the PUPIE research project was formally commissioned by the Council of Europe in the first half of 2011.

---

[6] Cannataci, Joseph A. 2010. Council of Europe Recommendation R(87)15 & ETS Convention 108: Data Protection Vision 2020 – options for improving European policy and legislation during 2010-2020. Accessed at http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf

[7] *Ibid.*

The first draft of the questionnaire was submitted to and approved by the T-PD Bureau during its meeting of March 2011 and some minor amendments were consequently made. The questionnaire was distributed by the T-PD's secretariat to all member States of the CoE in April 2011. Responses were received between May and September 2011, enabling a preliminary analysis and report to be completed in draft form in September 2011. A first draft of the preliminary analysis was presented to and considered by the T-PD Plenary session at its meeting of 29-30 November 2011. At this meeting, the T-PD approved an extension of the date for response to the questionnaire to 28 February 2012 in order to give those member States which had not responded the opportunity to dedicate adequate resources to the collation and formulation of responses to the CoE. Furthermore, the T-PD encouraged those member States which had actually responded to the questionnaire to take the opportunity to review the quality and detail of the responses provided, and communicate any reviewed response to the research team by the same new deadline date. During this extended period some further responses to the questionnaire were received. Some clarifications or corrections were also received with regard to the manner in which the data received had been interpreted and presented in the Preliminary Report.

The questionnaire (reproduced here as Annex A) was distributed to the pertinent authorities within the 47 States of the Council of Europe. Of these, responses were received from thirty (30) countries. These are:

- Albania
- Andorra
- Austria
- Bosnia and Herzegovina
- Croatia
- Cyprus
- Czech Republic
- Estonia
- Finland
- France
- Germany
- Hungary
- Ireland
- Italy
- Liechtenstein
- Lithuania
- Luxembourg
- Macedonia
- Malta
- Monaco
- Montenegro
- Netherlands
- Portugal

- Serbia
- Slovak Republic
- Slovenia
- Sweden
- Switzerland
- Ukraine
- United Kingdom

It should be emphasised that the analysis of the responses received to the questionnaire is entirely dependent on the answers received, which have yet to be independently confirmed by field-work. It is possible that the real situation on the ground in a minority of countries may be somewhat different to the impression obtained from reading the responses to the PUPIE questionnaire. The level of analysis possible at this stage is therefore that of the letter of the law. The extent to which the spirit of the law is actually respected and R(87)15 is really implemented in practice is something which can only be determined through detailed field-work in the country concerned. At this stage therefore, apart from formal legal rule analysis, the questionnaire responses are particularly useful in providing insights into areas which would especially benefit from further investigation.

In addition to formal legal rule analysis, questionnaire responses in 3 countries were immediately followed up by a further phase of empirical research using semi-structured interviews with selected interviewees per country. The aim was to interview representatives from the national Independent Supervisory Authority (ISA), the police-specific ISA (if one existed), the relevant government Ministry and, where possible, the Head of IT and/or Data Protection from inside a law enforcement agency in that country, etc. Ultimately, it was possible to carry out interviews with ISAs and police forces in Germany, Italy, Malta and the United Kingdom. For each of these interviews, a personalised semi-structured interview schedule was prepared beforehand. Interviews were carried out with:

In Italy:

Dr Vanna Palumbo, head of *Servizio relazioni comunitarie e internazionali* at the *Garante per la Protezione dei Dati Personali* (the Italian DPA)

In Germany:

Dr. Ulrich Lepper, Data Protection Commissioner for NordRhein-WestPhalia

In Malta:

Mr Joseph Ebejer, Data Protection Commissioner
Dr Domenic Micallef, inspector within the Malta Police Force
Mr. Andrew Seychell, Assistant Police Commissioner in charge of Immigration
Mr George Cremona, Inspector, Counter-terrorism, Malta Police

In the United Kingdom:

Mr David Smith, Deputy Commissioner, Information Commissioner's Office
Joined by Jonathan Bamford, Head of Strategic Liaison
Simon Rice, Principal Policy Adviser, Technology – Strategic Liaison
Libs Davies, Senior Policy Officer, Policy Delivery

While the R(87)15 Evaluation Reports provide a useful starting point for discussion, the 2010 study, noted above, suggests that it is necessary to investigate both how the Recommendation has been implemented by European States, and its effect upon police practices in the use of personal data. The main aim of this report is thus to assess the extent to which R(87)15 has practically been implemented across Europe. This report is *not* a synopsis of the national responses submitted to the questionnaire, but *is* a summary of the qualitative analysis performed on the national responses. It also does not involve a detailed jurisprudential analysis of the implementation of various legal principles in different European states. Rather, the objective is to obtain an overview or snapshot of the pan-European position in police data protection, based on a comparative analysis of the progress achieved in national legislation since 1987. Given this aim, rather than going through national laws on a nation-by-nation, section-by-section basis, the analytical approach is via an 'achievement matrix' premised on the framework of R(87)15. By this means, it is possible to obtain a clearer viewpoint of practical implementation.

The responses to the questionnaire included a wide range of information and legislative texts, and presented a problem of how to sort and analyse this information. The method employed consisted of creating tables that would categorise or list (depending on the nature of the question/response) the data received per question put. These tables are attached to this report as Annex B and Annex C.

Part 1 – Overview

All the countries surveyed indicated they had a law containing general data protection rules. In most countries that have ratified Convention 108 and have data protection rules in force, these general rules apply to the police sector. Some countries have specific police sector data protection rules, usually grounded in a Code of Criminal Procedure, or in a specific Act regulating the police. A majority of states indicated their legislation also provides some element of specific regulation of police uses of personal data;[8] though at least 3 of them require further investigation to determine the precise level of protection, especially in countries with rather generic laws. Ireland and the UK have internal police guidelines. In Cyprus, R(87)15 was adopted via a Circular of the Chief of Police.[9] The questionnaire requested information regarding laws and regulations directly, or indirectly, relating to the police use of personal data. Responses have been compiled and are listed for reference in Annex B.

[8] No specific legislation: Cyprus and Ireland.

[9] Dated 4th January 2007, for the implementation of R(87)15 by the Cyprus Police.

Part 2 – Detailed provisions

Scope and definitions

Definition of personal data "for police purposes"

Thirteen countries reported that they had a specific legal definition of personal data processed "for police purposes".[10] Despite semantic differences between them, countries that provide a definition generally do so, as R(87)15 does, by reference to the police authorities or the "public entities, authorities or bodies exercising police powers"[11] carrying out the processing. Whilst this approach complies with the "purpose specification" principle, what national legislation often fails to clarify is the extent to which certain other State agencies might also be considered to be exercising police powers. For example, while the primary responsibility of customs authorities is oversight of imports and exports, under national legislation and regulations the import or export of some goods may be restricted or forbidden, and the customs authority responsible for enforcing these rules. In this sense, the customs authority would be performing its tasks 'for the prevention and suppression of criminal offences'. Similar considerations apply to immigration authorities. Border control may not consist solely of controlling immigration by monitoring persons entering or leaving the country, but include apprehending individuals wanted under international arrest warrants, and barring entry of others deemed dangerous to the country. Another variable is whether, and to what extent, processing by national security services falls within "police purposes" and is subjected to data protection legislation and safeguards.

The controller of police files

The majority of countries indicated that the "responsible body" competent under national law to determine the purpose of an automated file, categories of personal data which must be stored, and operations to be applied to them, was either their Ministry of the Interior or police authorities themselves.

Only automated, or also manual processing?

The overwhelming majority of countries extend the principles contained in R(87)15 to personal data undergoing manual processing. However, as automation of data processing becomes the norm, the issue of manually processed data seems to have declined substantially in importance. Very few responses were received concerning manual processing by the police.

Legal or only natural persons?

Responses were more varied as regards extension of the principles contained in R(87)15 to data relating to groups of persons, associations, foundations, companies, corporations or any other body consisting directly or indirectly of individuals (whether or not such bodies possess legal personality). Over a third of the countries surveyed indicated that legal persons enjoy identical protection to natural persons. This reflects a long-standing divide in European

[10] Country-by-country responses are outlined in Table 2, Annex C.

[11] E.g. Malta: SL 440.05 – Data Protection (Processing of Personal Data in the Police Sector) Regulations, Art.2.

approaches over the treatment of legal persons for data privacy purposes.[12] Indeed, this debate appears no closer to resolution now than it did thirty years ago, with some experts claiming that privacy is a concept exclusive to natural persons and that legal persons are more appropriately protected through other legal avenues, e.g. for commercial enterprises, via business confidentiality.

Only police or also state security?
There is limited agreement on the meaning of 'state security', as it depends on national policies (at national level, the use/application of the phrase 'national security' or 'state security' may be confusing). The majority of countries surveyed applied data protection rules to data processed for state security purposes, while two countries reported such activity is regulated by a specific, separate data protection law.

Basic Principles

Principle 1 – Control and notification

General or security/police-specific ISA?
All the countries surveyed have a (general) Data Protection Authority (DPA). There are additional police or security-specific data protection institutions in Austria, Luxembourg and Sweden:

- In addition to the Data Protection Commission (*Datenschutzkommission*), Austria established a specific independent control institution, the Legal Protection Commissioner, with functions defined in §91c, Federal Act on the Organisation of Security Administration and the Exercise of Security Police Services (Security Police Act – *Sicherheitspolizeigesetz*).

- In addition to the *Commission nationale pour la protection des données* (CNPD), Luxembourg has a specific ISA to oversee processing of data for police purposes under Art.17, *La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*.

- In Sweden, The Data Inspection Board[13] is the general DPA, while the Swedish Commission on Security and Integrity Protection[14] supervises use of secret surveillance and qualified assumed identities and associated activities by crime-fighting agencies. It also supervises processing of personal data by the Swedish Security Service.

Privacy Impact Assessments or other reasonable measures
While privacy/data protection impact assessments (PIA/DPIA) are not currently mandatory at the European level, well over a third of the respondent countries indicated that assessments are

[12] Cf. Korff, Bouwe. 1998. Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons. Commission of the European Communities (Study Contract ETD/97/B5-9500/78).

[13] www.datainspektionen.se

[14] www.sakint.se

undertaken when new technical means for data processing are introduced, to ensure their use complies with the spirit of existing data protection legislation.[15] Another eight countries apply other measures for similar reasons. In Italy any processing that is more likely to be prejudicial to data subjects – with particular regard to genetic and/or biometric databases, location-based processing, databases relying on specific information processing techniques, and the introduction of certain types of technology – must be compliant with such measures and arrangements as may be set forth by the *Garante* to safeguard data subjects following a prior checking procedure.[16] In Switzerland the Federal Act on the protection of data (LPD) and the relevant Federal Ordinance (OLPD) require measures ensuring technical and organizational security and protection of data processed, and that networks or systems available are up-to-date and adequate to ensure confidentiality, availability and integrity of data. It is necessary to integrate these technical and organizational requirements early in the development of an IT project. This may be considered an example of legislated Privacy by Design (PbD).[17]

Consulting the ISA

In fifteen of the thirty countries surveyed, the "responsible body" is obliged to consult the ISA in advance in any case where introduction of automated processing methods raises questions about the application of R(87)15. In most of these countries, primary legislation defines categories of processing operations subject to consultation, but this is sometimes left to secondary legislation. Five countries indicated that, while not mandatory, such consultation is regularly implemented in practice. In some countries, notably those where personal data processing requires a legal basis, consultation is carried out as part of the legislative process.

In Germany, where new technical means for processing personal data may only be introduced on the basis of legislation, the legislator will involve the Federal Commissioner for Data Protection and Freedom of Information, among others, in order to ensure conformity with existing data protection legislation;[18] Any "opening order" – a required special legal basis specifying *inter alia* the purpose of further processing of personal data by the Federal Criminal Police Office with special technical means, such as automated data files, irrespective of whether it is done in the context of threat prevention or criminal prosecution – requires the consent of the Federal Ministry of the Interior as the supervisory authority for technical matters. The Federal Commissioner for Data Protection and Freedom of Information is consulted before the order opening a data file is adopted.[19]

The R(87)15 consultation requirement bears some resemblance to Art.20, Directive 95/46/EC requiring that processing operations likely to present specific risks to the rights and freedoms of data subject should be examined prior to their start, an intervention described by the Directive

---

[15] For a broad study of PIAs, see Wright, David, and Paul De Hert, eds. 2012. Privacy Impact Assessment. Edited by P. Casanovas and G. Sartor. Vol. 6, Law, Governance and Technology Series. Dordrecht: Springer.

[16] DPC, section 55.

[17] Privacy by Design is an initiative pioneered by the Ontario Information and Privacy Commissioner, Ann Cavoukian: see http://privacybydesign.ca/

[18] Joint Rules of Procedure of the Federal Ministries, s.21.

[19] Federal Criminal Police Office Act, s.34; Code of Criminal Procedure, s.483 et seq.

as “prior checking”. However, since the questionnaire utilised the language of R(87)15, and not the language of the Directive, it is possible that national respondents interpreted the question differently, as some responses were inconsistent with the information reported in Annex H of the UK ICO’s *Privacy Impact Assessments: International Study of their Application and Effects* (2007); alternatively, some countries could have introduced prior checking since that study. The ICO Report – which included information about the legal position in countries not fully captured by this study, e.g. Belgium – found that use of prior checking across the EU Member States varies widely, with some having adopted prior checks for particular types of processing. e.g. sensitive data, offences and criminal convictions, and genetic data. This was confirmed by this study.

While not obliging the “responsible body” to consult the ISA in advance, Switzerland provides an example of good practice: the responsible federal agency (The Federal Office of Police, or fedpol) has a legal obligation to submit to their data protection advisor (fedpol legal service) and, failing this, to the Federal Data Protection and Information Commissioner (PFPDT), all new projects involving automated processing of personal data, at their inception. While the PFPDT has no power to authorise, or to refuse, a new information system, or the introduction of new means of data processing prior to implementation, it is consulted when processing involves creation, or a modification, of legal bases.[20] The PFPDT is also consulted during the federal legislative process when a federal law or ordinance on aspects of data protection is adopted or amended.

A limitation of the prior consultation procedure is that, absent a PIA or DPIA, it can be difficult to identify when the R(87)15 consultation requirement will be applicable. It is arguable that the “responsible body” should be required to consult the ISA where any new automated processing methods are introduced, subject to an exception where mandatory PIAs or DPIAs are in place. In the latter case, given the higher level of internal review, the scope of the consultation procedure might be reasonably limited to cases seen as presenting specific risks.

Notification to ISA

The response to the questions concerning the obligation to notify permanent automated police files to an ISA suggests quite a mixed picture. In a quarter of the States surveyed there is no obligation to notify automated police files to the ISA. Responses suggest the obligation to notify permanent automated police files to ISAs is regarded as imposing a disproportionate administrative burden whilst, given the general nature of the information notified, failing to achieve the desired transparency or “openness” of processing. The requirement is redundant in countries requiring a legal basis for personal data processing, e.g. Germany, Italy, Sweden, since absent a legal basis, no processing is permitted.

Manual files – Notification to ISA and ancillary matters

To date the survey has provided a similarly mixed picture of the obligation to notify manual police files to the ISA. In two States, while permanent automated police files must be notified to

[20] This is a general data protection rule and not specific to data processing for police purposes. See Art. 11a LPD and Art. 20 OLPD.

the ISA, manual files need not be notified. Aside from those countries, the countries requiring notification of permanent files to the ISA apply this to all police files, automated or manual.

Notification of ad hoc files

At first glance, the responses concerning any obligation to notify to the ISA *ad hoc* files set up at the time of particular inquiries also suggests a mixed approach. However, this may stem either from respondents misunderstanding R(87)15 terminology, or the inapplicability of the concept in some jurisdictions. A closer examination suggests that, in practical terms, the apparent differences arise because at least eight States do not explicitly differentiate between *ad hoc* and other files, meaning all files are subject to the data protection law applicable to police files, including notification. One State indicated that the notion of *ad hoc* files does not exist in its national law; all police files must be notified according to the ordinary legal rules, at the time of the creation. In four States, while there is an obligation to notify all (automated and manual) permanent police files to the ISA, this does not apply to *ad hoc* files. In another, the obligation to notify only applies to automated permanent police files, and not to manual or *ad hoc* files. Finally, in one State, while neither automated, nor manual permanent police files are subject to notification, by law the purpose of every *ad hoc* police file must be identified within a week and the privacy officer is obliged to keep a register of the purposes of those files.

Principle 2 – Collection of data

Collection Limitation principle and Wider police powers

There were a range of responses providing some interesting variations, especially in follow-up questions. Ten States declared categorically that collection of personal data for police purposes is limited to that necessary for the prevention of a real danger, or the suppression of a specific criminal offence. However, it seems likely that this question was worded in a way that gave respondents some pause, and that a 'yes' or 'no' response from respondents from different countries may have arisen from dissimilar interpretations of similar practices. Germany commented that the terms "the prevention of a real danger" and "the suppression of a specific criminal offence" are unclear, and considered that they were only able to provide general information: pursuant to the Federal Criminal Police Office Act, the BKA may only store data if this is necessary to fulfil its tasks. Where countries indicated instances of collection of personal data for police purposes not limited to that necessary for the prevention of a real danger or the suppression of a specific criminal offence, only five (of thirteen) provided details supporting their claims of appropriate specific national legislation authorising wider police powers to gather information.

Informing the data subject

Ten States indicated that that there had been no occasions on which data subjects had been informed where data concerning them had been collected and stored without their knowledge and had not been deleted once the object of the police activities was unlikely to be prejudiced (it is unclear whether data subjects were simply not informed, or whether data was in fact always deleted). Most other countries were unable to provide information on the issue. One State noted that their police are not required to communicate such information to the data subject. The

responses could be interpreted as indicating excellent police practice, inadequate information gathering or monitoring, or a mixture of all.

Data collection by automated means

Principle 2.3, R(87)15 refers to the "collection of data by technical surveillance or other automated means" requiring that such collection be placed on a legal basis. As originally drafted, "technical surveillance" was intended to refer to interception generally, and wiretapping in particular.[21] *Malone v. United Kingdom*[22] states that such technical surveillance must be authorised with reasonable precision in accessible legal rules that sufficiently indicate the scope and manner of exercise of the discretion conferred on the authorities, and be accompanied by adequate safeguards against abuse.

In their responses to the questionnaire, eight States identified specific provisions in national law regulating interception and providing safeguards, eight States identified specific provisions in their laws regulating covert surveillance and seven States indicated regulation of (overt) video surveillance (however, in each of these categories, the seven States were not precisely the same set of seven States). One state referred to laws regulating audio-visual recordings of the hearings in custody and audiovisual recordings of hearings of minors or incapacitated adults; another two referred to laws regulating the secret search of information systems. German federal law provides different legal bases depending on whether the purpose of the police activities is the prevention of threats posed by international terrorism or criminal prosecution (provided for in the Federal Criminal Police Office Act and in the Code of Criminal Procedure respectively). While all countries surveyed provided references to their laws, eleven (of thirty) did not indicate specific legal articles or provisions. One State's law indicates that "[t]he collection of personal data by technical surveillance or other automated means can be performed for police purposes, *or* in accordance with any law." This formulation clashes with R(87)15, which requires "specific provisions" for every instance of collection by automated means, but the respondent was unable to provide an example of such national law.

Concerning guarantees against abuse, many responses referred generally to national Constitutional or human rights provisions, procedural mechanisms (e.g. requirement of judicial warrant or Ministerial authorisation), and/or punitive measures in case of abuse. References were also made to:

- conditions for the exercise of such police powers narrowly defined in law;
- national jurisprudence premised on that of the ECrtHR;
- oversight mechanisms exercised by the ISA and/or by another independent control authority or institution specifically charged with such functions;
- restriction of use of particularly intrusive forms of surveillance to cases of terrorism and serious crime, and only in cases of concrete threats;
- the establishment of codes of practice, for e.g. in relation to video surveillance.

[21] See Explanatory Memorandum at para.46.

[22] 7 EHRR 14.

The responses to this question suggest that there is no common understanding of the term "technical surveillance or other automated means" among the States surveyed; national laws are not harmonized; and/or police practices, in so far as technical or other automated means of surveillance is concerned, vary from State to State. It is possible that if the question had instead asked specifically for a reference to law regulating, for example, interception, every State would have been able to identify some national law, and the procedures mandated therein (whether or not adequate safeguards are actually built in the law).

In general, States do not appear to have attained practical implementation of the related principle laid down in Art.7, CFD 2008/977/JHA dealing with "automated individual decisions", equivalent to Art.9, proposed Police and Criminal Justice Data Protection Directive (pPCJDPD) which refers to "measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject". The responses (or lack of them) to the questionnaire suggest many EU States are unprepared for implementation of either Art.7, CFD 2008/977/JHA or Art.9 pPCJDPD which both require specific laws with appropriate safeguards.

Collection of sensitive data

In brief, responses to the question about whether national law prohibited the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law, unless absolutely necessary for the purposes of a particular inquiry, was "Yes". However, further exploration uncovers a more complex picture with the following variations:

- collection of data on individuals solely on the basis of sensitive data elements is generally prohibited, subject to those exceptions and/or other special provisions generally applicable to all sensitive data (eleven States);
- collection is generally prohibited with no mention of exceptions (seven States);
- collection is generally prohibited with exceptions provided for in law (three States);
- collection is generally prohibited 'unless absolutely necessary for the purposes of a particular inquiry' – a precise borrowing of the language of R(87)15 (three States);
- collection is generally prohibited, unless explicitly provided for in law, and the law considers all police data as sensitive and provides restrictive provisions for all such processing (one State);
- collection is 'not explicitly authorised' while regulations are in force for when sensitive data is processed (one State)

As with the response to the question about informing data subjects, responses to further questions about sensitive data collection practices could be interpreted as indicating excellent police practice, inadequate information gathering or monitoring, or a mixture of all.

Principle 3 – Storage of data

Data Quality Principle

Reponses relating to the accuracy and necessity of storage of personal data for police purposes tended to focus upon general principles of data processing, including accurate and not excessive storage of data, in national law. Some States do, however, impose legal obligations upon the police to assess the accuracy or reliability of data. Seven States provide for internal controls, e.g. in Ireland, the Garda Information Service Centre (GISC) has a key role in ensuring the accuracy of data collected and stored for policing purposes; details of the role of the GISC in ensuring accuracy of data are set out in Section 4.5 of the Garda Síochána Data Protection Code of Practice. In eight States, in some cases coupled with internal controls, controls are also exercised by audits and/or spot checks carried out by supervisory authorities.

Accuracy and reliability

Responses received suggest that a slim majority of States have processes in place designed to improve data quality. Some States clarified that, while their police authorities do not distinguish categories of data by accuracy or reliability, they do distinguish data depending on type, e.g. data of a personal nature, data of a non-personal nature, data of a sensitive personal nature, data required for policing purposes, administrative data etc; and an assessment of accuracy or reliability of the data, or its factual or opinion/personal assessment-based nature, would, where possible, be attached to registered data.

A majority of States indicated measures are in place to improve data quality by distinguishing data based on facts from data based on opinions or personal assessment. This is an important issue for data subjects as police authorities often have recourse to soft data based on presumptions rather than on facts, and a data subject might be disproportionately affected by lack of accuracy in data relating to suspicions about him or her. It is also important for effective law enforcement: where there is exchange of data between police authorities, data may be processed far from their source, and completely out of the context in which they were originally collected and used. Failure to indicate some measure of accuracy and reliability could undermine the effectiveness of data exchanges, as police authorities would not be able to ascertain whether the data should be construed as ‘evidence’, ‘fact’, ‘hard intelligence’ or ‘soft intelligence’.

Administrative purposes

The majority of police forces in Europe are clearly still involved in the gathering of data which may be classified as administrative rather than investigative. It remains subject to conjecture why eleven States subject their administrative data (as distinct from the investigative or preventative data) to the special regime for police data.

Principle 4 – Use of data by the police (statement of the notion of finality)

Police data used for other purposes

In general, it appears that the principle of purpose, the hallmark achievement of R(87)15, is respected. The majority of countries declare the principle of finality/purpose specification/purpose limitation in their laws. On the issue of whether national rules permitted

personal data collected and stored by the police for police purposes to be used for other purposes, eleven countries responded 'no', without exception; eight responded 'yes', when in accordance with law. For e.g. in Germany, generally data stored for police purposes may only be used for police purposes. The use of stored data for other purposes is possible only on the basis of a special legal provision[23]; other countries responded 'yes', giving examples of such other purposes, e.g. for vetting and security clearance purposes, e.g. vetting for people applying for public sector posts, posts involving the care of minors, etc.; and disclosure of criminal records and police information about potential employees to prospective employers.

Principle 5 – Communication of data

Exchange of data between police bodies

The picture that emerges is that while communication of data between police authorities appears broadly to be taking place as permitted, or as provided for, by law, what this means depends upon the legal culture of the country concerned, e.g. in some countries it is unclear if bilateral agreements with other police forces are subjected to legal scrutiny. The variety of the responses is instructive in the nuances of the local legal cultures of the States surveyed.

Legitimate interest?

While States were overwhelmingly of the opinion that their police authorities were required to have a "legitimate interest" in order to obtain data from other police authorities, precisely how "legitimate interest" is defined is a case-study in European diversity.

- nine States averred that performance of duties/fulfilment of a task conferred upon a receiving law enforcement authority by law constituted a legitimate interest;
- two States were of the opinion that it should be the requestee, i.e. the would-be provider of the data, who determines the presence or otherwise of a legitimate interest, while the requesting party should give reasons;
- some police authorities had to rely on specific legal provisions authorising the communication or exchange of data with other police bodies for specific purposes – indeed in some countries data may only be communicated or exchanged when a legitimate interest is established pursuant to law;
- some States require the use of appropriate channels, evaluation and handling codes, and conventions; in cases of routine data exchanges, specific memoranda of understanding ("MoUs") may also be in place to regulate the process.

The UK proved an exceptional case in that, in general terms, in the UK 'legitimate interest' means that there should be no law specifically prohibiting such processing; in the specific context of the DPA 1998, 'legitimate interest' means that any legitimate interest pursued by the Police or third party in conjunction with the Police should only be initiated without prejudicing the rights and freedoms or legitimate interests of the data subject.[24]

[23] E.g. Federal Criminal Police Office Act, s.29.

[24] ICO response to questionnaire.

Most states indicated that they had an oversight mechanism for exchange of data between police authorities. In general, respondents did not elaborate further; it appears that most States consider the oversight exercised by their ISA to be sufficient in the case of internal exchanges of personal data between police bodies.

Communication to other public bodies

A police authority may be able, or be required, to transfer data it has collected to another public authority for a purpose unrelated to law enforcement, e.g. police authorities could be required under national law to disclose information to immigration services or taxation authorities, or these recipients could be allowed under national law to receive police information from competent authorities.

It is possible to identify a range of approaches to when communication of police data to other public bodies is permissible:

- if explicitly provided for by law (nine States);
- on the basis of a legal provision or with the authorisation of the ISA (three States);
- on the basis of a legal provision or with judicial authorisation (four States);
- on the basis of a legal provision or with ministerial authorisation (one State);
- on the basis of a legal provision or with the authorisation of the ISA and in other cases (one State);
- on the basis of a legal provision or with judicial authorisation and in other cases (three States);
- on the basis of a legal provision or with the authorisation of the ISA or with judicial authorisation (one State);
- on the basis of a legal provision or with ministerial authorisation and in other cases (one State);
- on the basis of a legal provision and in other cases (three States);
- on the basis of agreements with public bodies who require the data for the performance of their tasks, e.g. social security (three States).

Thus, in two-thirds of the countries surveyed the police authorities require a legal basis or an official authorisation from the ISA, a judicial body or a Minister to communicate data to another public body, i.e. they may not communicate personal data under any other condition, suggesting that European legislation regarding this matter is quite strict.

It is interesting to note what is “lost in translation” into national laws. Maltese legislation provides that communication of personal data from bodies exercising police powers to other public bodies may only be made if (inter alia) “there exists a legal obligation or authorisation to communicate such data.” The adjective “clear” found in R(87)15 in “clear legal obligation” is thus omitted in the Maltese provision. One may speculate why Malta felt the need to lower the

R(87)15 standard, even despite largely adopting a 'cut and paste' approach in transposing the Recommendation into Maltese Law.

Legal authorisation or obligation to communicate data to other public bodies

Most States indicated that their national legislation placed a clear legal obligation on the police authorities to communicate data to other public bodies.[25]

Apart from whether there instances in the law of a clear legal *obligation* on the police authorities to communicate data to any other public bodies, this author (and drafter of the questionnaire) should have also asked whether there are instances in the law of a clear legal *authorisation* on the police authorities to do so; in other words, distinguishing between that which is "permissible" and that which the police may be "obliged" to do. Not having asked this further question was an omission on the author's part. Nevertheless there are generally instances of national legislation concerning certain other authorities and providing for the right of those authorities to obtain data from the police in specific circumstances.

Swiss Federal law provides an interesting example of flexible provisions in this instance: the communication of police data to other public bodies is permitted to the extent necessary to assist such other bodies in performing their legal tasks. The police authorities may communicate data to other Swiss and foreign authorities, for e.g. law enforcement, customs and immigration, in view of the performance of their legal duties or the execution of international obligations. Several public services have access to police information systems, in accordance with their purposes, for the accomplishment of certain of their tasks provided for in law, e.g. migration and law enforcement authorities to the SIS. The police may also communicate data to internal control services for the accomplishment of their legal tasks together with their maintenance and programming work.

Authorisation to communicate data to other public bodies

The overwhelming majority of states reported that there are no instances in which the ISA may authorise communication of data by the police authorities to other public bodies.

The rationale for this appears to be that in some (11 of those surveyed) states there may be some other authority which is so empowered, e.g. judicial authority (7 countries) or the Minister for Justice or the Minister for Home Affairs (2 countries).

While roughly half the countries surveyed reported that there are no other circumstances in which their police authorities are authorised to communicate data to other public bodies, there are at least nine member States where they are authorised to do so, e.g. processing is necessary in order to protect the vital interests of the data subject or in the general public interest. In such circumstances, the police generally exercise a certain margin of discretion. Once again, unfortunately, the wording of the question wasn't ideal in so far as it may have

[25] The determination of the sufficiency or otherwise of the clarity of the legal obligation is based on the determination provided by the countries in their responses. The authors did not, for the purposes of this report, attempt to set any such standard of clarity and determine, according to such other standard or measure, whether the qualification of clarity was in fact justified.

been confusing with regard to whether the term ‘legal’ also qualifies ‘authorisation’ – as in, ‘legal authorisation’, or in other words, a legal basis.

Only a few States reported qualifications to the authority granted in cases of transmission of police data to other public bodies.

On the matter of oversight mechanisms and finer distinctions between determinations of authorisation and the authorisation itself, a third of the countries surveyed explicitly confirmed the existence of an oversight mechanism. In those countries where communication of data is only allowed in cases of legal obligation or authorisation or on the basis of an authorisation of an official authority such as a judicial or ISA, oversight mechanisms would not in this case be necessary.

States responded that there have been no cases of communication to other public bodies being exceptionally permitted, or that there is no such information/statistics available, or that the question is not applicable to them.

Communication to private parties

Three States reported that the communication of police data to private parties is not permitted in any circumstance.

For the other States, it is possible to identify a range of approaches to when communication of police data to private parties is permissible:

- only if there is a clear legal obligation or authorisation (three States);
- only if there is a clear legal obligation or authorisation, or with the authorisation of the ISA (one State);
- only if there is a clear legal obligation or authorisation, or with the authorisation of a judicial authority (three States);
- if there is a clear legal obligation or authorisation, and in other circumstances circumscribed by law (five States);
- if there is a legal obligation or authorisation (not necessarily a clear one?) (three States);
- if there is a legal obligation or authorisation, or the consent of the data subject (one State);
- if there is a legal obligation or authorisation, or with the authorisation of the Attorney General and in other circumstances (one State);
- with judicial authorisation and in other cases (one State);
- only at the request of the data subject (one State);
- only on the basis of consent (one State);
- as provided in the police code of practice (one State).

The comment made with regard to the Maltese legislation in the section on communication of police data to other public bodies is again applicable in the case of communication to private parties: Maltese legislation merely requires the existence of a "legal obligation", rather than the "clear legal obligation" stipulated by R(87)15. This may be contrasted with the position in Switzerland where the communication of police data to private parties is allowed only in specific cases and under restrictive conditions: such communication is regulated for each police information system, in principle by ordinance, e.g. under the ordinance on the system for computerised searches of the police (RIPOL), such communication is not expressly prohibited or excluded; the Ordinance provides that the communication of data to third parties must be accompanied by a note specifying that the data must be processed confidentially and that they may not be transferred to other interested parties.[26] In the federal law instituting measures for the maintenance of internal security, the communication of personal data to individuals is only allowed: if it is undoubtedly in the interest of the person concerned and this person has given his or her consent or circumstances indicate that such consent would have certainly been given; if it is necessary to avoid an immediate, serious danger; if it is necessary to justify a request for information."[27]

It is interesting to note that almost half the countries surveyed reported a clear legal obligation or authorisation on the police authorities to communicate data to some private party or parties.[28] Eight countries reported no such instance in their laws.

The lack of discretion allowed to ISAs is highlighted by two thirds of countries responding that there are no instances in which the ISA may authorise communication of data to private parties. Of the other third, only two countries appear to have explicitly made provision enabling the ISA to authorise the communication of police data to private parties. Nevertheless, almost one-third of the countries report other mechanisms which may achieve the same result; indeed, roughly half of the countries that do not provide for any instance in which the ISA may authorise communication of data to private parties, grant such power of authorisation to some other authority, e.g. judicial authority (five countries), the Attorney General (one country) or the Minister of Justice (one country). This state of affairs raises the question as to whether it is appropriate, i.e. whether it would have been better to let such decisions be taken by the ISA. It is as yet unclear as to how much public consultation or parliamentary discussion has underpinned those policy decisions which have accorded discretion for transfer of police data to private parties to any other authority which is not the ISA.

Finland provided a clear example of a practical instance in which data processed for police purposes is communicated to private parties: for the purposes of background checks referred to in the Act on the Processing of Personal Data by the Police,[29] a private corporation and foundation, whose seat, central administration or main operative unit is located in Finland, and a foreign corporation or foundation that has a registered branch in Finland, may apply for a

[26] Ordonnance RIPOL, Art. 7 (al.5).

[27] LMSI, Art. 17 al. 2.

[28] The determination of the sufficiency or otherwise of the clarity of the legal obligation is based on the determination provided by the countries in their responses.

[29] Act 761/2003, s. 21.

background check on persons seeking an office or position, persons to be admitted to a position or training, or persons who are performing an office or position. However, the data is communicated to the Security Police that is responsible for carrying out the background checks.

The research did not reveal whether communication of police data to private parties had ever been exceptionally permitted. Six States stated that no cases are known while the rest reported that no data was available…or said nothing at all. In Germany this has never taken place as it is not permissible.

Communication to Foreign Authorities

Roughly one third of the countries surveyed reported that the communication of personal data to foreign authorities is limited to police authorities; three other countries reported communication only to police and judicial authorities; four other countries reported that they can communicate police data to a foreign non-police organisation if this is specifically provided for by law.

Switzerland applies a wide definition to what may be termed a police authority interpreting it as law enforcement authorities in the broad sense: not only police authorities, but also prosecuting authorities, migration authorities, road traffic authorities, civilian and military justice authorities, authorities of execution of sentences.

Law regulating communication

Without exception, in all the countries surveyed, communication of data by a police force to a foreign authority is covered by a clear legal provision under national or international law, including bilateral and multinational international agreements. Much exchange of police data across borders happens within the framework of international conventions relating to police and judicial cooperation, such as multilateral conventions of the CoE, (e.g. the Convention on Extradition;[30] the Convention on Mutual Assistance in Criminal Matters;[31] the Convention for the Suppression of Terrorism;[32] the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime;[33] The Criminal Law Convention on Corruption[34]); UN multilateral conventions (e.g. the United Nations Convention against Transnational Organized Crime;[35] the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[36]); as well as conventions on the fight against terrorism or drug trafficking, bilateral agreements, extradition treaties, and cooperation within international police organisations, such as Interpol and Europol.

Most States surveyed indicated that without a clear legal provision enabling them to do so, there are no circumstances in which police authorities in their countries could communicate personal data to foreign authorities. Four states provided novel exceptions: Ireland stated that such

30 CETS no. 24, in particular Art.16 para.3 (transmission by Interpol).

31 CETS no. 30.

32 CETS no. 90.

33 CETS No. 141 (in particular Chapter III).

34 CETS no. 173, (particularly Chapter IV).

35 Of 2000.

36 Of 1988.

communication may happen only with the approval of the Commissioner of An Garda Síochána; Malta merely cites the grounds given in R(87)15 itself, i.e. “if the communication is necessary for the prevention of a serious and imminent danger, or necessary for the suppression of a serious criminal offence”; Switzerland cites reciprocity and the UK refers to compliance with the Information Commissioner’s Data Sharing Code of Practice.

Oversight mechanisms

Generally oversight of those circumstances which are determined to warrant communication of data to foreign authorities is exercised by national ISAs. There are also a number of Joint Supervisory Authorities at EU level including the Europol Joint Supervisory Body, the Joint Supervisory Authority of Schengen, the Joint Supervisory Authority of Customs, etc.

Ireland provides a useful example of good practice, in that apart from oversight by the national ISA, the Garda Síochána also has internal audit and professional standards mechanisms, and is independently overseen by both an Inspectorate and an Ombudsman Commission with legislative basis and high levels of access to data. Sweden has also established an array of oversight mechanisms: the Central Security Log, inspections carried out by the National Police Board, ordinary supervision by the Data Inspection Board and the Swedish Commission on Security and Integrity Protection, as well as extraordinary supervision by the Parliamentary Ombudsman or the Chancellor of Justice.

It is unclear whether communication of police data to foreign authorities has ever been exceptionally permitted in the absence of a clear national or international provision. Eleven States indicated that no cases are known while the remainder (bar one) reported that no data was available. Consistent with their response to the previous question, most countries returned a blank when asked what circumstances would justify a communication of data by the police to foreign authorities if this was not provided for by law.

Information required by countries

When faced with a request for information from another country, the States all require identification of the body or person requesting the data, the reason for the request and its objective, and an indication of the data being requested. Unsurprisingly, much exchange of police data takes place within the framework of cooperation agreements (including Schengen, Prüm, the European Convention on Mutual Assistance in Criminal Matters etc.) and international police organisations, such as Europol and Interpol.

Verification and completeness of data

Less than half of the States surveyed reported they have structures in place to verify data quality by the time of their communication, e.g. internal supervisory functions, internal audit, professional standards etc. A third of the States reported no specific structures, but suggested that data protection principles, including data quality, are applied. Approximately half the States indicated the primary strategy required by law where inaccurate or out-of-date data have been communicated is that the communicating body should inform, as far as possible, all the data recipients of its non-conformity.

Six countries reported their police authorities have structures to ensure for all communications of data, that judicial decisions, as well as decisions not to prosecute are indicated and data based on opinions or personal assessments are checked at source before being communicated. Three countries explained that they explicitly do not communicate judicial data: in one case the police services do not systematically dispose of judicial data and thus specify to the receiving authority that the data transmitted are police data; in another case although details of convictions and acquittals are public information, while decisions not to prosecute are not and are therefore not communicated internationally; in the last case, court decisions are only mentioned with the express authorisation of the Prosecutor General. In the latter case, data communicated are based solely on official decisions, avoiding opinion or personal appreciation.

Safeguards and purpose

Most States surveyed responded that safeguards are in place to ensure that data communicated to other public bodies, private parties or foreign authorities are not used for purposes other than those specified in the request for communication; however, when specifying what they understood by "safeguards", reference was usually to data protection principles, national legal provisions , or the fact that data was transferred subject to this condition. Three States reported that they employed further safeguards, e.g. requesting the recipient to report back on the use of the data and the results accomplished, or the possibility of a sanction being imposed by the ISA. Germany noted that the fact that data are transmitted only if necessary helps minimize the risk that the data are processed for other than the agreed purpose; the legal provisions governing data transfers to foreign countries are even stricter: personal data may not be transmitted if there is reason to assume that their transmission would be contrary to the objectives of a German law.[37] Three States reported that no safeguards are in place. Whether this means that the latter set of countries are the least diligent or the most honest requires further investigation, e.g. the Netherlands does not categorize a condition for transfer as a safeguard.

From the responses received it is clear that in general, if public bodies, private parties or foreign police authorities use the communicated data for purposes other than those specified in the request for communication, then they are not asking permission to do so. The Swiss response revealed that approximately twice a year the Federal Office of Police receives requests seeking all available data linked to a person of a given nationality – which requests have never been acceded to.[38] Ireland noted that Europol periodically discovers links with new investigations, and requests that the sending country allows their data to be shared with a different investigative group; while specific data are not available, most would be acceded to where clear justification is provided.[39]

Interconnection of files

A minority of States reported (but did not always provide the relevant legal text) that their laws contain clear legal provisions authorising interconnection of police files with files held for

[37] Federal Criminal Police Office Act, s.14(7)

[38] Switzerland, response to questionnaire.

[39] Ireland, response to questionnaire.

different purposes (for e.g. social security bodies, passenger lists kept by airlines, trade union membership files). Thirteen States replied that their laws do not contain any such provision.

It appears that there are seven States where the supervisory body may grant authorisation for the interconnection of files with files held for different purposes e.g. in Andorra, the authorisation is granted only for specific purposes which must be in conformity with a statutory provision. In the other States the authorisation does not appear to be limited to 'the purposes of an inquiry into a particular offence'.

With the exception of Andorra and Cyprus, there appear to be no available records of occasions or instances where the interconnection of files with files held for different purposes have been authorised by supervisory bodies. The information from Andorra provides an interesting example of an application of their law in practice: this authorization was given only once on the basis of a regulation in the context of the organisation of the Games of the Small States of Europe; the purpose was to ensure state security and consisted in the communication to the police services of persons lodging in hotels.

Secure on-line systems

Police forces across Europe do not seem to have escaped the general trend to moving information systems on-line. While seven States definitively stated that none of their police systems are available on-line, the others have some of their systems accessible on-line, albeit usually with a variety of security measures. Germany clarified its understanding of the term "on-line" to refer to access via the Internet, stating that the Internet was intentionally excluded as an access to police data systems; however, there exists an electronic data network between the Federation and the Länder which is accessible through separate police networks. This data network is run by the BKA as the central agency. The legal basis for this network is section 11 *et seq.* of the Federal Criminal Police Office Act.

Legal direct access to a file

Responses to the possibility of the police having a direct computerised access to files held by different police bodies or by other bodies,[40] suggested approximately half the States' domestic legislation allows direct access or online access to a file. A note should be added here: the question in the questionnaire reads – "Does the domestic legislation of your country allow direct access or online access to a file?" In retrospect, there is a lack of clarity insofar as the question did not specify that the direct access that R(87)15 refers to is to files held by different police bodies, or by other bodies.

With regard to specific safeguards where direct access or online access to a file is permitted, States referred to a mix of legal, technical and organisational measures, e.g. legislation that allows direct access only in specific cases or that defines, expressly and exhaustively, for each police information system, the authorities and services having online access to that system, as well as the purposes for which these data are to be exclusively used; with regard to IT security, some countries have established a legal requirement upon the controller of personal data to implement appropriate technical and organisational measures to protect the personal data that

[40] Explanatory Memorandum, para. 80.

is processed. One country specified the following mechanisms: access read-only, not copy; risk analysis; security documentation; rules of personal, premises and industrial security.

Principle 6 – Publicity, right of access to police files, right of rectification and right of appeal

Transparency

The measures taken by ISAs to satisfy themselves that the public is informed of the existence of police files, as well as of the rights of individuals in regard to these files, range from the publicising of a register of data applications notified to the ISA as a legal requirement (of eight states, two publicise the existence and nature of files by publication in a Government Gazette, and one has set up a web-accessible register) to making the relevant information available on the website of the police, or of the relevant Ministry and/or of the ISA, and providing additional information through other media. One state organises seminars addressing these issues.

Publicity vs. ad hoc

Approaches were divided on the issue of *ad hoc* files where just over a quarter of States reported no differentiation being made between permanent and *ad hoc* files while just under a quarter report that the special nature of *ad hoc* files are taken into account. The responses of the other States were unclear on this point.

Access to police data

The vast majority of the States surveyed (more than 75%) report that a direct right of access to their police file is, where appropriate, available to the data subject.

In Luxembourg the right of access to a police file may only be exercised indirectly, that is to say through the Art.17 ISA. This authority carries out verifications and investigations within the framework of an access request, makes the necessary rectifications and subsequently informs the data subject that the processing in question contains no data contrary to conventions, to the law and to its implementing regulations.[41] French law also allows the controller, in some cases, to limit the right of access to indirect access through the ISA. Monaco provides for both direct and indirect rights of access, but the modalities for the exercise of such rights are unclear from the response received.

Register of requests

Roughly half the countries surveyed operate a registration of requests for access to data while the other half claim not to do so. Where a request for access is registered this is maintained separate from a person's criminal record. The response from the Slovak Republic explains that their law requires the police force to keep records of every provision and accessibility of personal data for purposes of verification of legitimacy of personal data processing, internal control and assurance of personal data protection and safeguards.[42]

---

41 Art.17 para.(2) of the amended law of August 2, 2002.

42 Act No. 171/1993 Coll., Art. 69(14). When reading this law clarity was at times lacking due to a poor translation.

Rectification or erasure of data

While one might have expected that States would have set up a communication channel for data subjects to address requests for rectification or erasure, in most cases such information was not provided. Neither was much (or any) detail given as to what precisely is expected from the data subject by way of request formalities.

In general, data subjects are expected to address themselves to "the controller" or other person responsible for the processing of police files – although who the controller or the person responsible for the processing of police files is, is not always clear. In some cases, the data subject may address the ISA, e.g. a clear channel of communication is established in Luxembourg where the data subject is required to apply to the Art.17 ISA in writing; in France a request may be directed to the person responsible for the processing, or to the CNIL.

Half the States surveyed reported that they have no information on how many data subject requests for rectification or erasure of data contained in a police file have been received by the police authorities. Where States provided figures, these ranged from one to hundreds, with the Swiss reporting the highest single annual total (416, 2010), and the Irish reporting the highest average per annum (600).

It is disturbing to realise that more than half the States surveyed were unable to declare on how many occasions data held by police in their countries was found to be excessive, inaccurate or irrelevant as per R(87)15. Eight countries declared that this had not happened within their jurisdiction while the UK reported that there have been 42 cases since 2005 where the ICO has found that the information held by a police or law enforcement authority was inaccurate, excessive or irrelevant.

Follow-up action

The range of follow-up action to requests for access ranged from audits being undertaken to better awareness of creation, supervision and deletion. The time lapses required for remedial action ranged from "without delay" (Sweden) to non-specified cases at the discretion of the case officer (UK). Ireland reported that data must be either provided or amended, as appropriate, within forty days but, in practice, data are updated and corrected more rapidly.

Refusing access, rectification and erasure

With regard to the instances in which the rights of access, and thus the rights of rectification and erasure, have been refused, States referred to those cases when the data requested regarded ongoing proceedings or surveillance, or when state security, defence or public safety were involved or generally when, if the data were to be communicated to the data subject, it would jeopardize the purpose pursued. The questionnaire asked about practical examples where rights to access/rectification/erasure were denied or restricted as laws alone were unlikely to provide any new insight. Previous research[43] (albeit within the context of the EU and the EEA Member States) has already noted that

[43] Report from the Commission on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, COM(2012) 12 final.

all Member States provide for exemptions from the right of access. The most frequently mentioned reasons for not granting the right of access are:

– to prevent, investigate, detect and prosecute criminal offences;

– national security, defence and public security;

– economic and financial interests of a Member State and of the EU (including monetary, budgetary and taxation matters);[44]

– to protect the rights and freedoms of the data subject or other persons.

Most responses did no more than refer us to the relevant legal provision. While in general the grounds for refusal of access, rectification or erasure are laid down by law, few countries appear to have considered the possibility of the police refusing to communicate the *reasons* for a restriction or refusal of the data subject's rights to access, rectification or erasure of data. It is possible that some countries did not quite understand the focus of the next question on a refusal to *give reasons* rather than grant access/rectification/erasure.

A minority of the States reported that their laws obliged the police authority to provide a data subject with a *reasoned* restriction or refusal of the exercise of their rights to access, rectification or erasure of their data. France and Luxembourg both responded that their laws do not oblige the police authority to provide the data subject with a reasoned restriction or refusal, as access is indirect, i.e. exercised via the respective ISA.

With regard to the circumstances in which the police may refuse *to communicate the reasons* for a restriction or refusal of the data subject's rights to access, rectification or erasure of data, many States stated or repeated the set of reasons for the actual restriction or refusal. Interestingly however, four States stated that the police may not refuse to communicate the reasons for a restriction or refusal.

A majority of States reported that a data subject is given information on how to challenge decisions if he is not granted access to, or rectification/erasure of, his data. Nevertheless, there were three exceptions: Austria responded that there is no legal obligation to inform the data subject on the ways and means to challenge the decision; Cyprus responded that the Police's self-binding Charter of Citizens' Rights, which is posted on its website, does not provide any information regarding the right to appeal to the Commissioner in accordance with the provisions of s.12(3) of the law; the UK reported that, while not a mandatory obligation on police authorities, in any response to a subject access request, it is good practice to refer to the right to contact/appeal to the ICO.

Right of appeal

Nearly all countries surveyed reported that their law provides for a right of appeal to the ISA or to another independent body (for e.g. a court or tribunal) from a refusal to grant access. Principle 6.6 of R(87)15 seems to have been implemented fairly consistently around Europe.

[44] This is not an exemption that is expressly mentioned in Art.17 of Framework Decision 2008/977. It does, however, reflect an exemption listed in Art.13 (1) of Directive 95/46/EC.

Only in six States is the ISA or other independent body obliged to communicate the data to the individual if there is no justification for refusing access. In just under half of the States, the ISA is not obliged, or not permitted, to communicate the data. In the latter cases, if the data controller does not respect the decision of the ISA, additional action normally involves the taking of administrative or judicial action to enforce the decision, e.g. in Austria, if the Data Protection Commission renders a binding decision in accordance with § 31 of the Federal Act concerning the Protection of Personal Data (DSG 2000), the public sector data controller is obliged to abide by the decision. If the decision is not abided with, the relevant servant of the controller may be subject to criminal charges which are brought by the prosecution service; if the Data Protection Commission adopts a non-binding recommendation in accordance with § 30 of the same Act and the controller does not implement it, then the Data Protection Commission may initiate criminal action by informing the prosecution service or the competent district authority.

Appeals to independent supervisory authority

The number of occasions where denial of an access request has been challenged before the ISA or other independent body varies very widely across Europe, ranging from no cases (in ten States) to over a thousand in the past five years (in the UK).

Only 3 countries could provide information regarding occasions in which the ISA or other independent body decided that there was no justification for the police authorities refusing access: Estonia reported that there have been about 15 cases in the last 2 years in which the ISA granted access; Ireland reported that, while the Office of the Data Protection Commissioner would, if appropriate, provide advice to the Gardaí to supply additional data following the review of a complaint, there were no cases in which the Office had to use its legal powers to require provision and it always received full cooperation from the Gardaí; the UK ICO has investigated 1100 cases of request for assessment against police authorities since 2005 and of these has found 273 to involve non-compliance, advising remedial action in 165 cases and recommending no remedial action in the others. As regards remedial action, the UK reported that various methods have been undertaken to achieve compliance, including requesting disclosure of the data refused, updating procedures to comply with the UK DPA 1998 or the ICO's opinion, or disclosing the information in a format that would not breach the DPA 1998.

Principle 7 – Length of storage and updating of data

Time-limitation principle

In relation to handling of personal data kept for police purposes when those purposes have ended, a minority of countries have automatic systems in place to flag or delete certain data, on expiry of set time periods. Other typical measures include legal provisions, police internal controls/measures and the supervisory function exercised by ISAs.

Most States have, or are about to introduce, rules fixing storage (or conservation) periods for different categories of personal data collected and stored for police purposes. The diversity of authorship of those rules demonstrates the variety of approaches found within Europe's legal cultures. Most States attribute the authorship to one, or a combination, of: the legislator or legal

drafter within the responsible ministry (by federal law, ordinary legislation, bye-laws, regulations etc.), the police authorities and the ISA.[45]

Data quality principle

Most States indicated that they have rules requiring regular checks on the quality of personal data collected and stored for police purposes. However, ten States provided no evidence of close attention to Principle 7.2, R(87)15. Ireland provided a good practice example: the Garda Information Services Centre (GISC) are tasked with quality assurance of data entered into PULSE by both Garda members and GISC staff on foot of incident reports phoned in by Garda members; the Gardaí utilises a data analysis service to determine crime trends: this has the added benefit of identifying erroneously entered or missing data.

The diversity of responses about authorship of data quality rules is not dissimilar to those on the time-limitation principle; again one, or a combination, of the legislator/legal drafting by the relevant government ministry, the police authorities, and the ISA.[46]

Principle 8 – Data security

Physical and logical security

Most States reported that the "responsible body" (i.e. controller of the police files) has taken all the necessary measures to ensure the appropriate physical and logical security of the personal data collected and stored for police purposes. Examples include denying physical access by unauthorized personnel to buildings, facilities, resources, or stored information, by various authentication processes (e.g. using pass cards/badges and keys), and preventing logical access using software safeguards for the police's systems (e.g. user identification and password access, authentication, access rights and authority levels, right to make changes, log of access, creation, modification and printing). Some States reported the use of tiered access/edit/save rights; the appropriate level of rights provided to officers is established by police management depending on the category of staff, staff skillsets, and workplace requirements.

Audits may be used by data processing centres ensure security and reliability of data. The Czech Republic and Hungary specifically referred to checks/inspections carried out by their ISAs.

Italy provided a good practice example, noting that the *Garante* carried out investigations in 2005 to verify appropriateness of the legally required security measures relating to personal data processed by the Data Processing Centre (DPC) of the police. Following those investigations – which highlighted several criticalities in terms of data security – the *Garante* issued a decision (on 17 November 2005) requiring the Public Security Department (PSD) to enhance the protection of DPC information.

Two-thirds of the States indicated that they have implemented Principle 8, R(87)15 ensuring the different characteristics and contents of files containing personal data collected and stored for

[45] Country-by-country responses are outlined in Table 91, Annex C.

[46] Country-by-country responses are outlined in Table 93, Annex C.

police purposes are taken into account. In the decision noted above, the Italian *Garante* considered it necessary and appropriate to use encrypted storage for at least some data categories, the PSD having indicated that they used encrypted storage for especially confidential information contained in their systems.

R(87)15 – From findings to the future - Where do we go from here?

Key findings – Thirty-three points to ponder

The key findings of the report may be organized into two broad categories: two overall findings and thirty-one provision-specific findings.

Overall findings

The States' responses suggest that, at the very least, the majority of the provisions of R(87)15 have resulted in, or influenced development of, national rules. While, as is to be expected, there are variations in the way that States have chosen to implement R(87)15, it appears that, on paper at least, there is political will to at least acknowledge data protection principles in the law enforcement sector. There is little doubt that some States take data protection in the police sector very seriously indeed, but difficult to also escape the impression that such approaches are neither uniform nor universal.

Even with greater harmonization of legislation, it is likely that national interpretations and enforcement practices would remain divergent in practice, because of the principle-based style of R(87)15. Open-textured norms, and broad concepts in the style of general clauses (such as the "legitimate interest test"), will inevitably be interpreted and applied differently against a backdrop of different legal cultures and traditions.

This first overall finding is very significant: it should cause the policy maker and the data protection law expert to pause and reflect on the *raison d'etre* of a legal instrument in this field and especially on the virtue of having a new one and what form should such a new legal instrument take. Some recommendations arising out of these reflections are considered in the final section below.

A second overall finding concerns the lack of clear understanding of the practical application of the law or, at least, the lack of information available (or willingly communicable) regarding what actually happens in practice. A common feature of the responses received to the questionnaires is the relative ease with which respondents could identify relevant legal principles/regulation, but found difficulty in providing accurate information with regard to application of the 'law in practice' by police authorities. Respondents from the Independent Supervisory Authorities (ISAs), but also from the ministries responsible for the police, often seemed to have limited knowledge of, or information about, police practices. Audits of police authorities and in particular of their data processing practices do not appear to be a common practice among the CoE States. This second overall finding is also addressed in the final section below.

Provision-specific findings

A number of observations may be drawn from the analysis carried out in this report, especially if one were to examine the findings on a provision-by-provision basis:

1. Lack of clarity regarding the definition of “police purposes” – does this cover processing carried out only by ‘police authorities’ or also certain processing by customs and immigration authorities? Certainly data processing activities for police or law enforcement purposes are also carried out by the latter authorities.
2. The issue of manual processing appears to have become a non-issue – most countries subject manual processing to data protection regulations – and most processing for police purposes is now carried out using automated means.
3. The question regarding whether bodies consisting of individuals should have data privacy rights is not yet settled: there remain persistent differences between national legal regimes.
4. Most States subject data processed for purposes of state security to data protection rules, only two countries reported that it is regulated by a specific, separate data protection law.
5. All States have a (general) supervisory or data protection authority; only three countries have established an additional police or security-specific data protection institution.
6. There appears to be increasing uptake in Europe of practices such as PIAs, and the concept of Privacy by Design (PbD), although States do not necessarily use these precise terms, or interpret them in similar ways.
7. There is a trend to require advance consultation with ISAs where introduction of automated processing methods raises questions about the application of data protection principles. In those countries which require a legal basis for personal data processing, consultation is generally carried out during the legislative process.
8. There is a less pronounced trend to remove requirements of notifications of data processing operations to ISAs.
9. Many countries do not make a distinction between permanent and *ad hoc* files.
10. As regards “technical surveillance or other automated means”, national police practices, and the laws regulating them/providing safeguards remain diverse.
11. The collection of personal data solely on the basis of sensitive data categories is generally prohibited.
12. Obligations which go beyond a mere declaration of data quality principles in the law of the country concerned include: assessing the quality of data e.g. by internal controls, with oversight, e.g. via audits or spot checks, by the ISA.
13. Systems of data classification are implemented by a majority of police forces.
14. A majority of police forces are involved in the gathering of administrative data.
15. The principle of finality (purpose–specification and –limitation) appears to be accepted and adopted, at least in principle, across Europe.
16. Generally police bodies may exchange personal data based on (1) the duties/tasks of the receiving police body or (2) pursuant to a law or MoU. Generally police authorities

are granted discretion as to whether to reject or accede to a request for communication of personal data.

17. In a third of the countries surveyed the police authorities require a legal basis to communicate data to another public body, i.e. they may not communicate personal data under any other condition.

18. In the vast majority of member States, there are instances of a legal obligation or authorisation for the police to communicate data to other public bodies such as customs and immigration services.

19. The transfer of police data to private parties is a sensitive matter and is strictly regulated in the majority of the countries surveyed – either by not being permitted at all, or by being permitted but only if there is a legal basis or subject to specific cases and under restrictive conditions.

20. It appears that, without exception, in all the countries surveyed, communication of data by a police force to a foreign authority is covered by a clear legal provision under national or international law, including bilateral and multinational international agreements.

21. Oversight is mainly carried out by national ISAs and EU-level Joint Supervisory Authorities (e.g. Europol JSA, Schengen JSA etc.).

22. Less than half of the States reported that they do have structures in place whereby, at the latest at the time of their communication, the quality of data is verified, e.g. by way of internal supervisory functions, internal audit, professional standards etc.

23. Less than half the States reported (but did not always provide the relevant legal text) that their laws contain clear legal provisions that authorise interconnection of police files with files held for different purposes.

24. Police forces across Europe appear to have joined the general public/private sector trend of moving data systems on-line.

25. Safeguards include a mix of legal, technical and organisational measures.

26. There are two types of system governing the right of access to police data files: in some countries the right of access is direct, i.e. the person concerned applies directly to the authorities handling the data (police, customs, etc.); in others it is indirect, i.e. the person sends his request for access to the national data protection authority; the data stored for law enforcement purposes is verified by the data protection authority. Arrangements for disclosing data vary from country to country and can be extremely limited in some cases.

27. The grounds for refusing access/rectification/erasure are quite harmonised in principle (this study did not afford an in-depth view of the application of these grounds in practice).

28. Less than half of the States oblige their police authorities to provide a data subject with a reasoned restriction or refusal of the exercise of the data subject's rights to access, rectification or erasure of her data. This would appear to be a key failing as regards the openness/transparency requirements of R(87)15.

29. Nearly all States provide for a legal right of appeal to the ISA or to another independent body from a refusal to grant access.
30. Nearly all States have rules setting down data storage (or conservation) periods for different categories of personal data collected and stored for police purposes.
31. In most States the controller of the police files has put measures in place to ensure appropriate physical and logical security of personal data collected and stored for police purposes.

These thirty-one provision-specific findings are also significant, each in its own way. They serve to, on the basis of what R(87)15 had specifically provided for:

i. highlight those points where the provisions of R(87)15 may require further clarification or detailed explanation;
ii. illustrate those points where European states seem to have moved more easily towards a consensual way forward;
iii. suggest those areas where national practices remain at their most diverse and where most attention may be required in order to achieve harmonisation where this is useful and appropriate;
iv. point to a number of areas where detailed guidelines and operational procedures for law-enforcement agencies may be most useful

Utility and Futility – some reflections on the way forward

The advocates of "soft law" might find some encouragement in the thirty-three key findings listed above for R(87)15 certainly seems to have left its mark across Europe. Some states integrated it into their laws lock, stock and barrel while others gave effect to its provisions in ways which they felt were more appropriate at the time. The issue as to how much R(87)15 is really "soft law" however remains an open question. It may be argued that it did not remain "soft law" for too long and that its adoption as a reference point for the Schengen Agreement was the point in time when one could mark its transition into something much less soft, so much so, that by the period 1999-2004, its adoption by aspiring EU candidate countries signified its at least partial integration into the "acquis communautaire". While this is not a finding which emerges directly from the questionnaire responses, ancillary research suggests that, clearly, the pressure was on for new EU Member States to comply with R(87)15 in order to "tick all the boxes" for EU accession. In such a context, the term "soft law" is debatable and arguably inapplicable.
The first overall finding indicated above does compel one to examine the raison d'être of the existing R(87)15 as well as that of any new legal instrument that may be designed to become a worthy successor.

Perhaps it is most useful to start these considerations by explicitly asking the obvious question "What is the point of having a legal instrument of any sort in the field of data protection and law-enforcement?" More specifically "why would such a legal instrument be useful to both the citizen and the law-enforcement agencies entrusted with protecting the citizen?" This leads one to consider a number of realities that characterise the European and indeed the global position in 2012-2013, the point in time when this report is being finalized:

Traditional national boundaries are breaking down or changing in nature. Two key factors here contribute to this reality that faces both citizens and law-enforcement agencies: the mobility of people and their data. Citizens and especially European citizens within those 28 member States of the Council of Europe that form the EU, have become much more mobile and computerisation in the form of e-services and e-government in tandem with the advent of the Internet as a commercial conduit has meant that personal data has become even more mobile than the physical person could ever be. Citizens and their data are increasingly in different places to their original national jurisdiction and are increasingly present in several national State jurisdictions at the same time on the basis of their work-patters, residential patterns and their on-line activities. In the past, in a different technological context, this mobility of citizens across States led to different solutions: international organs for police co-operation such as INTERPOL or national agencies which transcend state boundaries such as the FBI in the United States of America or, more recently, EUROPOL within the EU. When INTERPOL and the FBI were founded, they were predicated on the increased mobility of citizens across boundaries achieved thanks to technologies such as ships, aircraft and motor vehicles. The main difference in 2012-2013 is the added dimension to mobility to be found in personal data going across borders for myriad reasons, sometimes in synch with the movement of the physical person and often quite divorced from the physical movement or location of a data subject. The dictum “all politics are local” has recently been brought into doubt as the actions of politicians in one country increasingly have an impact on the citizens – and thus the politicians – in another country and this in synch with other aspects of globalization in the business sector. In 2012-2013, life has often stopped being “local” on account of mobility of people and their data and crime has thus often stopped being “purely local” and is increasingly transnational.

The opportunity to commit crime or become a victim of crime in “another place” while remaining in “yet another place”. The advent of the Internet has created cyberspace as a new location where citizens can trade and be robbed or defrauded. Cyberspace is also a new space where people meet and interact for reasons which traditionally have been held to be part of their private and family life, often falling under Article 6 of Convention 108. In both of these scenarios i.e. cyberspace as a market-place and cyberspace as a meeting place for private and family life, personal data has mushroomed into a marketable commodity as the basis of a new business model.

The opportunity for and ability of a law-enforcement agency to monitor and obtain personal data from far beyond its borders but without moving from within its borders. The prevention and detection of crime, as well as its investigation and prosecution, have taken on new dimensions as law enforcement agencies have been compelled to teach their staff new skills, whether it is financial crime units being trained in Anti-Transnational Financial Crime (ATFC) techniques or officers being trained on how to monitor behaviour on Facebook and Twitter. When doing so however, investigators and prosecutors are faced with a constant jurisdictional issue: what precisely are the limits to their activities as they follow leads and suspects in cyberspace far across their borders into databases or user-generated content nominally or notionally under the jurisdiction of another law-enforcement agency?

The increasing reliance of law-enforcement agencies world-wide on access to data collected and processed in the private sector. The timely access to personal data which could be important or essential to the prevention, detection, investigation or prosecution of crime increasingly depends on the ability of the law enforcement agency in one country to access data held by the private sector possibly in another country;

The blurring of lines between public and private in law-enforcement. The on-going trend to increasingly privatise a number of functions previously carried out by law-enforcement agencies in the public sector is further blurring the lines as to who should have access to which data. Many European and non-European states have privatised a number of surveillance roles, whether in terms of CCTV or even using private security firms to provide other forms of on-site surveillance. Others have even launched public procurement exercises to privatise the building and running of what used to be police stations, leaving only "core police" activities to public officials sworn to protect the citizen as their primary duty.47 As the shrinking core is continuously debated, in data protection terms it becomes clear that the focus is upon what is being protected i.e. the citizen and his/her personal data rather than who is being actually trusted with providing the protection.

The growing avalanche of personal data generated in the 21st century far outstrips the ability of human beings to sift through it unaided and automated analysis is here to stay. Research carried outside the scope of the questionnaire analysis, such as that reported upon in the SMART, IRISS and RESPECT projects,48 suggests that the amount of human resources available within the budgetary constraints of law enforcement agencies is woefully inadequate to deal with the amount of personal data available for analysis; thus, in an exponentially increasing way, the amount of personal data that needs to be analysed in a timely manner will mean that this will increasingly need to be carried out in an automated way across national borders. This is increasingly happening and, at present, most often in an un-regulated manner.

The post-Snowden phenomenon: For some time before the revelations by Edward Snowden in June 2013, operators in the field of surveillance in cyberspace had often encountered problems caused by the blurring of the distinctions between cyber-crime, cyber-espionage and cyber-warfare. The extent of this problem became even more acute when the revelations by Snowden about PRISM, TEMPORA and similar programmes led to an increase in public awareness that the same personal data that is collected by what is most often a private commercial organisation for one purpose (eg Google, Facebook, Twitter, Chrome, Internet Explorer and several thousand web-sites) is open to scrutiny and potential abuse for a host of other purposes ranging from law enforcement carrying out surveillance for child pornography, organised crime, financial fraud, ID theft, and/or cybercriminals intent on carrying out one or more of the criminal activities sanctioned in the Cybercrime convention, and/or to intelligence and security agencies more

47 See Travis, Alan, and Zoe Williams. 2012. Revealed: government plans for police privatization West Midlands and Surrey police offer £1.5bn contract under which private firms may investigate crime and detain suspects. *The Guardian*. Accessed at http://www.theguardian.com/uk/2012/mar/02/police-privatisation-security-firms-crime

48 CONSENT, SMART, RESPECT and IRISS are EU-supported projects within the Seventh Framework Programme (FP7). Information from those projects is increasingly being put into the public domain through their respective websites: http://www.consent.law.muni.cz/; http://www.smartsurveillance.eu/; www.respectproject.eu; http://irissproject.eu/

bent on ferreting out potential terrorists or carrying out more traditional espionage activities. That the same personal data resident in the private sector lends itself to uses for or may be subject to surveillance for purposes as diverse as cyber-crime, cyber-espionage and cyber-warfare poses a new conundrum to data protection regimes predicated on a narrow definition of purpose or compatible purposes for processing. As will be seen later, regulation, especially about adequate safeguards and oversight mechanisms, would seem to be one of the many complementary ways for purpose-compatible activities or other purposes laid down by a law providing the necessary safeguards to be carried out in a manner which is more useful and acceptable to the international community.

Personal data, like physical persons and their behaviour in cyberspace, will increasingly lie outside the confines of European borders whether Council of Europe or European Union. This means that any new solution must perforce take into account the possibility of its acceptance and application in countries outside Europe. In other words a new solution may be European only in inspiration: its ownership, development and deployment must be international with as wide a take-up rate as possible within the realities of the international political situation.

The eight realities outlined above are realities in 2012-2013 but were not pressing realities in cold-war era, pre-Internet 1987 when post-war social democracy economics were pervasive and when R(87)15 came into being. They do however point to real requirements in a balanced approach to fundamental human rights secured in a society where vigilance by law enforcement and intelligence/security agencies is a reasonable expectation on the part of the citizen.

In a nutshell, in order to prevent and detect crime as well as investigate and prosecute it, a law enforcement agency (public or private) requires timely but measured access to personal data. Likewise, a security service or and intelligence agency (SIS) in its bid to prevent terrorism, protect national security or carry out espionage and counter-espionage. Often, but not always, delays in access will put human life, dignity, privacy and property at risk. For the access to be timely it often needs to dispense with ad hoc authorization and may need to rely on pre-authorisation, something which can only be properly provided for across borders by binding laws. The ever-increasing pressure for data analysis to be carried out across borders in an automated manner by definition also requires that this be carried out within the context of strict rules which provide appropriate safeguards for the protection of personal data. This access additionally calls into being the existence of oversight agencies with powers which transcend national jurisdictions. None of this is achievable without the right legal framework and neither the Council of Europe through R(87)15, nor the EU through its current regulations (CFD/977/JHA) or the contemplated new rules (draft EU Directive 2012), provide a legal framework which responds adequately to the realities outlined above.

On the basis of this (necessarily summary) analysis it is clear that it would be worse than useless to rely on the legal instruments currently in place or presently contemplated, as one would be relying on the illusion that the current and contemplated legal instruments provide an adequate response to the realities of 2012-2013 when they patently do not. They provide a basis for further and on-going development of the regulatory framework but not for reliance upon it in its present form.

The lessons from the findings outlined previously and specifically the first overall finding are that mere harmonization at a level of principles is only a starting point and in itself is not enough.[49] Indeed there would appear to be a rule of proportionality between automation and volumes of personal data processed and the level of detail and binding force of the legal instrument regulating the access to and the onward processing of such data: the higher the level of automation and the volume of personal data processed the more detailed and the more binding the legal rules should be. Put another way, for one jurisdiction to increasingly allow incursions into the personal data of its citizens by a national or transnational law enforcement agency especially in cases where that personal data is under the control of a data controller or processor in a third jurisdiction, it would require reassurance that that personal data is being treated, at minimum, with the same standards of care that are applicable in the first jurisdiction. The level of detail grows where there is an increasing reliance on pre-authorisation for search and the subsequent requirement for timely action for the arrest and investigation of the suspect in a manner where the evidence has been obtained through fair and lawful means which respect the data protection regimes applicable across the national boundaries involved in a case. Unless the safeguards are provided in a sufficiently detailed manner within a binding legal framework which provides a sufficient level of legal certainty as well as sanction and dispute resolution mechanisms, then the timely access to and exchange of personal data by law enforcement agencies across borders will remain a pipe-dream or a hopelessly and dangerously unregulated reality.

At least three possible options for the way forward

In "Council of Europe-speak" the clear functional requirement for the new legal regime to be binding takes it at least one level up from the current level of a non-binding legal instrument such as a Recommendation (which is the current status of R(87)15) to the level of a binding, multi-national treaty as a convention. It will be noted that the discussion above deliberately avoids mentioning whether a national boundary is a European or a non-European one since the way personal data flows is in a manner which does not care if the national boundary it crosses is European on non-European. Thus the binding legal instrument utilized must be one which is capable of attracting consensus and enforcement across borders.
In the context of personal data in the law enforcement sector the Council of Europe has a number of options open to it when considering possible avenues for future action:

a) It can launch the process to create an entirely new convention dedicated to regulating the access to and exchange of personal data for law enforcement purposes. This option was actually actively considered over twenty years ago. In Recommendation 1181

[49] A point which questions the fundamental logic of the current dual approach being undertaken in the EU's data protection reform package. For a more detailed treatment of this point see Cannataci, Joseph A. Defying the logic, forgetting the facts. In Proceedings of the SMART Policy Workshop, Florence, Italy, September 2012. In the European Journal of Law & Technology Vol. 4, No. 2, 2013 available at http://ejlt.org/article/view/284/390 Furthermore, as explained in further detail in the Epilogue of this report infra the revelations of the post-Snowden era appear to be met by the inability of the European Union to do much about part of the problem in the short term since national security is a matter reserved to national governments under Art 4 Section 2 of the Treaty of the European Union and has reportedly been successfully invoked in this sense by the governments of the United Kingdom and Sweden.

(1992)1 of the Parliamentary Assembly of the Council of Europe dealing with police co-operation and protection of personal data in the police sector it was agreed that

1. As a result of the Schengen Agreement, the European states co-operating in that agreement will proceed with the exchange of automatically processed personal data in the police sector. It is most likely that such an exchange will cover the whole of the European Community after the disappearance of frontier controls at its internal borders.
2. Nowadays there is already an intensive exchange of data in the police sector among Council of Europe member States on a bilateral or multilateral basis and through Interpol.
3. It is of vital importance for an efficient combat against international crime that it is fought at national and at European level.
4. An efficient fight against crime implies an exchange of data in the police sector.
5. In this respect it is useful to recall the Assembly's Recommendation 1044 (1986) on international crime and its plea for a European information and intelligence centre (Europol), and Recommendation No. R (87) 15 of the Committee of Ministers to member states of the Council of Europe regulating the use of personal data in the police sector.
6. It is necessary, however, that there be adequate protection of personal data in the police sector and one may note with satisfaction that the Council of Europe concluded, in 1981, a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. However, in order to be fully effective, it is not sufficient that this convention has, to date, only been ratified by eleven member states.
7. The Assembly therefore recommends that the Committee of Ministers :
i. draw up a convention enshrining the principles laid down in its Recommendation No. R (87) 15 ;

ii. promote the application of these principles in the exchange of data in the police sector between member States and between member States and third countries via Interpol. In this respect the implementation of the following principles is of the utmost importance :

a. data should be accurate, relevant, not exceed the purpose for which they are stored and, where necessary, kept up to date ;

b. they should be screened before they are stored ;

c. an individual should have the right to know whether personal data concerning him are kept ;

d. he should have an appropriate right of access to such data ;

e. he should have the right to challenge such data and, if necessary, have them rectified or erased ;

f. individuals who are denied access to files relating to them should have a right to appeal to an independent authority which has full access to all relevant files and which can and should weigh the conflicting interests involved ;

g. there should be an independent authority outside the police sector responsible for ensuring respect of the principles laid down in such a convention ;

iii. appeal to member States to ensure that data in the police sector may only be exchanged with other member States and with Interpol on the lines provided for in the proposed draft convention.

This Recommendation of the Parliamentary Assembly did lead to a regular review process for R(87)15 but it did not ever produce a new convention. The case for a binding legal instrument has been made above but the question arises: should it be a completely new instrument or should it seek to build on the level of international consensus already achieved? The alternative approaches to such a route are the focus of options (b) and (c) below. The advantages of a stand-alone convention would be three-fold: a) the starting of a fresh debate on a clean slate, with as many leading players as possible, taking into consideration all that has been learned thanks to R(87)15 and focusing on a discussion led by an adequate understanding of functional specifications and requirements which would then need to be encased in legally binding

provisions and b) it would be able to capture the required level of detail which is required for the objectives to be attained. Suffice it to say that the INTERPOL Rules on the Processing of Data (RPD) run to 135 provisions across 52 pages of rather small print and it is our considered opinion that, for it to be truly useful to its main users and especially law enforcement agencies, the successor of R(87)15 would possibly need to be even more detailed and comprehensive than the INTERPOL RPD; c) It would permit a realistic "joined-up" approach to privacy and data protection examining the access to and surveillance of on-line and off-line activity by citizens irrespective of whether the information exchange, surveillance, lawful interception or monitoring is carried out by a law enforcement agency or a security and intelligence service.

A second non-exclusive option is to create an additional protocol to Convention 108 or otherwise work the provisions of what would be an independent stand-alone convention into the main body of the text of Convention 108 which is currently entering into a "modernisation" phase. While this would have the advantage of building upon the undoubted international consensus that exists around the principles of Convention 108 it would have the disadvantage of discouraging the detractors of Convention 108 and especially of complications of form. Integrating the new binding rules into the main text would be unwieldy because of the level of detail required, while the size of the additional protocol envisaged, although legally and notionally viable, would beg the question "Why have it as a protocol when it is more than sizable enough to have as a separate convention?" (which would additionally have the advantage of having new players around the table sitting at par with established ones, always to the level possible within Council of Europe "house-rules"). That being said, Convention 108 has, after the European Convention on Human Rights, been one of the Council of Europe's success stories; it has inspired the development of the EU's entire data protection regime and is designed to be open to signature to countries outside Europe so it certainly meets functional requirements on that score.

A third non-exclusive option would be to create an additional protocol to Convention 185, the Cybercrime Convention. Although 20 years younger than Convention 108, the Cybercrime Convention can be considered to be another of the Council of Europe's success stories and its ratification by countries like the United States adds further to its wide appeal. An additional protocol to Convention 185 would also have pros and cons. It would provide a useful framework for signatories to that Convention enabling them to meet functional requirements in the efforts to combat cybercrime in a measured way which respects the fundamental rights of citizens to private and family life. As in the case of Convention 108, the sheer physical bulk of the additional protocol might discourage some, but notionally there is nothing which would preclude a quasi-identical Additional Protocol being bolted onto either or both Convention 108 and Convention 185. If this route were to be followed however it should be noted that Convention 185 to date deals exclusively with the law enforcement sector and is not intended to cover the activities of security and intelligence agencies operating in the area of national security.

As part of the outcome of the findings of the report and on the basis of the new evidence now available it is our clear recommendation to the Council of Europe that an Ad Hoc Drafting Committee be set up, containing representatives of both the T-PD and the T-CY. This Ad Hoc

Committee would be tasked with terms of reference which would seek to determine which one or more of the three options identified above would be most appropriate and timely for the Council of Europe to follow under the circumstances. Once the relative decisions are approved by the T-PD and the T-CY and the Committee of Ministers, then the same drafting group would go on to the task of the actual drafting of the new binding instrument, whether an entirely new Convention or one or more additional Protocols.

A second task of the Ad Hoc Drafting Committee would conceivably be to examine new draft Guidelines being produced outside the Council of Europe50 and examine the extent to which these could be adopted or adapted to supplement any new binding rules developed by the Ad Hoc Drafting Group.

New provisions on private sector data in the new binding instrument

Any new binding instrument would naturally take into account the thirty one provision-specific findings outlined above and attempt to significantly improve upon the current position. There are however a number of areas which are not adequately covered by R(87)15 and which therefore are not prominently highlighted in the thirty-one findings in question. While an exhaustive consideration of these issues would fall to the Ad Hoc Drafting Group proposed above, it is opportune to bring to the attention of the Council of Europe the glaring issue of access to and onward use of data collected and processed in the private sector.
Purpose, or finalité in its French incarnation, is the principle on which much of European data protection law is predicated, whereby the collection and onward processing of personal data is only permissible if it is for the legitimate and specified purpose of its collection or, at minimum, a compatible purpose. This aspect of the present study deals with what has probably been one of the greatest changes in the realities of data protection law in the area of police use of personal data since the inception of R(87)15.

To better understand these developments and reflections it is useful to go back 26-28 years to the period of 1984-1986 when R(87)15 was being drafted and to examine the final results of the deliberations of the Council of Europe's Project Group on Data Protection (the Committee of Experts on Data Protection subsequently became the Project Group on Data Protection (CJ-PD) in 1978.). As explained in further detail in the background material annexed to other reports51 prepared by the present consultant, one of the great innovations of R(87)15 is that it introduced the notion of purpose fairly and squarely into the sector of police use of personal data. Hitherto, the period 1981-1987 may be considered to be "the limbo years" for police use of personal data since many European police, security and law enforcement agencies interpreted Convention 108 as providing a blanket exception from the purpose provisions of data protection law. So, although Art. 5 of Convention 108 provides that "Personal data undergoing automatic

50 At least three such documents come to mind here and specifically those being produced by the SMART, IRISS, SURVEILLE and RESPECT projects funded by the EC FP7.

51 Cannataci, Joseph A. 2013. Concept paper on the application of data protection regulations in relation to transborder private/public information sharing for (a) network security purposes and (b) criminal justice purposes. paper commissioned by the Council of Europe produced in two versions December 2012 and September 2013 available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/presentations/default_en.asp .

processing shall be: obtained and processed fairly and lawfully;" and "stored for specified and legitimate purposes and not used in a way incompatible with those purposes", in practice law enforcement agencies relied heavily on the provisions of Art. 9.2 of Convention 108 which states that derogations from Art. 5, 6 and 7 "shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences". At that time (some would say even now) there was little if any evidence of many police forces around Europe being allergic to collecting and processing personal data "just in case it comes in handy" without any specific reason or clear specific purpose.

The deliberations of the CJ-PD were finally encapsulated in R(87)15 and firstly through an innovation in the definitions section of that seminal Recommendation: "The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order." This definition therefore puts meat on the skeleton provided by Articles 5 and 9 of Convention 108 and was then further supplemented by the provisions of R(87)15's Article 2 where one reads:

> "2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation."

This provision was the result of a two-year long debate within the CJ-PD and, in legal jargon, may also be interpreted as a "for the avoidance of doubt" provision." Building upon the words of Art 9 of Convention 108 and specifically "a necessary measure" and "is provided for by law" it laid down the principle that the police are no exception to the principle of purpose and that collection of personal data is limited to that which is strictly necessary "for the prevention of a real danger or the subject of specific criminal offence", thus placing firmly out of bounds the collection of personal data "just in case it comes in handy". Much to the chagrin of some national delegations (and notably those of Ireland and the UK which, respectively, entered a general reservation and reservations to Arts 2.2 and 2.4 of R(87)15), this Recommendation left no doubt that legislative intervention was and remains required. If any European legislator wishes to exempt a police force from the obligation to collect only that personal data which is necessary for the prevention of a real danger and the suppression of a specific criminal offence, then he or she must take the trouble to reflect properly, indulge in an open and proper debate as a prerequisite to legislating specifically on the matter. When faced with the practical and political consequences of making such a choice, many politicians and law-makers often shy away from making any laws which may draw adverse public reaction on account of their being perceived as giving powers to the police which may be considered to be too intrusive.

This then was the context for R(87)15 at a time when the cold war was not yet over and the spectre of a state-sponsored Big Brother was still very much at the root of the reasoning behind this then-new legal instrument. Times have changed however. Originally (e.g. in 1984-1987 at the time of drafting of R(87)15) personal data used by the police was largely if not almost

exclusively data collected “for police purposes”. In 2012-2013, there has been a shift to a position where police increasingly access data originally collected not by themselves but by other public agencies or very often a private entity (e.g. airline, bank, insurance company, transport company as in metro, bus, train, tram, taxi, etc.). This is a paradigm shift for police use of personal data. A law enforcement agency is today sometimes less concerned with the use of personal data that it itself collects for police purposes but rather is very interested in the personal data collected by third parties in the private sector - it should be said at the expense of the private sector – and which is normally collected for other purposes, i.e. not for police purposes as defined by R(87)15. The situation envisaged in the scenario of another report commissioned by the Council of Europe is that of personal data collected in the private sector and then transmitted within the private sector or to law enforcement agencies, locally or across national boundaries.52 This was not the primary preoccupation of the authors of R(87)15 when dealing with communication of personal data when in Section 5.4 it is provided that “Communication of data to foreign authorities should be restricted to police bodies. It should only be permissible:

a. if there exists a clear legal provision under national or international law,

b. in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law, and provided that domestic regulations for the protection of the person are not prejudiced.”

This provision on international communication should be read together with Art 5.3.i. of R(87)15. This states that the “communication of data to private parties should only be permissible if, in a particular case, there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority.” This provision is in turn complemented by Art 5.3.ii. which stipulates that “Communication to private parties is exceptionally permissible if, in a particular case: a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if b. the communication is necessary so as to prevent a serious and imminent danger.”

The authors of R(87)15 had contemplated file-matching and on-line access as may be seen in provisions of Art 5.6.: “The interconnection of files with files held for different purposes is subject to either of the following conditions:

a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or

b. in compliance with a clear legal provision.

Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation which should take account of Principles 3 to 6 of this recommendation.”

[52] Ibid.

So while Principle 5 - Communication of data - is one of the longest sections of R(87)15, there one only finds provisions almost exclusively written with the communication of data collected by the police in mind. This is clear from the opening paragraphs on the scope of this Recommendation "The principles contained in this Recommendation apply to the collection, storage, use and communication of personal data for police purposes which are the subject of automatic processing" which should in turn be read together with the definition of police purposes outlined earlier. In summary the most important European legal instrument dealing with data protection in the law enforcement sector regulates communication of data collected for police purposes to other police bodies and to private parties but, significantly, i) not from private parties to the police and not ii. between private parties, which, in default of anything specific laid down by R(87)15, must then presumably fall under the general tenets of data protection law. This consideration therefore takes one back to the principles of Convention 108 and specifically to its Art. 12 which provides that:

> 1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
>
> 2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.
>
> 3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
>
> insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
>
> when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

The logic of the Convention and its drafters was the creation of a common European area where the same minimum standards of data protection applied equally regardless of geographic location and therefore the mere fact that personal data crosses a national boundary does not warrant the introduction of any additional safeguards or the creation of obstacles to such transborder data flow provided that the data flow is between parties to Convention 108.

These issues of the problems raised by private sector-created/held data are dealt with in considerably more detail in a separate report entitled "Concept paper on the application of data protection regulations in relation to transborder private/public information sharing for (a) network security purposes and (b) criminal justice purposes" prepared by the Consultant for the Council of Europe in December 2012. 53The findings in that report should not be taken to be the final word on the matter but rather as an illustration of parts of the problem which would need to be dealt with by the Ad Hoc Drafting Group when considering a host of issues in a holistic manner.

[53] Ibid.

In the area of law enforcement and personal data, perhaps even more than in other areas, the devil is in the detail.

Epilogue for the post-Snowden era

Most of this report and its recommendations were researched and written well before the revelations made about PRISM and similar programmes by Edward Snowden throughout the months since May 2013. It will be noted however that the bulk of the personal data that Snowden confirmed is being regularly processed by the NSA and GCHQ - to name but two of the intelligence agencies involved - is data collected and processed in the course of transactions by private citizens with other private citizens and/or commercial corporations in on-line media owned and operated by the private sector. A careful consideration of the implications of these revelations has not caused the authors of this report to change their recommendations. On the contrary the post-Snowden era is one which prompts us to reinforce the value of the recommendations and emphasise the unique position of the Council of Europe to take action in this sector.

The issues for privacy and data protection of European citizens posed by programmes such as PRISM, TEMPORA and X-Keyscore have been dealt with in some detail elsewhere and most recently in a briefing note to the European Commission's Directorate General for Internal Policies.54 Such studies should be read together, but not confused, with ongoing debates over the value of personal data processed "for police purposes" under the 2006 Data Retention Directive where the latest evidence made available in the public domain55 is not as complete or as clear as one would wish. As one looks at all the various ways in which personal data is processed for use by LEAs and security agencies one should remember that beyond PRISM and TEMPORA the personal data of European citizens is also being captured en masse in 28 of the 47 member States of the Council of Europe as a result of the EU's 2006 Data Retention Directive (DRD). There can be little doubt that the European Commission is trying its best to put together the available evidence on the basis of statistics provided by member States but it is careful to make no claims as to the conclusions that could be drawn from statements like "It appears that there are over two million requests per year for retained data, equivalent to about two requests for every police officer in the EU or 11 requests for every 100 recorded crimes". Indeed when it comments on the quantitative data at its disposal it warns that "it would not be possible to identify meaningful statistical trends only a few years after the DRD entered into force."

Some qualitative data recently published is however very valuable: thanks to the European Commission's latest report we obtain an insight into the way data retention proved useful or how its absence proved to be a hindrance. Summaries have been made available for five (5) cases

54 Bowden, Caspar. The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights. A briefing note prepared for Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs. Accessed at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

55 See report: Evidence for necessity of data retention in the EU. Accessed at http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf

in the category of terrorism, twenty-one (21) cases of murder and manslaughter, eleven (11) cases of Serious sexual offences and child abuse, nine (9) cases of Buying or offering online child pornography, six (6) cases of Drugs trafficking, six (6) cases of armed robbery, twenty-four (24) cases of burglary, theft and organised trafficking, five (5) cases of cybercrime and six (6) cases of fraud. These latest revelations in a report released after March 2013 will doubtless fuel the debate further. With the member states apparently unable to report a total of more than ninety-three (93) documented cases over what appears to be a period of some seven years since the Directive came into force on 03 May 2006, legitimate questions on the proportionality and cost-effectiveness of the DRD will doubtless be raised over the coming months and years.

Yet citizens concerned with their privacy and data protection can take some solace that access to their personal data collected and processed under the DRD at least requires a court order. That is a conventionally strong safeguard which is most often conspicuously missing in cases where their personal data being collected under PRISM, TEMPORA et al. Under TEMPORA we are presented with the case of an intelligence agency based in the EU (GCHQ of the UK) which is going far beyond mere metadata but which in the first instance for a period of at least three days records contents of e-mail and telephone calls and traces of web searches and on-line activity on a previously unimaginable scale. How do these activities sit in the context of Convention 108?

A few reminders of what Convention 108 actually stipulates would appear to be useful at this stage:

In Article 1 we find that, unlike FISA in the United States, the European Data Protection Convention does not makes any distinction based on nationality or residence but specifies that "The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")".

After laying out the now "standard" safeguards in Articles 5 – 8, it is in Article 9 of Convention 108 that we find important provisions that apply to both LEAs and SIS. Firstly we find the exception:

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.
2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:
    a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
    b. protecting the data subject or the rights and freedoms of others.

The key safeguards laid out in Article 9 are that the derogation must be provided for by law and is proportional. Indeed some would argue that the test set by the Convention is higher than mere proportionality: a measure must be necessary. "Must have" rather than "nice to have". If

one were to use TEMPORA as a case study, does it meet the requirements of "provided for by law" and absolutely "must have"?

The most recent debates in the UK media and analysis of English law such as RIPA[56] would suggest that there is some element of wide generic legal provision but the jury is still out on whether this is unreasonably wide[57] and generic, or whether the currently applicable oversight mechanisms in the UK are up to the task of providing adequate measures of protection from unwarranted intrusion into citizen privacy. Even the Chairman of the UK Parliament's Intelligence & Security Committee has most recently gone on record to admit that

> There are real issues that do arise out of the Snowden affair, in Britain as elsewhere. Even if the intelligence agencies always act within the law, it must be right for that law to be reviewed from time to time to see whether the safeguards are adequate. Sometimes they are not. The intelligence and security committee criticised the government's original proposals for closed proceedings in civil actions as being wider than was necessary. We have criticised some of the provisions in the proposed Communications Data Bill.
>
> There has also been a crucial need for greater powers for the committee. That has now been conceded by the government. As of this autumn, the intelligence agencies can no longer refuse it any information it seeks. We now have the statutory power to investigate MI6, MI5 and GCHQ operations, which we did not have in the past. Our budget is being almost doubled to £1.3m and our staff are being greatly strengthened.[58]

These comments by Malcolm Rifkind actually go to the heart of the matter: it is not that the law may not exist but rather is it still adequate for the current situation and are the means of oversight and resources allocated for enforcement appropriate? It is clear that what is actually required in Europe, at the level of the Council of Europe and elsewhere, is a healthy open debate about the adequacy of existing safeguards, necessity and proportionality of current practices, best practices, resources, structures and procedures of oversight mechanisms.

For the research within the PUPIE project as referred to previously suggests that Security Services across Europe are not always dealt with in comparable terms and that their access to and use of personal data would benefit greatly from a significant level of harmonisation. Indeed, earlier on it was noted that "There is limited agreement on the meaning of 'state security', as it depends on national policies (at national level, the use/application of the phrase 'national security' or 'state security' may be confusing). The majority of countries surveyed applied data protection rules to data processed for state security purposes, while two countries reported such activity is regulated by a specific, separate data protection law."[59] What then would be the legal instrument capable of most rapidly delivering such harmonisation? An EU Directive/Regulation

---

56 Regulation of Investigatory Powers Act 2000, UK.

57 An almost incredibly wide power available under UK law is to be found within Section 7 of the Intelligence Services Act whereby the Minister can effectively authorise GCHQ to break UK law in relation to anything appearing to originate from [overseas] apparatus. The precise text is 1") If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section" last accessed on 24 September 2013 at http://www.legislation.gov.uk/ukpga/1994/13/section/7

58 Rifkind, Malcolm. 2013. What rubbish, Sir Simon! Our intelligence agencies are not outside the law. The Guardian. Accessed at http://www.theguardian.com/commentisfree/2013/sep/20/rubbish-sir-simon-intellignence-snowden

59 Previously indicated at page. 11 supra.

baked in Brussels or a binding legal instrument produced in Strasbourg within the wider ambit of the 47-member state Council of Europe?

The fact that some member States of the Council of Europe have reported that data collected for state security purposes is subjected to data protection rules in terms of Convention 108 does not mean that the same standards of protection are achieved or that these standards are high enough. The extent to which oversight mechanisms may lack adequacy and may not be working at comparable levels is also highlighted by the most recent statements of the German Federal Data Protection Commissioner Peter Schaar. On the same day of September 2013 when Malcolm Rifkind was publicly taking critics to task in the UK media as to the level of legal protection actual existing in the UK, one finds the German media reporting that "Since whistleblower Edward Snowden revealed the methods of the US intelligence gathering service, NSA, Schaar says he has felt let down by the German government. He says he cannot assess the role played by the German intelligence services in the scandal because the German interior ministry says it is not his jurisdiction."[60] He went on to say that "a lack of transparency in public authorities' activities could lead to a loss of trust in democracy itself".[61]

This issue of transparency is also clearly not a major source of concern within Europe alone. The US President's reaction to the torrent of public concern unleashed by Snowden's revelations was to announce a number of initiatives aimed at bolstering transparency: "It's not enough for me as president to have confidence in these programs," Obama declared at a White House news conference. "The American people have to have confidence as well."

Among other things, Obama called for the creation of an outside task force to advise his administration on how to balance civil liberties and security issues. He also said he had directed the intelligence community to make public as much information about the spying programs as possible and directed the NSA to create a website that would be a "hub" for that information. "These steps are designed to make sure the American people can trust that our interests are aligned with our values," Obama said."[62]

When striving towards greater transparency and contemplating new mechanisms aimed at advising on how better to achieve a balance between security and civil liberties such as privacy the US administration would appear to be moving in directions which would be very much aligned with the current political mood in much of Europe. Likewise, it would be very surprising if the values of US citizens would not align themselves with those of EU citizens. Reference should here be made to the findings of *inter alia* the CONSENT and SMART Research projects about the perceptions of citizens and their attitudes to privacy and surveillance. In SMART emerging results[63] from research carried out in a number of EU Member States suggest that

---

60 Fürstenau, Marcel. "Transparency lacking, says top data watchdog", Deutsche Welle, 21 Sep 2013 last accessed on 24 Sep 2013 at http://www.dw.de/transparency-lacking-says-top-data-watchdog/a-17104023

61 Ibid.

62 Bailey, Holly. 2013. Obama speaks out on Snowden, calls for greater transparency on surveillance. Yahoo News. Accessed at http://news.yahoo.com/obama-to-hold-white-house-news-conference-164610288.html

63 Brockdorff, Noellie, Sandra Appleby Arnold, Christine Garzia et al. European citizens' perspective of smart dataveillance: preliminary results from Work Package 10 of the SMART project. Presented at Intelligent Investigation Policy Workshop

European citizens are very unhappy about integrated large-scale dataveillance and especially being unconsciously "spied upon"[64] by either the state or private companies. Forthcoming research[65] may help establish more precisely as to whether citizens actually care as to whether they are being spied upon by their own state or by a foreign state but one would not be surprised if most citizens would turn out to be upset either way if they feel that their privacy is being infringed upon in a disproportionate and unnecessary manner.

In all of the three examples cited above, the UK, Germany and the USA there is clearly a call for action with varying degrees of satisfaction with the current national levels of adequacy of safeguards, oversight and resources available for enforcement. If gauged by reactions in the media or public statements from data protection authorities and some politicians it would be fair to say that the situation and mood across most European states in September 2013 is not dissimilar to that in these three prominent members of the G20. So, the question naturally arises, would it be helpful and possible for joint action at the international level to develop a satisfactory way forward? Within a European context, to continue reflecting on the opportunity afforded to us by the UK case study in TEMPORA, there may be areas where the other 46 member States of the Council of Europe may stand to learn quite a few things from the UK's experience and vice-versa. It would not be unreasonable to assume that the development of a set of legally-enforceable – and enforced – safeguards, oversight mechanisms and resourcing levels common to all European states would also improve the international collaboration to fight crime and terrorism which is increasingly required in the Internet era.

This goal remains difficult to achieve but is not beyond the realms of the imagination. Long years of mutual mistrust will need to be overcome but the alternatives - technical counter-measures at national and regional levels, parallel internets, refusal to collaborate or exchange information, boycott of whole swathes of existing fibre-optic cables and cloud service providers – could prove to be a far more damaging prospect than a common European or indeed international approach to data protection in the case of security and intelligence services. Of course the debate will continue to be muddled further by the complications induced by espionage for economic reasons or cyber-warfare but this is no reason to avoid having a calm, well-reasoned Europe-wide discussion on improving the currently available set of safeguards.

The European discussion would only be a start for many other states outside Europe, not least long-standing allies like the United States, Canada, Australia and New Zealand, not to mention a whole host of emerging and established economies would doubtless be keener to adopt comparable and compatible measures rather than go for alternatives which might involve the "balkanisation" of the internet, perennial economic espionage and cyber-warfare.

---

conference http://www.iri.uni-hannover.de/programme.html on 19 September, 2013, Brussels. Final report to be put into the public domain in 2014.

64 See Deliverable D10. in the SMART project. In these findings citizens are actually more upset if the "surveillance" is carried out by private companies than by the state. To be made available on-line at www.smartsurveillance.eu by May 2014.

65 E.g. in WP12 of the RESPECT project http://respectproject.eu/

These considerations should be made against some stark legal realities. The Council of Europe, within its Data Protection Convention and/or within the Cybercrime Convention has both the legal framework and the credibility to explore the development of a tripod of measures aimed at achieving the balance between privacy and security or crime detection and prevention:

1. Adequate legal safeguards;

2. Meaningful Oversight Mechanisms;

3. Sufficient resources for effective enforcement.

An additional protocol to either Convention or possibly an entirely new Convention – i.e. one or more of the three options outlined in the Recommendations made above – may be a viable way forward in the current political climate.

Such a way forward for the 47 member States of the Council of Europe would meet the triple imperatives of a) the modernisation of R(87)15, b) the modernisation of Convention 108 and c) a proportionate reaction to the public outcry following the Snowden revelations. It would not be incompatible with the options open to the member States of the Council of Europe who also happen to be EU Member States. The latter group of 28 are at present faced with a number of procedural difficulties and political uncertainties should they wish to go it alone in the immediate future. The type of surveillance carried out in those sectors revealed by Snowden crosses over between strictly LEA areas of competence such as serious organised crime and into national security, an area which in terms of Article 4 Section 2 of the Treaty of the European Union falls outside the scope of EU law: "In particular, national security remains the sole responsibility of each Member State."[66].

It is reported personally to the authors by reliable sources who must at the time of writing remain unnamed that this provision has already been utilised by the UK and Sweden to block some level of formal action at EU level over the Snowden affair. This in spite of the fact that a special ad hoc working group including the data protection commissioners from Austria and Slovenia[67] has been appointed with a mandate "to clarify the actual state of activities of the US National Security Agency (NSA) in relation to the alleged collection of information and personal data on EU citizens".[68] There is not much transparency or information forthcoming about the results of joint EU-USA negotiations on this matter at this stage: "The group is not allowed to make any public statements before the end of the mandate, when a report needs to be submitted to the European Commission"[69] Other reports held that: "The EU members of the group will report to

---

66 Art 4 Section 2, Consolidated version of the Treaty on European Union, Official Journal of the European Union.

67 The Information Commissioner Nataša Pirc Musar has been appointed member of a special ad hoc working group EU – USA. Accessed at https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1182&cHash=a8790b0646e9527bd35eb55e1a2f052f

68 Ibid.

69 Ibid. The UK delegation to the T-PD commented thus on this quotation from the cited sources: "We do not consider that this text accurately reflects the agreed remit of the ad hoc EU-US working group. It is therefore absolutely vital that this is factually correct. As set out in the Lithuanian Council of the EU Presidency's statement of 19 July, the ad hoc EU-US working group was established to consider data protection in relation to the personal data of EU citizens, and specifically the group is "tasked with discussing questions of data protection". A link to the Presidency statement is

Member States' ambassadors to the EU in October. Their conclusions will be shared with the EEAS, the European Commission, and the Council's secretariat, but, officials said, it is not clear if the institutions will receive the report itself. No official was able to say if any of the conclusions would be shared with the public.[70] A national diplomat said that the Member States were showing little enthusiasm for pursuing their inquiries at the EU level."[71] Thus, while there has been considerable noise made about the Snowden revelations in the European Parliament,[72] especially during September 2013,[73] it is unlikely that the Council of Ministers would move away from a position where at least one national EU Government, possibly more, are opposed to concerted action at EU level. The agenda for the European Council scheduled for 25 Ocotber 2013 and published on 23 September 2013 makes no specific mention of any discussion of reports resulting from the Snowden allegations though this can possibly be included under the

---

below. http://www.eu2013.lt/en/news/statements/presidency-statement-on-outcome-of-discussions-on-euus-working-group " Authors' Note: The Presidency statement may well be the formal wording agreed to on the 18th July 2013 in Brussels but in no way has any evidence been advanced by the UK or any other delegation to the T-PD that the reporting reproduced in the main text above and cited as source-indicated in footnotes 66-68 is inaccurate. The evidence available to the authors from other sources as well as the actual contents of the report corroborates many of the impressions given in the report cited above.

[70] Authors' up-date note entered 18 Feb 2014: The Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection dated 27 November 2013 was actually made public and is available as a pdf document on-line. Its main findings are damning insofar as the position that EU citizens may find themselves in with regard to data gathered about them by the US intelligence agencies. In Section 5 at page 17 one reads
"(2) There are differences in the safeguards applicable to EU data subjects compared to US data subjects, namely:
i. Collection of data pertaining to US persons is, in principle, not authorised under Section 702. Where it is authorised, data of US persons is considered to be "foreign intelligence" only if necessary to the specified purpose. This necessity requirement does not apply to data of EU citizens which is considered to be "foreign intelligence" if it relates to the purposes pursued. This results in lower threshold being applied for the collection of personal data of EU citizens.
ii. The targeting and minimisation procedures approved by FISC under Section 702 are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons. These procedures do not impose specific requirements or restrictions with regard to the collection, processing or retention of personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. Oversight of the surveillance programmes aims primarily at protecting US persons.
iii. Under both Section 215 and Section 702, US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the US.
(3) Moreover, under US surveillance programmes, different levels of data protection safeguards apply to different types of data (meta-data vs. content data) and different stages of data processing (initial acquisition vs. further processing/analysis).
(4) A lack of clarity remains as to the use of other available legal bases, the existence of other surveillance programmes as well as limitative conditions applicable to these programmes. This is especially relevant regarding Executive Order 12333.
(5) Since the orders of the FISC are classified and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues, judicial or administrative, for either EU or US data subjects to be informed of whether their personal data is being collected or further processed. There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress."

[71] Gardner, Andrew. 2013. EU and US to discuss snooping allegations. The European Voice. Accessed at http://www.europeanvoice.com/article/imported/eu-and-us-to-discuss-snooping-allegations/77956.aspx

[72] Schmitz, Gregor-Peter. 2013. EU Parliament Furious about NSA Bank Spying. Der Spiegel. Accessed at http://www.spiegel.de/international/europe/nsa-spying-european-parliamentarians-call-for-swift-suspension-a-922920-druck.html

[73] Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm. Der Spiegel 20 September 2013. Accessed at http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

standard catch-all “The European Council may also address specific external relations issues in the light of developments on the international scene.”[74]

Would the same apparent lack of enthusiasm remain evident at Council of Ministers level in the period October – December 2013? Would the wider ambit and track-record of the Council of Europe provide an environment where the lack of enthusiasm of one or even a handful of national governments would not prevent the creation of an impetus which would result in new legally enforceable safeguards? Would an overwhelming majority in say the T-PD leave a tiny minority – or even a minority of one – quite hopelessly isolated in their opposition to concerted European and eventually international action? These are some of the questions which remain outstanding at the time of finalisation of this version of this report.

It should be noted too that matters for the EU States are not helped by the uncertainty that hangs over the fate of the draft Directive[75] aiming at data protection in the criminal justice sector. While some data protection experts welcome the draft Directive as a step forward in terms of EU law where it represents an improvement over the currently applicable EU law CFD/977/JHA/2008, at the time of writing it is uncertain whether it will be adopted at all before the EU parliament is dissolved in May 2014 or which is the precise form it would go through in.

In real terms however its adoption, or lack of it, would have little real impact for European citizens. Firstly, as demonstrated by the results of the research in this PUPIE project, most of the provisions contemplated in this Directive have already in point of fact been transposed into national law across Europe thanks to the impact of R(87)15. Secondly, even if the current or a revised draft of the proposed European Directive were ever to see the light of day, it would not adequately address the data protection implications raised by Snowden, since there can be little doubt that the exclusion of competence of EU institutions and EU law in matters of national security in terms of Art 4 Section 2 of the EU Treaty would be successfully invoked by one or more EU Member States. This lack of legal competence is an obstacle to EU action but it does not prima facie exist within the context of the Council of Europe. As indicated in the section on recommendations above, the Council of Europe may have at least one or more out of at least three possible options to choose from. Each of these will present pros and cons to any Ad Hoc Drafting Committee entrusted with drawing up a suitable new legal instrument. However the furore created by Snowden has led to an increase in public awareness which may present a favourable climate for new safeguards, oversight mechanisms and resourcing levels to be legislated into being.

---

74 European Council (24-25 October 2013) – Annotated draft agenda – Doc 12389/13. Accessed at http://www.european-council.europa.eu/council-meetings/documents-submitted-to-the-european-council?lang=en

75 European Commission’s proposal 25.1.2012 COM(2012) 10 final 2012/0010 (COD) for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf

Annex A: Text of questionnaire

The protection of personal data is one of the priorities of the Council of Europe. The Council of Europe is currently engaged in an important exercise aimed at revising legal instruments which form part of the protective framework intended to provide safeguards for European citizens. One of the key areas where the Council of Europe is up-dating its legal framework aims at achieving the right balance between privacy and the legitimate, proportional use of personal data for police purposes. This questionnaire is an important tool which member states are very strongly encouraged to complete in order to provide the basis for evidence-based policy decisions during the near future.

This document is part of research carried out on behalf of the Consultative Committee of the Convention for the protection of individuals with regard to the automatic processing of personal data (T-PD) facilitated by the Secretariat of the T-PD within the Division for information Society, Media and Data Protection, Directorate General of Human Rights and Legal Affairs of the Council of Europe.

Ms Sophie Kwasny, T-PD Secretary

Professor Joseph A. Cannataci and Dr. Mireille M. Caruana

This research is also supported by:

Completed questionnaires should be returned to: lwxmc@bristol.ac.uk, cc.ed to: joseph.cannataci@um.edu.mt and data.protection@coe.int

Processing of Personal Data in the Criminal Justice sector – Questionnaire

This study is designed to trace the historical development, and current status, of different legislation regulating the use of personal data in the police and criminal justice sector in the Member States of the Council of Europe. The main aim is to assess the extent to which Recommendation R(87)15 aiming for the regulation of the use of personal data in the police sector of the Council of Europe has been implemented across Europe.

Answering this questionnaire is not compulsory. However, your input into this process will greatly assist the Council of Europe, the European Commission, academic researchers and policy makers in obtaining a clearer picture of the current status of data protection in the police sector. Your response will be completely confidential unless you tick the box below which indicates that you agree to be cited or named in an individual capacity.[76]

I agree that my name and affiliation may be cited in outputs of the Study including reports and publications. ☐

In order to assist you in your response, at the end of every question, the Principle of the Recommendation[77] being referred to and, if appropriate, the relevant paragraph of the Explanatory Memorandum, are indicated in brackets.

Please attach to this questionnaire the original version, as well as a translation in English or in French, of the relevant laws of your country.

When answering the questions please include a precise reference, using Article and page number, to the text that you attach and preferably you may wish to cut and paste the relevant sections in to the space provided.

Note: If you can't answer a question, please move on to the next one.

[76] For the purposes of the Data Protection Act 1998 of the United Kingdom and the Data Protection Act 2001 of Malta, this data will be retained in a secure, confidential format by the Directorate General of Human Rights and Legal Affairs of the Council of Europe, as well as by Professor Joseph A. Cannataci and Dr Mireille M. Caruana who will be identified as controllers of the files in terms of the respective laws.

[77] https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=608011&SecMode=1&DocId=694270&Usage=2

Respondent's Information

Last name: Click here to enter text. First name: Click here to enter text.

Email address: Click here to enter text.

Tel no: Click here to enter text.

Responding Institution: Click here to enter text.

Address: Click here to enter text.

Position held within institution: Click here to enter text.

Date:

Part 1 – Overview	Implementing law & section
Q.1 Which pieces of legislation, or other regulatory measures, govern the use of personal data by police and/or security agencies in your country? Please provide the title of the legislation/measure, its reference number, date of enactment and the date it came into effect.	
Click here to enter text.	Click here to enter text.

Q.2 [For Schengen countries] Following the Treaty of Amsterdam of 1997 your country agreed to implement, partially or wholly,[78] CoE Recommendation R(87)15 on Regulating the Use of Personal Data in the Police Sector. What is the title of the Act or other regulatory measure that ensures that your country is in compliance with this part of the *acquis communautaire*? Please provide the title of the legislation/measure, its reference number, date of enactment and the date it came into effect.	
Click here to enter text.	Click here to enter text.

Q.3 [For non-Schengen countries] As a non-Schengen state, implementation of that part of the *acquis communautaire* which includes Recommendation R(87)15 is not obligatory on your country. Has your country however, directly or indirectly, passed an Act or other regulatory measure that implements Recommendation R(87)15? If so, please describe the title of any legislation/measure, its reference number, date of enactment and the date it came into effect.	
Click here to enter text.	Click here to enter text.

[78] There is some debate as to the interpretation of the Schengen Agreement, especially in so far as participating states may be expected to implement Recommendation R87(15) *in toto* or only to specific instances of police use of personal data.

Part 2 – Detailed provisions Scope and definitions	Implementing law & section

Q.4 How does the law of your country define personal data “for police purposes”? (R87(15) ‘Scope and definitions’; Explanatory Memorandum para. 22)	
Click here to enter text.	Click here to enter text.

Q.5 Who in your country is the “responsible body” (authority, service or other public body) which is competent under national law to decide on the purpose of an automated file, the categories of personal data which must be stored and the operations which are to be applied to them (i.e. the controller of the police files)? (R(87)15 ‘Scope and definitions’; Explanatory Memorandum para. 25)	
Click here to enter text.	Click here to enter text.

Q.6 Has your country extended the principles contained in Recommendation R(87)15 to personal data undergoing manual processing? (R(87)15 ‘Scope and definitions’; Explanatory Memorandum para. 26–27)	
Click here to enter text.	Click here to enter text.
Q.7 If not, what, if any, manual processing of data is likely to take, place? What is the aim of such processing? (R(87)15 ‘Scope and definitions’; Explanatory Memorandum para. 26–27)	
Click here to enter text.	Click here to enter text.

Q.8 Has your country extended the principles contained in Recommendation R(87)15 to data relating to groups of persons, associations, foundations, companies, corporations or any other body consisting directly or indirectly of individuals, whether or not such bodies possess legal personality? (R(87)15 ‘Scope and definitions’; Explanatory Memorandum para. 28)	
Click here to enter text.	Click here to enter text.

Q.9 Has your country extended any of the principles of R(87)15 to the collection, storage and use of personal data for purposes of state security? (R(87)15 ‘Scope and definitions’; Explanatory Memorandum para. 29)	
Click here to enter text.	Click here to enter text.

Basic Principles
Principle 1 – Control and notification

Q.10 Principle 1.1: What is the name of the independent supervisory authority outside the police sector responsible for ensuring respect for the principles contained in Recommendation R(87)15? (R(87)15 Principle 1.1; Explanatory Memorandum para. 31–33)	
Click here to enter text.	Click here to enter text.

Q.11 Principle 1.2: Is a privacy/data protection impact assessment undertaken when new technical means for data processing are introduced, to ensure that their use complies with the spirit of existing data protection legislation? (R87(15) Principle 1.2; Explanatory Memorandum para. 34)	
Choose an item. Comment: Click here to enter text.	Click here to enter text.
Q.12 If a privacy/data protection impact assessment is not undertaken, what other reasonable measures are taken to ensure compliance? (R87(15) Principle 1.2; Explanatory Memorandum para. 34)	
Click here to enter text.	Click here to enter text.

Q.13 Principle 1.3: Is the "responsible body" obliged to consult the supervisory authority in advance in any case where the introduction of automated processing methods raises questions about the application of R(87)15? (R87(15) Principle 1.3; Explanatory Memorandum para. 35)	
Choose an item. Comment: Click here to enter text.	Click here to enter text.
Q.14 If the consultation is not legally obliged, is it such considered to be a mandatory practice? (R87(15) Principle 1.3; Explanatory Memorandum para. 35)	
Click here to enter text.	Click here to enter text.

Q.15 Principle 1.4: Is there an obligation in your country to notify permanent automated police files to the supervisory authority? (R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 36–38)	
Choose an item. Comment: Click here to enter text.	Click here to enter text.
Q.16 If yes, what should the notification specify? (R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 36–38)	

Click here to enter text.	Click here to enter text.
Q.17 Is there an obligation in your country to notify manual police files to the supervisory authority and, if so, what should the notification specify? (R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 38–39)	
Choose an item. Comment: Click here to enter text.	Click here to enter text.
Q.18 If the answer to Q.17 is No, has a general description been drawn up at central level to which manual police files are required to conform? (R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 38–39)	
Click here to enter text.	Click here to enter text.
Q.19 If a police force does not comply with this general description, would it be obliged to make its own description and to notify it to the supervisory authority? (R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 38–39)	
Choose an item.	Click here to enter text.
Q.20 Are the principles laid down in R(87)15 extended to manual police files in any other ways? (R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 38–39)	
Click here to enter text.	Click here to enter text.

Q.21 Principle 1.4: Is there any obligation in your country to notify *ad hoc* police files which have been set up at the time of particular inquiries? (R87(15) Principle 1.4 second sub-paragraph; Explanatory Memorandum para. 40–42)	
Choose an item. Comment: Click here to enter text.	Click here to enter text.
Q.22 If the answer to Q 21. was Yes, under what conditions/national legislation is this done? (R87(15) Principle 1.4 second sub-paragraph; Explanatory Memorandum para. 40–42)	
Click here to enter text.	Click here to enter text.

Principle 2 – Collection of data

Q.23 Principle 2.1: Are there instances of collection of personal data for police purposes for purposes others than the prevention of a real danger or the suppression of a specific criminal offence? (R87(15) Principle 2.1; Explanatory Memorandum para. 43)	
Choose an item.	Click here to enter text.

Comment: Click here to enter text.	
Q.24 If the answer to Q 23. was Yes, is such collection the subject of specific national legislation clearly authorising wider police powers to gather information? (R87(15) Principle 2.1; Explanatory Memorandum para. 43)	
Click here to enter text.	Click here to enter text.

Q.25 Principle 2.2: According to existing records, on how many occasions have data subjects been informed where data concerning them have been collected and stored without their knowledge and have not been deleted as soon as the object of the police activities was no longer likely to be prejudiced? (R87(15) Principle 2.2; Explanatory Memorandum para. 44–45)	
Click here to enter text.	Click here to enter text.

Q.26 Principle 2.3: Which laws/specific provisions provide for collection of data by technical surveillance or other automated means? Please provide the title of the legislation/measure, its reference number, date of enactment and the date it came into effect. (R87(15) Principle 2.3; Explanatory Memorandum para. 46–47)	
Click here to enter text.	Click here to enter text.
Q.27 Are those laws/specific provisions accompanied by adequate guarantees against abuse? If yes, please provide examples of such guarantees. (R87(15) Principle 2.3; Explanatory Memorandum para. 46–47)	
Choose an item. Click here to enter text.	Click here to enter text.

Q.28 Principle 2.4: Does the law of your country prohibit the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law, unless absolutely necessary for the purposes of a particular inquiry? (R87(15) Principle 2.4; Explanatory Memorandum para. 48)	
Click here to enter text.	Click here to enter text.
Q.29 According to existing records, on how many occasions has data on individuals been collected solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law? (R87(15) Principle 2.4; Explanatory Memorandum para. 48)	

Click here to enter text.	
Q.30 How was/is the question of “absolute necessity for the purposes of a particular inquiry” determined? (R87(15) Principle 2.4; Explanatory Memorandum para. 48)	
Click here to enter text.	Click here to enter text.

Principle 3 – Storage of data

Q.31 Principle 3.1: What measures are in place to ensure that, as far as possible, the storage of personal data for police purposes is limited to accurate data and to data necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law? (R87(15) Principle 3.1; Explanatory Memorandum para. 49–51)	
Click here to enter text.	Click here to enter text.

Q.32 Principle 3.2: The Explanatory Memorandum refers to ‘a system of data classification’. In your country, are different categories of data stored by police authorities distinguished in accordance with their degree of accuracy or reliability? (R87(15) Principle 3.2; Explanatory Memorandum para. 52)	
Click here to enter text.	Click here to enter text.
Q.33 In particular, do the police authorities of your country distinguish data based on facts from data based on opinions or personal assessments? (R87(15) Principle 3.2; Explanatory Memorandum para. 52)	
Click here to enter text.	Click here to enter text.

Q.34 Principle 3.3: Do the police authorities of your country store data which has been collected for administrative purposes (for example, information on firearms certificates granted, lost property, etc) and are to be stored permanently, in a separate file? (R87(15) Principle 3.3; Explanatory Memorandum para. 53–54)	
Click here to enter text.	Click here to enter text.
Q.35 Is such administrative data also subject to the special regime for police data? (R87(15) Principle 3.3; Explanatory Memorandum para. 53–54)	
Click here to enter text.	Click here to enter text.

Principle 4 – Use of data by the police (statement of the notion of

finality)

Q.35 Principle 4: Are there instances in which personal data collected and stored by the police for police purposes (the prevention and suppression of criminal offences or the maintenance of public order) are used for other purposes? (R87(15) Principle 4; Explanatory Memorandum para. 55)	
Click here to enter text.	Click here to enter text.

Principle 5 – Communication of data

Q.36 Principle 5.1: In what circumstances is the communication between police bodies of data to be used for police purposes permissible? (R87(15) Principle 5.1; Explanatory Memorandum para. 56)	
Click here to enter text.	Click here to enter text.
Q.37 Does it require the police authorities to have a “legitimate interest” in obtaining the data? (R87(15) Principle 5.1; Explanatory Memorandum para. 57)	
Choose an item. Click here to enter text.	Click here to enter text.
Q.38 If it is required that the receiving police authority possess a “legitimate interest” in obtaining the data, how is such a “legitimate interest” for such communication to be determined? (R87(15) Principle 5.1; Explanatory Memorandum para. 57)	
Click here to enter text.	Click here to enter text.
Q.39 Is any oversight mechanism in place? (R87(15) Principle 5.1; Explanatory Memorandum para. 57)	
Choose an item. Click here to enter text.	Click here to enter text.

Q.40 Principle 5.2: In what circumstances is the communication of police data to other public bodies (e.g. social security authorities, inland revenue authorities, immigration control, customs authorities etc.) permissible? (R87(15) Principle 5.2.i; Explanatory Memorandum para. 58–61)	
Click here to enter text.	Click here to enter text.

Q.41 Are there instances in your law of a clear legal obligation on the police authorities to communicate data to any other public bodies? (R87(15) Principle 5.2.i.*a*; Explanatory Memorandum para. 60)	

Click here to enter text.	Click here to enter text.
Q.42 Are there instances in which the supervisory authority may authorise such a communication of data by the police authorities to any other public bodies? (R87(15) Principle 5.2.i.*a*; Explanatory Memorandum para. 60)	
Click here to enter text.	Click here to enter text.
Q.43 Is any other authority empowered to authorise the police authorities to communicate data to any other public bodies? (R87(15) Principle 5.2.i.*a*; Explanatory Memorandum para. 60)	
Click here to enter text.	Click here to enter text.

Q.44 Are there any other circumstances in which the police authorities of your country are authorised to communicate data to other public bodies (apart from when there exists a clear legal obligation or authorisation)? (R87(15) Principle 5.2.i.*b* and 5.2.ii; Explanatory Memorandum para. 61–62)	
Click here to enter text.	Click here to enter text.
Q.45 Are there any provisos to this authority being granted? (R87(15) Principle 5.2.i.*b* and 5.2.ii; Explanatory Memorandum para. 61–62)	
Click here to enter text.	Click here to enter text.
Q.46 Is any oversight mechanism in place with regard to determinations of authorisation to communicate data to other public bodies? (R87(15) Principle 5.2.i.*b* and 5.2.ii; Explanatory Memorandum para. 61–62)	
Click here to enter text.	Click here to enter text.

Q.47 According to existing records, on how many occasions has communication to other public bodies been exceptionally permitted, in a particular case?	
Click here to enter text.	

Q.48 Principle 5.3: In what circumstances is the communication of police data to private parties permissible? (R87(15) Principle 5.3; Explanatory Memorandum para. 58, 63–64)	
Click here to enter text.	Click here to enter text.

Q.49 Are there instances in your law of a clear legal obligation on the police authorities to communicate data to any private parties (R87(15) Principle 5.3; Explanatory Memorandum para. 63–64)	
Click here to enter text.	Click here to enter text.

Q.50 Are there instances in which the supervisory authority may authorise such a communication of data by the police authorities to any private parties? (R87(15) Principle 5.3; Explanatory Memorandum para. 63–64)	
Click here to enter text.	Click here to enter text.
Q.51 Is any other authority empowered to authorise the police authorities to communicate data to a private party? (R87(15) Principle 5.3; Explanatory Memorandum para. 63–64)	
Click here to enter text.	Click here to enter text.

Q.52 Are there any other circumstances in which the police authorities of your country are authorised to communicate data to private parties (apart from when there exists a clear legal obligation or authorisation)? (R87(15) Principle 5.3; Explanatory Memorandum para. 63–64)	
Click here to enter text.	

Q.53 According to existing records, on how many occasions has communication to private parties been exceptionally permitted, in a particular case?	
Click here to enter text.	

Q.54 Principle 5.4: Is communication of data to foreign authorities restricted to police bodies? (R87(15) Principle 5.4; Explanatory Memorandum para. 65–69)	
Click here to enter text.	Click here to enter text.

Q.55 Is there clear legal provision under national or international law enabling the communication of data by your police authority to foreign authorities? (R87(15) Principle 5.4.*a*; Explanatory Memorandum para. 65–69)	
Click here to enter text.	

Q.56 In the absence of such a provision, in what other circumstances may your police authorities communicate data to foreign authorities? (R87(15) Principle 5.4.*b*; Explanatory Memorandum para. 65–69)	
Click here to enter text.	Click here to enter text.
Q.57 Is any oversight mechanism in place with regard to determinations of circumstances warranting the communication of data to foreign authorities? (R87(15) Principle 5.4; Explanatory Memorandum para. 65–69)	
Click here to enter text.	Click here to enter text.

Q.58 According to existing records, on how many occasions have your police authorities communicated data to foreign authorities in the absence of a clear legal provision under national or international law permitting such communication? (R87(15) Principle 5.4; Explanatory Memorandum para. 65–69)	
Click here to enter text.	
Q.59 What circumstances justified such a communication? (R87(15) Principle 5.4; Explanatory Memorandum para. 65–69)	
Click here to enter text.	

Q.60 Principle 5.5.i: What information does your country require to be included when requests for communication of data are made to the police authorities? (R87(15) Principle 5.5.i; Explanatory Memorandum para. 70–72)	
Click here to enter text.	Click here to enter text.
Q.61 In particular, is it a requirement that requests for communication of data be justified, i.e. that they include the reason for the request and its objective? (R87(15) Principle 5.5.i; Explanatory Memorandum para. 70–72)	
Choose an item. Click here to enter text.	Click here to enter text.
Q.62 Are there any specific provisions contained in national legislation or in international agreements applicable to your country in regard to requests for communication of data? (R87(15) Principle 5.5.i; Explanatory Memorandum para. 70–72)	
Click here to enter text.	Click here to enter text.

Q.63 Principle 5.5.ii: Do your police authorities have structures in place whereby, at the latest at the time of their communication, the quality of data is verified? (R87(15) Principle 5.5.ii; Explanatory Memorandum para. 73–75)	
Click here to enter text.	Click here to enter text.
Q.64 Do your police authorities have structures in place whereby, in all communications of data, judicial decisions, as well as decisions not to prosecute, are indicated and data based on opinions or personal assessments checked at source before being communicated? (R87(15) Principle 5.5.ii; Explanatory Memorandum para. 73–75)	
Choose an item. Click here to enter text.	Click here to enter text.

Q.65 What strategy does the law require when data which are no longer accurate or up to date are to be, or have been, communicated? (R87(15) Principle 5.5.ii; Explanatory Memorandum para. 73–75)	
Click here to enter text.	Click here to enter text.

Q.66 Principle 5.5.iii: Are any safeguards in place to ensure that data communicated to other public bodies, private parties and foreign authorities are not used for purposes other than those specified in the request for communication? (R87(15) Principle 5.5.iii; Explanatory Memorandum para. 76–77)	
Click here to enter text.	

Q.67 According to existing records, have requests ever been made by other public bodies, private parties or foreign police authorities to use the communicated data for purposes other than those specified in the request for communication?	
Click here to enter text.	
Q.68 If yes, to how many of those requests has the communicating police body acceded?	
Click here to enter text.	

Q.69 Principle 5.6: Is there any clear legal provision in the laws of your country that authorises any interconnection of police files with files held for different purposes (for e.g. social security bodies, passenger lists kept by airlines, trade union membership files, etc.)? (R87(15) Principle 5.6; Explanatory Memorandum para. 78–79)	
Click here to enter text.	Click here to enter text.
Q.70 If so, does the clear legal provision state the conditions under which interlinkage can take place? (R87(15) Principle 5.6; Explanatory Memorandum para. 78–79)	
Click here to enter text.	Click here to enter text.
Q.71 May the supervisory body grant authorisation for the interconnection of files with files held for different purposes, and if so, is such authorisation limited to particular purposes? (R87(15) Principle 5.6; Explanatory Memorandum para. 78–79)	
Click here to enter text.	Click here to enter text.

Q.72 According to existing records, on how many occasions and in what instances has the interconnection of files with files held for different	

purposes been authorised by the supervisory body?	
Click here to enter text.	
Q.73 What limited purposes, if any, was this authorisation granted for?	
Click here to enter text.	

Q.74 How many of your police systems are accessible on-line even if in a secure fashion? (R87(15) Principle 5.6; Explanatory Memorandum para. 80)	
Click here to enter text.	
Q.75 Does the domestic legislation of your country allow direct access or online access to a file? If yes, does it provide specific safeguards in those cases where direct access or online access to a file is permitted? (R87(15) Principle 5.6; Explanatory Memorandum para. 80)	
Choose an item. Click here to enter text.	Click here to enter text.

Principle 6 – Publicity, right of access to police files, right of rectification and right of appeal

Q.76 Principle 6.1: Does the supervisory authority of your country take any measures so as to satisfy itself that the public is informed of the existence of police files, as well as of the rights of individuals in regard to these files (the requirement of publicity)? (R87(15) Principle 6.1; Explanatory Memorandum para. 81–82)	
Click here to enter text.	Click here to enter text.
Q.77 In what manner does implementation of the requirement of publicity take account of the specific nature of *ad hoc* files, in particular the need to avoid serious prejudice to the performance of a legal task of the police bodies? (R87(15) Principle 6.1; Explanatory Memorandum para. 81–82)	
Click here to enter text.	

Q.78 Principle 6.2: What arrangements does your country provide for the data subject to be able to obtain access to a police file at reasonable intervals and without excessive delay? (R87(15) Principle 6.2; Explanatory Memorandum para. 83–84)	
Click here to enter text.	Click here to enter text.
Q.79 Does your country operate a system of registration of requests for access to data? (R87(15) Principle 6.2; Explanatory Memorandum para. 84)	
Choose an item.	
Q.80 If the answer to Q.79 is Yes, is the register of requests kept separate	

from the normal criminal files held by the police, and is data deleted from the register after the lapse of a period of time? (R87(15) Principle 6.2; Explanatory Memorandum para. 84)	
Click here to enter text.	Click here to enter text.

Q.81 Principle 6.3: What is required of the data subject for her to be able to obtain, where appropriate, rectification or erasure of her data which are contained in a file? (R87(15) Principle 6.3; Explanatory Memorandum para. 85–86)	
Click here to enter text.	Click here to enter text.

Q.82 According to existing records, how many data subject requests for rectification or erasure of data contained in a police file have been received by the police authorities?	
Click here to enter text.	
Q.83 According to existing records, on how many occasions were data found to be excessive, inaccurate or irrelevant in application of any of the principles contained in R(87)15?	
Click here to enter text.	
Q.84 What action, if any, was taken or is planned to be taken pursuant to these findings?	
Click here to enter text.	
Q.85 Within what time-frame was such action taken or is expected to be taken?	
Click here to enter text.	

Q.86 Principle 6.4: In what instances have the rights of access, and thus the rights of rectification and erasure, been refused? Please give examples. (R87(15) Principle 6.4; Explanatory Memorandum para. 87–90)	
Click here to enter text.	Click here to enter text.

Q.87 Principle 6.5: Does the law of your country oblige the police authority to provide the data subject with a reasoned restriction or refusal of the exercise of the data subject's rights to access, rectification or erasure of her data? How are such reasons communicated to the data subject? (R87(15) Principle 6.5; Explanatory Memorandum para. 91)	
Click here to enter text.	Click here to enter text.
Q.88 In what circumstances may the police refuse to communicate the reasons for a restriction or refusal of the data subject's rights to access, rectification or erasure of data? (R87(15) Principle 6.5; Explanatory Memorandum para. 92)	
Click here to enter text.	

Q.89 In either case, is the data subject given information on how to challenge the decision? (R87(15) Principle 6.6; Explanatory Memorandum para. 92)	
Click here to enter text.	

Q.90 In what sort of real case scenarios has the exercise of such rights been restricted or refused?	
Click here to enter text.	

Q.100 Does the law provide for a right of appeal to the supervisory authority or to another independent body (for e.g. a court or tribunal) from a refusal to grant access? (R87(15) Principle 6.6; Explanatory Memorandum para. 92–95)	
Click here to enter text.	Click here to enter text.
Q.101 Is the supervisory authority or other independent body obliged to communicate the data to the individual if there is no justification for refusing access? If not, what alternative action could it take? (R87(15) Principle 6.6; Explanatory Memorandum para. 92–95)	
Click here to enter text.	Click here to enter text.
Q.102 According to existing records, on how many occasions has a denied access request been challenged before the supervisory authority or other independent body?	
Click here to enter text.	
Q.103 On how many occasions has the supervisory authority or other independent body decided that there was no justification for refusing access, and what action did it take?	
Click here to enter text.	

Principle 7 – Length of storage and updating of data

Q.104 Principle 7.1: What measures are taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored? (R87(15) Principle 7.1; Explanatory Memorandum para. 96)	
Click here to enter text.	Click here to enter text.

Q.105 Principle 7.2: Has your country established rules aimed at fixing storage (or conservation) periods for the different categories of personal data collected and stored for police purposes? (R87(15) Principle 7.2; Explanatory Memorandum para. 97–99)	
Click here to enter text.	Click here to enter text.

Q.106 Who or which authority was responsible for formulating the rules. Please describe the content and application of the said rules. Kindly provide a reference to the rules. (R87(15) Principle 7.2; Explanatory Memorandum para. 98)	
Click here to enter text.	Click here to enter text.

Q.107 Has your country established rules aimed at regular checks on the quality of personal data collected and stored for police purposes? (R87(15) Principle 7.2; Explanatory Memorandum para. 98)	
Click here to enter text.	Click here to enter text.
Q.108 Who or which authority was responsible for formulating the rules. Please describe the content and application of the said rules. Kindly provide a reference and attach the relevant text. (R87(15) Principle 7.2; Explanatory Memorandum para. 98)	
Click here to enter text.	Click here to enter text.

Principle 8 – Data security

Q.109 Has the "responsible body" (i.e. the controller of the police files) taken all the necessary measures to ensure the appropriate physical and logical security of the personal data collected and stored for police purposes, and to prevent unauthorised access, communication or alteration thereto? (R87(15) Principle 8; Explanatory Memorandum para. 100)	
Click here to enter text.	Click here to enter text.
Q.110 For these purposes, have the different characteristics and contents of files containing personal data collected and stored for police purposes been taken into account? (R87(15) Principle 8; Explanatory Memorandum para. 100)	
Click here to enter text.	Click here to enter text.

La protection des données à caractère personnel est une des priorités du Conseil de l'Europe. Le Conseil de l'Europe est actuellement engagé dans un exercice important visant à réviser les instruments juridiques qui font partie du cadre de protection destiné à fournir des garanties pour les citoyens européens. L'un des domaines clés où le Conseil de l'Europe met à jour son cadre juridique vise à trouver un juste équilibre entre vie privée et l'emploi proportionné des données à caractère personnel dans l'utilisation à fins policières. Ce questionnaire constitue un outil important que les Etats membres sont fortement encouragés à remplir afin de fournir une base factuelle et circonstanciée aux décisions politiques qui seront prises dans un avenir proche.

Ce document fait partie de la recherche effectuée au nom du Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), facilitée par le Secrétariat du T-PD au sein de la Division de la Société de l'Information, des Médias et de la Protection des Données, Direction Générale des droits de l'homme et des affaires juridiques du Conseil de l'Europe.

Mme Sophie Kwasny, Secrétaire du T-PD
Professeur Joseph A. Cannataci et Dr. Mireille M. Caruana

Avec le concours de :

Les questionnaires complets sont à retourner à : lwxmc@bristol.ac.uk, avec, en copie : joseph.cannataci@um.edu.mt et data.protection@coe.int

Traitement des données à caractère personnel

dans le secteur de la justice pénale : questionnaire

La présente étude vise à présenter l'évolution historique et l'état actuel des différentes législations qui réglementent l'utilisation des données à caractère personnel dans les secteurs de la police et de la justice pénale dans les États membres du Conseil de l'Europe. L'objectif principal est d'examiner dans quelle mesure la recommandation R(87)15 du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police a été mise en œuvre en Europe.

Répondre à ce questionnaire n'est pas obligatoire. Cependant, votre contribution est précieuse car elle aidera le Conseil de l'Europe et les autres acteurs clefs du processus normatif à mieux comprendre l'état actuel de la protection des données dans le secteur de la police. Vos réponses resteront confidentielles, à moins que vous ne cochiez la case ci-dessous pour indiquer que vous acceptez d'être cité ou nommé en votre nom propre[79].

J'accepte que mon nom et [affiliation/établissement] soient cités dans les résultats de l'étude, y compris ses rapports et publications. ☐

Afin de vous aider à répondre, chaque question est suivie du principe de la recommandation[80] (entre parenthèses) auquel il est fait référence, et du paragraphe pertinent de l'exposé des motifs.

Vous êtes priés de retourner ce questionnaire accompagné en pièce jointe de la législation pertinente de votre pays (version linguistique originale ainsi que d'une traduction en anglais ou en français).

Lorsque vous répondez aux questions, nous vous remercions de bien vouloir inclure une référence précise au texte législatif, en renvoyant vers l'article et le numéro de page, du document attaché, et, idéalement, de copier/coller les sections pertinentes dans l'espace réservé à cet effet.

Nota Bene : si vous ne pouvez pas répondre à une question, passez directement à la suivante.

[79] Les données seront conservées dans un format confidentiel et protégé par la Direction générale des droits de l'homme et affaires juridiques du Conseil de l'Europe, et par M. Cannataci et Mme Caruana, qui seront les « maîtres des fichiers » en vertu des lois et règlements applicables.

[80] https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2766610&SecMode=1&DocId=694310&Usage=2

Informations personnelles

Nom : Cliquer ici pour saisir le texte. Prénom : Cliquer ici pour saisir le texte.

Courriel: Cliquer ici pour saisir le texte.

Numéro de téléphone : Cliquer ici pour saisir le texte.

Institution ayant répondu à ce questionnaire : Cliquer ici pour saisir le texte.

Adresse : Cliquer ici pour saisir le texte.

Fonction dans l'institution : Cliquer ici pour saisir le texte.

Date:

Partie 1 – Aperçu	**Application de la loi & section**
Q.1 Quels sont les textes de loi, ou autres mesures réglementaires, qui encadrent l'utilisation de données à caractère personnel par la police de votre pays? Veuillez donner l'intitulé de la loi, son numéro de référence, sa date de promulgation et sa date de mise en vigueur.	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.2 [Pour les pays de l'espace Schengen] Conformément au Traité d'Amsterdam de 1997, votre pays a accepté d'appliquer, partiellement ou totalement,[81] la recommandation R(87)15 du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Quel est l'intitulé de la loi, ou autres mesures réglementaires, qui garantissent que votre pays soit en conformité avec cette partie de l'*acquis communautaire*? Veuillez donner l'intitulé de la loi, son numéro de référence, sa date de promulgation et sa date de mise en vigueur.	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.3 [Pour les pays en dehors de l'espace Schengen] En tant qu'Etat en dehors de l'espace Schengen, l'application de cette partie de l'*acquis communautaire* qui comprend la recommandation R(87)15 n'est pas	

[81] Il y a un débat quant à l'interprétation de l'Accord de Schengen, en particulier dans la mesure où les Etats participants peuvent s'attendre à mettre en œuvre la recommandation R87 (15) dans sa totalité ou seulement à des cas spécifiques d'utilisation des données à caractère personnel à fins policières.

obligatoire dans votre pays. Votre pays a-t-il cependant, directement ou indirectement, adopté des lois ou autres réglementations appliquant la recommandation R(87)15? Si tel est le cas, veuillez donner l'intitulé de la loi, son numéro de référence, sa date de promulgation et sa date de mise en vigueur.	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Partie 2 – Dispositions détaillées Champ d'application et définitions	**Application de la loi & section**

Q.4 Comment la législation de votre pays définit-elle les données à caractère personnel « à des fins de police »? (R87(15), Champ d'application et définitions; Exposé des motifs, paragr. 22)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.5 Dans votre pays, quel est l' « organe responsable » (autorité, service ou autre organisme public) compétent en droit interne, pour décider de la finalité d'un fichier automatisé, des catégories de données à caractère personnel qui doivent être archivées et des opérations qui leur sont appliquées (c'est-à-dire le « maître des fichiers de police »)? (R(87)15, Champ d'application et définitions ; Exposé des motifs, paragr. 25)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.6 Votre pays a-t-il élargi les principes contenus dans la recommandation R(87)15 aux données à caractère personnel faisant l'objet d'un traitement manuel ? (R(87)15, Champ d'application et définitions ; Exposé des motifs, paragr. 26–27)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.7 Dans la négative, quel, traitement manuel des données existe t-il? Quel en est le but ? (R(87)15, Champ d'application et définitions ; Exposé des motifs, paragr. 26–27)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.8 Votre pays a-t-il élargi les principes contenus dans la recommandation R(87)15 aux données afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique? (R(87)15, Champ d'application et définitions; Exposé des motifs, paragr. 28)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.9 Votre pays a-t-il élargi les principes de la recommandation R(87)15 à la collecte, l'enregistrement et l'utilisation de données à caractère personnel aux fins de la sécurité d'Etat ? (R(87)15, Champ d'application et définitions; Exposé des motifs, paragr. 29)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Principes de base
Principe 1 – Contrôle et notification

Q.10 Principe 1.1: Quel est le nom de l'autorité de contrôle indépendante et extérieure à la police, chargée de veiller au respect des principes énoncés dans la recommandation R(87)15? (R(87)15, Principe 1.1; Exposé des motifs, paragr. 31–33)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.11 Principe 1.2: Une évaluation de l'incidence sur la protection des données et la vie privée a-t-elle été réalisée lorsque de nouveaux moyens techniques ont été introduits, pour s'assurer que leur utilisation soit conforme à l'esprit de la législation existante sur la protection des données? (R87(15), Principe 1.2; Exposé des motifs, paragr. 34)	
Choisir un thème. Observation: Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.12 Si une évaluation de l'incidence sur la protection des données et la vie privée n'a pas été réalisée, quelles ont été les autres mesures raisonnables prises pour s'assurer que l'utilisation des données soit conforme ? (R87(15), Principe 1.2; Exposé des motifs, paragr. 34)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.13 Principe 1.3: L'organe responsable est-il obligé de consulter à	

l'avance l'autorité de contrôle chaque fois que l'introduction de procédés de traitement automatisé soulève des questions concernant l'application de la recommandation R(87)15? (R87(15), Principe 1.3; Exposé des motifs, paragr. 35)	
Choisir un thème. Observation: Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.14 Si la consultation n'est pas une obligation légale, est-elle rendue obligatoire par la pratique? (R87(15), Principe 1.3; Exposé des motifs, paragr. 35)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.15 Principe 1.4: Est-il obligatoire dans votre pays de déclarer les fichiers permanents automatisés à l'autorité de contrôle ? (R87(15), Principe 1.4, premier sous-paragraphe; Exposé des motifs, paragr. 36–38)	
Choisir un thème. Observation: Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.16 Si oui, que doit indiquer la déclaration? (R87(15), Principe 1.4, premier sous-paragraphe; Exposé des motifs, paragr. 36–38)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.17 Est-il obligatoire dans votre pays de déclarer les fichiers de police manuels à l'autorité de contrôle, et si oui, que doit indiquer la déclaration ? (R87(15), Principe 1.4, premier sous-paragraphe; Exposé des motifs, paragr. 38–39)	
Choisir un thème. Observation: Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.18 Si la réponse à la Q.17 est négative, une description générale a-t-elle été formulée au niveau central à laquelle les fichiers de police manuels doivent être conformes ? (R87(15), Principe 1.4, premier sous-paragraphe; Exposé des motifs, paragr. 38–39)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.19 Si une force de police ne respecte pas cette description générale, est-elle tenue d'élaborer sa propre description et de la déclarer à l'autorité de contrôle ? (R87(15), Principe 1.4, premier sous-paragraphe; Exposé des motifs, paragr. 38–39)	
Choisir un thème. Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.20 Les principes exposés dans la recommandation R(87)15 ont-ils été élargis aux fichiers de police manuels selon d'autres critères? (R87(15), Principe 1.4, premier sous-paragraphe; Exposé des motifs, paragr. 38–39)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.21 Principe 1.4: Est-il obligatoire dans votre pays de déclarer les fichiers *ad hoc* constitués à l'occasion d'affaires particulières? (R87(15), Principe 1.4, deuxième sous-paragraphe; Exposé des motifs, paragr. 40–42)	
Choisir un thème. Observation: Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.22 Si la réponse à la Q.21 était Oui, dans le cadre de quelles conditions ou législation nationale cette déclaration est-elle faite ? (R87(15), Principe 1.4, deuxième sous-paragraphe; Exposé des motifs, paragr. 40–42)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Principe 2 – Collecte des données

Q.23 Principe 2.1: Existe-t-il des exemples de collecte de données à caractère personnel à des fins de police qui ne se limitent pas à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée? (R87(15), Principe 2.1; Exposé des motifs, paragr. 43)	
Choisir un thème. Observation: Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.24 Si la réponse à la Q.23 était positive, existe-t-il une législation nationale spécifique qui accorde clairement des pouvoirs élargis à la police pour collecter de telles informations ? (R87(15), Principe 2.1; Exposé des motifs, paragr. 43)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.25 Principe 2.2: Selon les enregistrements existants, à combien de reprises des personnes ont-elles été informées que des données les concernant avaient été collectées et enregistrées à leur insu sans avoir été détruites à partir du moment où l'objet des activités de police ne risquait plus de subir un préjudice? (R87(15), Principe 2.2; Exposé des motifs, paragr. 44–45)	

Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.26 Principe 2.3: Quelles sont les lois ou les dispositions spécifiques qui prévoient la collecte de données par des moyens techniques de surveillance ou d'autres moyens automatisés? Veuillez donner l'intitulé de la loi, son numéro de référence, la date de promulgation et date de mise en vigueur. (R87(15), Principe 2.3; Exposé des motifs, paragr. 46–47)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.27 Ces lois ou ces dispositions spécifiques sont-elles assorties de garanties adéquates contre les abus ? Si oui, veuillez fournir des exemples de telles garanties. (R87(15), Principe 2.3; Exposé des motifs, paragr. 46–47)	
Choisir un thème. Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.28 Principe 2.4: La législation de votre pays interdit-elle la collecte de données sur des individus au motif unique de leur origine raciale, convictions religieuses, comportement sexuel ou opinions politiques ou qu'ils appartiennent à des mouvements ou organisations qui ne sont pas interdits par la loi, sauf si elle est absolument nécessaire pour les besoins d'une enquête déterminée? (R87(15), Principe 2.4; Exposé des motifs, paragr. 48)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.29 Selon les enregistrements existants, combien de fois des données sur des individus ont-elles été collectées au motif unique de leur origine raciale, convictions religieuses, comportement sexuel ou opinions politiques ou qu'ils appartiennent à des mouvements ou organisations qui ne soient pas interdits par la loi? (R87(15), Principe 2.4; Exposé des motifs, paragr. 48)	
Cliquer ici pour saisir le texte.	
Q.30 Comment a-t-on déterminé, ou détermine-t-on, qu'une collecte est « absolument nécessaire pour les besoins d'une enquête déterminée » ? (R87(15), Principe 2.4; Exposé des motifs, paragr. 48)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Principe 3 – Enregistrement des données

Q.31 Principe 3.1: Quelles mesures sont en place pour s'assurer que, dans la mesure du possible, l'enregistrement de données à caractère personnel à des fins de police ne concerne que les données exactes et se limite aux données nécessaires pour permettre aux organes de police d'accomplir leurs tâches légales dans le cadre du droit interne et des obligations découlant du droit national ? (R87(15), Principe 3.1; Exposé des motifs, paragr. 49–51)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.32 Principe 3.2: L'exposé des motifs fait référence à « un système de classification des données ». Dans votre pays, les différentes catégories de données enregistrées par les autorités de police sont-elles différenciées en fonction de leur degré d'exactitude ou de fiabilité? (R87(15), Principe 3.2; Exposé des motifs, paragr. 52)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.33 En particulier, les autorités de police de votre pays établissent-elles une distinction entre les données fondées sur des opinions et celles fondées sur des appréciations personnelles? (R87(15), Principe 3.2; Exposé des motifs, paragr. 52)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.34 Principe 3.3: Les autorités de police de votre pays enregistrent-elles les données qui ont été collectées à des fins administratives (par exemple les permis de port d'armes accordés, les objets trouvés, etc.) et sont-elles enregistrées de manière permanente, dans un fichier séparé ? (R87(15), Principe 3.3; Exposé des motifs, paragr. 53–54)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.35 Ces données collectées à des fins administratives sont-elles également soumises aux règles applicables aux données de police ? (R87(15), Principe 3.3; Exposé des motifs, paragr. 53–54)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Principe 4 – Utilisation des données par la police (énoncé de la notion de finalité)

Q.35/36 Principe 4: Existe-t-il des exemples dans lesquels des données à caractère personnel collectées et enregistrées par la police à des fins de police (la prévention et la répression d'infractions pénales ou le maintien de l'ordre public) ont été utilisées à d'autres fins? (R87(15), Principe 4; Exposé des motifs, paragr. 55)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Principe 5 – Communication des données

Q.36 Principe 5.1: Dans quelles circonstances la communication de données entre services de police dans la perspective d'une utilisation à des fins de police est-elle permise? (R87(15), Principe 5.1; Exposé des motifs, paragr. 56)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.37 Les autorités de police doivent-elle avoir un « intérêt légitime » pour obtenir les données ? (R87(15), Principe 5.1; Exposé des motifs, paragr. 57)	
Choisir un thème. Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.38 Si l'autorité de police destinataire doit avoir un « intérêt légitime » pour obtenir les données, comment l' « intérêt légitime » pour une telle communication est-il déterminé? (R87(15), Principe 5.1; Exposé des motifs, paragr. 57)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.39 Existe-t-il un mécanisme de contrôle en vigueur? (R87(15), Principe 5.1; Exposé des motifs, paragr. 57)	
Choisir un thème. Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.40 Principe 5.2: Dans quelles circonstances la communication de données de police à d'autres organes publics (par exemple la sécurité sociale, les autorités fiscales, le contrôle de l'immigration, les douanes, etc.) est-elle permise ? (R87(15), Principe 5.2.i; Exposé des motifs, paragr. 58–61)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.41 Existe-t-il dans votre législation une obligation juridique claire qui autorise les autorités de police à communiquer les données à d'autres organes publics ? (R87(15), Principe 5.2.i.*a*; Exposé des motifs, paragr. 60)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.42 Existe-t-il des exemples dans lesquels l'autorité de contrôle puisse autoriser une telle communication de données par les autorités de police à d'autres organes publics ? (R87(15), Principe 5.2.i.*a*; Exposé des motifs, paragr. 60)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.43 Existe-t-il une autre autorité ayant le pouvoir d'autoriser les autorités de police à communiquer les données à d'autres organes publics? (R87(15), Principe 5.2.i.*a*; Exposé des motifs, paragr. 60)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.44 Existe-t-il d'autres circonstances dans lesquelles les autorités de police de votre pays soient autorisées à communiquer les données à d'autres organes publics (en dehors des cas où il existe une obligation juridique claire ou une autorisation)? (R87(15), Principe 5.2.i.*b* et 5.2.ii; Exposé des motifs, paragr. 61–62)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.45 Existe-t-il des dérogations à cette autorisation ? (R87(15), Principe 5.2.i.*b* et 5.2.ii; Exposé des motifs, paragr. 61–62)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.46 Un mécanisme de contrôle at-il été mis en place pour déterminer qui est autorisé à communiquer les données à d'autres organes publics ? (R87(15), Principe 5.2.i.*b* et 5.2.ii; Exposé des motifs, paragr. 61–62)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.47 Selon les enregistrements existants, combien de fois la communication de données à d'autres organes publics a-t-elle été exceptionnellement autorisée, et dans quel cas particulier?	
Cliquer ici pour saisir le texte.	

Q.48 Principe 5.3: Dans quelles circonstances la communication de données de police à des personnes privées est-elle permise? (R87(15), Principe 5.3; Exposé des motifs, paragr. 58, 63–64)	

Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.49 Existe-t-il des exemples dans la législation de votre pays d'une obligation juridique claire qui autorise les autorités de police à communiquer des données à des personnes privées ? (R87(15), Principe 5.3; Exposé des motifs, paragr. 63–64)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.50 Existe-t-il des exemples dans lesquels l'autorité de contrôle puisse autoriser les autorités de police à communiquer des données à des personnes privées? (R87(15), Principe 5.3; Exposé des motifs, paragr. 63–64)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.51 Existe-t-il une autre autorité ayant le pouvoir d'autoriser les autorités de police à communiquer des données à des personnes privées? (R87(15), Principe 5.3; Exposé des motifs, paragr. 63–64)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.52 Dans quelles autres circonstances les autorités de police de votre pays sont-elles autorisées à communiquer des données à des personnes privées (outre celles pour lesquelles il existe une obligation juridique claire ou une autorisation)? (R87(15), Principe 5.3; Exposé des motifs, paragr. 63–64)	
Cliquer ici pour saisir le texte.	

Q.53 Selon les enregistrements existants, combien de fois la communication de données à des personnes privées a-t-elle été exceptionnellement autorisée, et dans quel cas en particulier?	
Cliquer ici pour saisir le texte.	

Q.54 Principe 5.4: La communication de données à des autorités étrangères est-elle limitée à des services de police ? (R87(15), Principe 5.4; Exposé des motifs, paragr. 65–69)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.55 Existe-t-il une disposition légale claire découlant du droit interne ou	

international autorisant la police de votre pays à communiquer des données à des autorités étrangères? (R87(15), Principe 5.4.*a*; Exposé des motifs, paragr. 65–69)	
Cliquer ici pour saisir le texte.	

Q.56 En l'absence d'une telle disposition, dans quelles autres circonstances la police de votre pays peut-elle communiquer des données à des autorités étrangères? (R87(15), Principe 5.4.*b*; Exposé des motifs, paragr. 65–69)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.57 Existe-t-il un mécanisme de contrôle qui détermine les circonstances selon lesquelles la communication de données à des autorités étrangères soit garantie? (R87(15), Principe 5.4; Exposé des motifs, paragr. 65–69)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.58 Selon les enregistrements existants, combien de fois les autorités de police de votre pays ont-elles communiqué des données à des autorités étrangères en l'absence d'une disposition juridique claire ou d'une loi internationale autorisant une telle communication? (R87(15), Principe 5.4; Exposé des motifs, paragr. 65–69)	
Cliquer ici pour saisir le texte.	
Q.59 Quelles sont les circonstances qui ont justifié une telle communication? (R87(15), Principe 5.4; Exposé des motifs, paragr. 65–69)	
Cliquer ici pour saisir le texte.	

Q.60 Principe 5.5.i: Quelles informations votre pays exige-t-il d'inclure lorsque les autorités de police reçoivent des demandes de communication de données? (R87(15), Principe 5.5.i; Exposé des motifs, paragr. 70–72)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.61 Existe-t-il en particulier une obligation de justifier les demandes de communication, c'est-à-dire de présenter le motif de la demande et son objectif? (R87(15), Principe 5.5.i; Exposé des motifs, paragr. 70–72)	
Choisir un thème. Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.62 La législation interne ou les accords internationaux applicables à votre pays contiennent-ils des dispositions spécifiques concernant les demandes	

de communication de données? (R87(15), Principe 5.5.i; Exposé des motifs, paragr. 70–72)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.63 Principe 5.5.ii: Les autorités de police de votre pays ont-elles les structures en place pour vérifier, au plus tard avant leur communication, la qualité des données? (R87(15), Principe 5.5.ii; Exposé des motifs, paragr. 73–75)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.64 Les autorités de police de votre pays ont-elles mises en place les structures pour faire en sorte que dans toutes les communications de données, les décisions juridictionnelles ainsi que les décisions de ne pas poursuivre soient mentionnées et que les données fondées sur des opinions ou des appréciations personnelles puissent être vérifiées à la source avant d'être communiquées ? (R87(15), Principe 5.5.ii; Exposé des motifs, paragr. 73–75)	
Choisir un thème. Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.65 Quelle stratégie prévoit la loi lorsque des données qui ne sont plus exactes ou à jour ont été communiquées ? (R87(15), Principe 5.5.ii; Exposé des motifs, paragr. 73–75)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.66 Principe 5.5.iii: Existe-t-il des protections pour s'assurer que les données communiquées à d'autres organes publics, à des personnes privées ou à des autorités étrangères ne soient pas utilisées à d'autres fins que celles qui sont spécifiées dans la demande de communication? (R87(15), Principe 5.5.iii; Exposé des motifs, paragr. 76–77)	
Cliquer ici pour saisir le texte.	

Q.67 Selon les enregistrements existants, d'autres organes publics, personnes privées ou autorités de police étrangères ont-ils demandé à utiliser les données communiquées à d'autres fins que celles prévues dans la demande de communication ?	
Cliquer ici pour saisir le texte.	
Q.68 Si oui, à combien de ces demandes l'organe de police qui a communiqué les données a-t-il répondu positivement ?	
Cliquer ici pour saisir le texte.	

Q.69 Principe 5.6: Existe-t-il une disposition juridique claire dans votre pays qui autorise la mise en relation de fichiers de police avec des fichiers utilisés à des fins différentes (par exemple avec ceux de la sécurité sociale, les listes de passagers conservées par les compagnies aériennes, les fichiers des membres syndicalistes, etc.)? (R87(15), Principe 5.6; Exposé des motifs, paragr. 78–79)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.70 Si elle existe, cette disposition juridique claire énonce-t-elle les conditions selon lesquelles cette mise en relation peut avoir lieu? (R87(15), Principe 5.6; Exposé des motifs, paragr. 78–79)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.71 L'organe de contrôle peut-il accorder une autorisation de mise en relation de fichiers avec des fichiers utilisés à des fins différentes, et, si oui, cette autorisation est-elle limitée à des fins particulières ? (R87(15), Principe 5.6; Exposé des motifs, paragr. 78–79)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.72 Selon les enregistrements existants, combien de fois et dans quelles circonstances la mise en relation de fichiers avec des fichiers utilisés à d'autres fins a-t-elle été autorisée par l'organe de contrôle ?	
Cliquer ici pour saisir le texte.	
Q.73 À quelles fins limitées, le cas échéant, cette autorisation a-t-elle été accordée?	
Cliquer ici pour saisir le texte.	

Q.74 À combien de systèmes d'accès à des fichiers de police peut-on accéder en ligne, même protégés ? (R87(15), Principe 5.6; Exposé des motifs, paragr. 80)	
Cliquer ici pour saisir le texte.	
Q.75 La législation interne de votre pays permet-elle un accès direct ou en ligne à un fichier ? Si oui, prévoit-elle des protections particulières dans les cas où un accès direct ou en ligne à un fichier est autorisé ? (R87(15), Principe 5.6; Exposé des motifs, paragr. 80)	
Choisir un thème. Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Principe 6 – Publicité, droit d'accès aux fichiers de police, droit de rectification et droit de recours

Q.76 Principe 6.1: L'organe de contrôle de votre pays prend-il des mesures afin de s'assurer que le public soit informé de l'existence de fichiers de police, ainsi que de ses droits vis-à-vis de ces fichiers (principe de publicité) ? (R87(15), Principe 6.1; Exposé des motifs, paragr. 81–82)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.77 De quelle manière la mise en œuvre de ce principe tient-il compte de la spécificité des fichiers *ad hoc*, en particulier de la nécessité d'éviter que l'accomplissement d'une tâche légale des organes de police ne soit gravement entravé ? (R87(15), Principe 6.1; Exposé des motifs, paragr. 81–82)	
Cliquer ici pour saisir le texte.	

Q.78 Principe 6.2: Quelles modalités prévoit votre pays pour que l'accès à un fichier de police ait lieu à des intervalles raisonnables et sans délais d'attente excessifs? (R87(15), Principe 6.2; Exposé des motifs, paragr. 83–84)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.79 Votre pays a-t-il mis en place un système d'enregistrement des demandes d'accès aux données? (R87(15), Principe 6.2; Exposé des motifs, paragr. 84)	
Choisir un thème.	
Q.80 Si la réponse à la Q.79 était positive, le registre des demandes est-il différencié des fichiers judiciaires normaux conservés par la police, et les données sont-elles supprimées du registre après un certain laps de temps? (R87(15), Principe 6.2; Exposé des motifs, paragr. 84)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.81 Principe 6.3: Que faut-il pour que la personne concernée puisse obtenir, le cas échéant, la rectification ou la suppression des données qui sont contenues dans un fichier? (R87(15), Principe 6.3; Exposé des motifs, paragr. 85–86)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.82 Selon les enregistrements existants, combien les autorités de police ont-elles reçu de demandes de personnes concernées souhaitant une rectification ou une suppression de données contenues dans un fichier de police?	

Cliquer ici pour saisir le texte.	
Q.83 Selon les enregistrements existants, combien de fois les données se sont-elles révélées excessives, inexactes ou non pertinentes en application de l'un des principes contenus dans la recommandation R(87)15?	
Cliquer ici pour saisir le texte.	
Q.84 Quelle mesure a, le cas échéant, été adoptée ou envisagée suite à ces résultats?	
Cliquer ici pour saisir le texte.	
Q.85 Dans quel délai une telle mesure a-t-elle été adoptée ou devrait l'être ?	
Cliquer ici pour saisir le texte.	

Q.86 Principe 6.4: Dans quels cas l'exercice des droits d'accès, et donc les droits de rectification ou d'effacement, a-t-il été refusé ? Veuillez donner des exemples. (R87(15), Principe 6.4; Exposé des motifs, paragr. 87–90)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.87 Principe 6.5: La législation de votre pays oblige-t-elle les autorités de police à restreindre ou à refuser, en motivant leur décision, l'exercice du droit d'accès, de rectification ou de suppression des données d'une personne concernée ? Comment de tels motifs sont-ils communiqués à cette personne? (R87(15), Principe 6.5; Exposé des motifs, paragr. 91)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.88 Dans quelles circonstances la police peut-elle refuser de communiquer à la personne concernée les motifs d'une restriction ou d'un refus des droits d'accès, de rectification ou de suppression des données ? (R87(15), Principe 6.5; Exposé des motifs, paragr. 92)	
Cliquer ici pour saisir le texte.	
Q.89 Dans les deux cas, la personne concernée est-elle informée des voies de recours existantes pour s'opposer à une telle décision? (R87(15), Principe 6.6; Exposé des motifs, paragr. 92)	
Cliquer ici pour saisir le texte.	

Q.90 Dans quelle catégorie de cas réels l'exercice de ces droits a-t-il été restreint ou refusé?	
Cliquer ici pour saisir le texte.	

Q.100 La loi prévoit-elle un droit de recours auprès de l'autorité de contrôle ou d'un autre organe indépendant (par exemple une cour ou un tribunal) dans le cas d'un refus opposé au droit d'accès?	

(R87(15), Principe 6.6; Exposé des motifs, paragr. 92–95)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.101 L'autorité de contrôle, ou un autre organe indépendant, est-elle obligée de communiquer les données à la personne s'il n'y a pas de motif de refuser l'accès? Si elle ne le fait pas, quelle autre mesure peut-elle prendre ? (R87(15), Principe 6.6; Exposé des motifs, paragr. 92–95)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.102 Selon les enregistrements existants, combien de fois un refus d'accès a-t-il été contesté devant l'autorité de contrôle ou un autre organe indépendant ?	
Cliquer ici pour saisir le texte.	
Q.103 Combien de fois l'autorité de contrôle, ou un autre organe indépendant, a-t-elle décidé qu'il n'y avait aucun motif de refuser l'accès, et quelle mesure a été prise?	
Cliquer ici pour saisir le texte.	

Principe 7 – Durée de conservation et mise à jour des données

Q.104 Principe 7.1: Quelles sont les mesures prises pour que les données à caractère personnel conservées à des fins de police soient effacées si elles ne sont plus nécessaires aux fins pour lesquelles elles avaient été enregistrées? (R87(15), Principe 7.1; Exposé des motifs, paragr. 96)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.105 Principe 7.2: Votre pays a-t-il établi des règles destinées à fixer des périodes d'enregistrement (de conservation) pour les différentes catégories de données à caractère personnel collectées et conservées à des fins de police? (R87(15), Principe 7.2; Exposé des motifs, paragr. 97–99)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.106 Quelle instance ou autorité était chargée de formuler ces règles? Veuillez décrire le contenu et l'application desdites règles. (R87(15), Principe 7.2; Exposé des motifs, paragr. 98)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Q.107 Votre pays a-t-il établi des règles visant à appliquer des contrôles périodiques de la qualité des données à caractère personnel collectées et conservées à des fins de police? (R87(15), Principe 7.2; Exposé des motifs, paragr. 98)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.108 Quelle instance ou autorité était chargée de formuler ces règles? Veuillez décrire le contenu et l'application desdites règles. (R87(15), Principe 7.2; Exposé des motifs, paragr. 98)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Principe 8 – Sécurité des données

Q.109 L' « organe responsable » (c'est-à-dire le maître des fichiers de police) a-t-il pris toutes les mesures nécessaires pour garantir la sécurité physique et logique adéquate des données à caractère personnel collectées et conservées à des fins de police, et pour empêcher l'accès ou la communication ou l'altération non autorisés ? (R87(15), Principe 8; Exposé des motifs, paragr. 100)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.
Q.110 À cette fin, a-t-il été tenu compte des différents contenus et caractéristiques des fichiers contenant les données à caractère personnel collectées et conservées à des fins de police ? (R87(15), Principe 8; Exposé des motifs, paragr. 100)	
Cliquer ici pour saisir le texte.	Cliquer ici pour saisir le texte.

Annex B: Table of legislation

Table of legislation

Jurisdiction	Act or other Regulatory Instrument	From	Most recently amended	Comments
Albania	Law No. 9887 "On personal data protection"	2008		Text provided in English.
	Law No 8792 "On Establishment of the Data Processing Centre"	2001		Text provided in English.
	Law No. 9749 "On state police"	2007		Text provided in English.
	Law 9614 "On electronic certificates of criminal record"	2006		No text.
	Law on information classified "State secret"			No text.
	Law no. 8389 "On Albanian citizenship"	1998		No text.
	Law no. 8492 "On foreigners"	1999		No text.
	Law no. 9049 "On property declaration and control of assets"	2003		No text.
	Law No. 8839 "On gathering, administering and storing of classified police information"	2001		No text.
	Regulation "For the automatic processing of data in the TIMS system", approved by Order of Minister of Interior No. 768	2009		Text provided in English.
	Regulation "On data protection and data security in the State Police", approved by the Order No. 330 of the Minister of Interior	2011		Text provided in English.
	Law No. 9604 "On ratification of the Convention on police cooperation for South-East Europe"	2006		No text.
	"Strategic Agreement between Republic of Albania and Europol"	2007		No text.
	"Memorandum of Understanding for securing safe communication lines (channels) between Europol and the Republic of Albania"	2009		No text.
Andorra	Constitution de la Principauté d'Andorre du 14 mars 1993, publiée au bulletin officiel le 28 avril 1993 et qui est entrée en vigueur le même jour de sa publication	1993		Links to all legislative texts in Catalan provided.
	La Loi 8/2004 du 27 mai, qualifiée du Service de police, publiée au bulletin officiel le 30 juin 2004 et qui est entrée en vigueur le lendemain de sa publication.	2007		
	La Loi qualifiée de modification du Code de	1998		

	procédure pénale, du 10 décembre 1998, publiée au bulletin officiel le 7 janvier 1999 et qui est entrée en vigueur le même jour de sa publication.			
	La Loi 10/2005, du 21 février, qualifiée de modification du Code de procédure pénale, publiée au bulletin officiel le 23 mars 2005 et qui est entrée en vigueur six mois après sa publication.	2005		
	Règlement législatif du 17-12-2008, de publication du texte révisée du Code de procédure pénale, publiée au bulletin officiel le 24 décembre 2008 et qui est entrée en vigueur le même jour de sa publication.	2008		
	La Loi qualifiée de la Justice du 3 septembre 1993, publiée au bulletin officiel le 28 septembre 1993 et qui est entrée en vigueur quinze jours après sa publication.	1993		
	La Loi du Ministère fiscal, du 12 décembre 1996, publiée au bulletin officiel le 8 janvier 1997 et qui est entrée en vigueur le même jour de sa publication.	1996		
	La Principauté d'Andorre a adopté la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 22 décembre 1995 (publiée au bulletin officiel le 7 février 1996 et en vigueur un mois après sa publication) qui en application de l'article 3 de la Constitution à été intégré directement lors de son adoption dans l'ordre juridique de la Principauté.	1995		
	La Loi du 29 décembre 2000 de coopération pénale internationale et de lutte contre le blanchiment d'argent ou de valeurs produits de la délinquance internationale, modifiée par la Loi 28/2008 de l'11 décembre, publiée au bulletin officiel le 21 janvier 2009 et qui est entrée en vigueur trois mois après sa publication.	2000	2008	
	Règlement législatif du 9/09/2009, de publication du texte révisée de la loi de coopération pénale internationale et de lutte contre le blanchiment d'argent ou de valeurs produits de la délinquance internationale et le financement du terrorisme du 29 décembre 2000, modifiée par la Loi 28/2008 de l'11 décembre, publiée au bulletin officiel le 16-09-2009 et qui est entrée en vigueur le même jour de sa publication.	2009		
	Convention des Nations Unies contre la			

	criminalité transnationale organisée (Convention de Palerme) du 15 novembre 2000, publiée au bulletin officiel le 22 juin 2011. Convention européenne d'entraide judiciaire en matière pénale fait a Strasbourg le 20-IV-1959, publiée au bulletin officiel le 23 mars 2005. Convention pénale sur la corruption fait à Strasbourg le 23-01-99, publiée au bulletin officiel le 21 novembre 2007. Règlement législatif du 17-12-2008, de publication du texte révisée du Code pénale, publiée au bulletin officiel le 24/12/2008 et qui est entrée en vigueur le même jour de sa publication Code de conduite pour l'administration publique publiée au bulletin officiel le 30 juin 2010 La Loi 15/2003 du 18 décembre, qualifiée de la protection des données personnelles, publiée au bulletin officiel le 21 janvier 2004 et qui est entrée en vigueur 15 jours après sa publication. Le règlement de l'agence andorrane de protection des données du 01 juillet 2004 publié au bulletin officiel le 07 juillet 2004 et qui est entrée en vigueur le lendemain de sa publication. Ce règlement à été entièrement dérogé par le règlement de l'agence andorrane de protection des données du 09 juin 2010 publié au bulletin officiel le 16 juin 2010 et qui est entrée en vigueur 15 jours après sa publication. Correction d'une erreur du règlement de l'agence andorrane de protection des données du 09 juin 2010 publié au bulletin officiel le 30 juin 2010 et qui est entrée en vigueur le lendemain de sa publication. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE nº 108) et le protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données publiée au bulletin officiel le 21 novembre 2007 et qui est entrée en vigueur le 1er septembre 2008	2008 2010 2003 2004 2010		
Austria	The Federal Act concerning the Protection of	1999	2009	Text in EN available.[82]

[82] At http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html

	Personal Data (DSG 2000)			
	The Federal Act on the Organisation of Security Administration and the Exercise of Security Police Services (Security Police Act – Sicherheitspolizeigesetz)	1991	2007	Translation in EN provided.[83]
	The Federal Act on International Police Cooperation (Bundesgesetz über die internationale polizeiliche Kooperation – Polizeikooperationsgesetz)	1997	2009	No text provided.
	The Federal Act on Police Cooperation with Member States of the European Union and with Europol (Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polzeiamt)	2009		No text provided.
Bosnia and Herzegovina	Law on Confidential Data Protection ("Official Gazette of BiH" No. 54/05 12/09)	2009		No text of laws attached.
	Law on Personal Data Protection ("Official Gazette of BiH" No. 49/06 76/11)	2006	2011	(Each of these laws and regulations came into effect on the 8th day after publication in the Official Gazette.)
	Regulation on and the format of keeping records of personal data ("Official Gazette of BiH" No. 52/09)	2009		
	Regulations on keeping and specific measures of technical protection of personal data ("Official Gazette of BiH" br.67/09)	2009		
	Law on Police Officials of BaH (Official Gazette of BaH 27/04, 63/04, 5 / 06, 33/06, 58/06, 15/08, 63/08 and 35/09) (hereinafter The Law) entered into force on 19.06.2004. Any amendment to the Act came into force on 8th day after publication.	2004	2008	
	The Law on Amendments to the Law on Police Officials of BaH (Official Gazette of BaH "br.15/08), which entered into force on 05.03.2008.	2008		
	Law on Control of Weapons and Military Equipment ("Official Gazette of BiH" No. 53/09)	2009		
	Law on Movement and Stay of Aliens and Asylum ("Official Gazette of BiH" No. 36/08)	2008		
	Law on Border Control ("Off. Gazette of BiH" No. 53/09 and 54/10)	2009	2010	

[83] "However, we would like to stress the fact that both English translations are not up to date. Even though there have been no fundamental changes the domestic law has evolved in some parts. Where the existing English translation of a given part of the law was not up to date we provided an answer to the questionnaire by generating an ad-hoc translation of the part concerned."

	Criminal Code ("Off. Gazette BiH "No. 03/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07 08/10)	2003	2010	
	Law on Prevention of Money Laundering and Financing of Terrorist Activities ("Official Gazette of BiH" No. 53/09)	2009		
	Law on the Prevention and Suppression of Drug Abuse ("Official Gazette of BiH" No. 8/06)	2006		
	Law on Protection of Witnesses Under Threat and Vulnerable Witnesses (Official Gazette of BiH, no. 03/03, 21/03, 61/04, 55/05)	2003	2005	
Croatia	Act on Police Affairs and Powers (Official Gazette No. 76/2009)	2009		No text in EN/FR.
	Data Secrecy Act (Official Gazette No. 79/2007 and 86/2012)	2007	2012	Text provided in EN translation.
	State Border Surveillance Act (Official Gazette No. 83/2013)	2013		"Provisional translation" in English.
	Aliens Act (Official Gazette No. 130/11 and 74/2013)	2011	2013	"Provisional translation" in English.
	Security and Intelligence System Act (Official Gazette 79/2006, 105/2006)	2006		Text in EN available.[84]
	Ordinance on Security and Protection of Official Data of the Ministry of Interior (Official Gazette No. 59/2006)	2006		No text in EN/FR.
	Ordinance on Secrecy of Official Data of the Ministry of Interior (Official Gazette No. 107/12)	2012		No text in EN/FR.
	Ordinance on Keeping the Operational Data Collections of the Border police within the National Information System for State Border Control (Official Gazette No. 36/2008)	2008		No text in EN/FR.
	The Act on Personal Data Protection (Official Gazette No. 103/2003, 118/2006, 41/2008 and 130/11; 106/12 consolidated text)	2003	2011	Text provided in EN translation.
	Regulation on the Procedure for Storage and Special Measures Relating to the Technical Protection of Special Categories of Personal Data (Official Gazette No. 139/2004)	2004		Text provided in EN translation.
	Regulation on the Manner of Keeping the Records of Personal Data Filing Systems and the Pertinent Records Form (Official Gazette	2004		Text provided in EN translation.

[84] At https://www.soa.hr/UserFiles/File/Zakon_o_sigurnosno-obavjestajnom_sustavu_RH_eng.pdf

	No. 105/2004) Numerous international (multilateral and bilateral) agreements on police cooperation and on suppression of the criminal activities			
Cyprus	Processing of Personal Data (Protection of Individuals) Law (Law 138(I)/2001) The Republic of Cyprus has ratified the Council of Europe Convention of 28 January 1981 and its Additional Protocol of 8 November 2001 with Ratification Law 28(III)/2001 and Law 30(III)/2003, respectively Circular of the Chief of Police for the implementation of Recommendation No R. (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe by the Cyprus Police The Commissioner has issued guidelines on the processing of personal data on police matters	2001 2007 2004		No texts provided.
Czech Republic	273/2008 Coll. ACT of the Czech National Council regulating the Police of the Czech Republic Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts. Act. No.412/2005 on the Protection of classified information Act. No. 124/1992 on the Military police Act. No. 553/1991 on the municipal police (brought into effect on January 1, 1992) Act No. 326/1999 Coll., on the Residence of Aliens in the Territory of the Czech Republic, as amended; (brought into effect as of January 1, 2000) Act No. 141/1961 Coll., Rules of Criminal Procedure, as amended; (brought into effect as of January 1, 1962 (numerous amendments regulating the use of personal data))	2008 2000 2005 1992 1991 1999 1961		Text provided in English. Text provided in English. No text provided. No text provided. No text provided. Text provided in English. No text provided.
Estonia	Personal Data Protection Act Surveillance Act	2008 1994		Text in EN available.[85] Text in EN available.[86]

[85] Available at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete

	Police and Border Guard Act	2009		Text NOT available in EN.[87]
	Statutes of Police Database	2009		Text NOT available in EN.[88]
	Statutes of National Schengen Information System	2009		Text NOT available in EN.[89]
Finland	Personal Data Act (523/1999)*	1999	2000	*Unofficial translations available[90]
	Act on the Openness of Government Activities (621/1999)*	1999		
	Act on the Processing of Personal Data by the Police (761/2003)	2003		Unofficial translation in English provided.
	Act on the Processing of Personal Data by the Border Guard (579/2005)	2005		No text in EN available.
	Customs Act (1466/1994)	1994		No text in EN available.
France	La loi n°78-17 relative à l'informatique, aux fichiers et aux libertés	1978	2004	Full texts not provided.
	La loi n° 2003-239 pour la sécurité intérieure	2003		
	La loi n°82-890 autorisant l'approbation d'une convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et publiée par décret le 15 novembre 1985	1982		
Federal Republic of Germany (federal level)	Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)			Note: For all legislation of the Federal Republic of Germany there have been prior laws with similar safeguards before the named dates of enactment.
	Act on the Federal Criminal Police Office and the Cooperation between Federal and State Authorities in Criminal Police Matters ("Federal Criminal Police Office Act") (Bundeskriminalamtgesetz, BKAG) (Federal Law Gazette I p. 1650);	1997		Note: The Länder do have similar legislation for their police and security agencies.
	Act on the Federal Police (Bundespolizeigesetz, BPOLG) (Federal Law Gazette I p. 2978, 2979)	1994		
	Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection	1990		

[86] Available at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30011K7&keel=en&pg=1&ptyyp=RT&tyyp=X&query=j%E4litustegevuse

[87] Text in Estonian available at https://www.riigiteataja.ee/akt/122032011011

[88] Text in Estonian available at https://www.riigiteataja.ee/akt/13251596

[89] Text in Estonian available at https://www.riigiteataja.ee/akt/13251567

[90] Unofficial translations available at http://www.tietosuoja.fi/27305.htm

	of the Constitution (Bundesverfassungsschutzgesetz, BVerfSchG) (Federal Law Gazette I, p. 2954, 2970); Military Counterintelligence Service Act (MAD-Gesetz) of 20 December 1990 (Federal Law Gazette I p. 2954, 2977); - the Federal Intelligence Service Act (BND-Gesetz) (Federal Law Gazette I p. 2954, 2979)	 1990		
Hungary	Act XXXIV on Police, 1994 (Police Act) Act CXXV on National Security Agencies, 1995 Act XIX on Criminal Procedure, 1998 Act CV of 2007 on cooperation and exchange of information in the framework of the Convention implementing the Schengen Agreement	1994 1995 1998 2007		Text not provided. Text not provided. Text not provided. Text not available in EN or FR.
Ireland	Data Protection Act 1988 (No. 25 of 1988) Data Protection (Amendment) Act 2003 (No. 6 of 2003) Criminal Justice (Miscellaneous Provisions) Act 2009 Data Protection Code of Practice for An Garda Síochána	1988 2003 2009 2006	2003	The Acts are available on www.irishstatutebook.ie Available on the Garda Siochana website (www.garda.ie) and on the Data Protection Commissioner's website (www.dataprotection.ie)
Italy	Section 53 et seq. of legislative decree no. 196/2003 ("Personal Data Protection Code" – "PDPC")[91] Act no. 121 dated 1 April 1981 Implementing regulations as per Presidential decree no. 378 "Schengen Agreement Ratification Act" (Act no. 388/1993) Decision of the Italian DPA concerning the processing of personal data at/by the Data Processing Centre (DPC) of the Public Security Dept. attached to the Ministry for Home Affairs	2003 1981 1982 1993 2007		Text available in English.[92] Text available in Italian.[93] Text available in Italian.[94] Text available in Italian.[95] Text not provided.

[91] Section 57 of the PDPC provides that a Presidential decree (yet to be issued), following a resolution by the Prime Minister's office acting on the proposal put forward by the Home Affairs Minister, will lay down implementing arrangements for the principles of the Code as for the processing of personal data for police purposes – pursuant to Recommendation R(87)15.
[92] At http://www.garanteprivacy.it/garante/document?ID=1219452
[93] At http://www.interno.it/mininterno/export/sites/default/it/assets/files/15/0583_Legge_1_Aprile_1981_n._121.pdf
[94] At http://www1.interno.it/mininterno/export/sites/default/it/assets/files/14/0632_D.P.R._3_maggio_1982_n._378.pdf
[95] At http://www.interno.gov.it/mininterno/site/it/sezioni/servizi/legislazione/accordi_internazionali/legislazione_359.html (source: Ministry of Interior's website)

Liechtenstein	Act concerning the National Police Force (Police Act; PolG) Ordinance on the routine operations and organization of the National Police Force (PolDOV) Ordinance on the information systems of the National Police Force (PolISV), LR 143.016 Data Protection Act, LR 235.1 Data Protection Ordinance, LR 235.11	1989 2000 2010 2002 2002		English translation of the data protection relevant articles from the Police Act (PolG) and the related ordinance (PolDOV) provided. Note: the translations come from former versions of the laws. No text provided. Text available in EN.[96] Text available in EN.[97]
Lithuania	The Law on Police Activities of the Republic of Lithuania No. VIII-2048 (Official Gazette 2000, No. 90-2777) ("LPA") The Law on Legal Protection of Personal Data No. I-1374 (Official Gazette, 1996, Nr. 63-1479; 2008, Nr. 22-804) ("LLPPD") Order of the Police Commissioner General of 19th December 2005 No. 5-V-835 On approval of action plan of police activities development implementing Schengen acquis	2000 1996 2005		No texts provided.
Luxembourg	La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel [*La loi du 27 juillet 2007, publiée au Mémorial A – N°131 du 8 août 2007 est entrée en vigueur le 1er septembre 2007.] Loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle La loi du 31 mai 1999 sur la Police et l'Inspection générale de la Police La loi du 22 juillet 2008 relative à l'accès des magistrats et officiers de police judiciaire à certains traitements de données à caractère personnel mis en oeuvre par des personnes morales de droit public et portant modification du Code d'instruction criminelle, de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police, et de la loi modifiée du 27 juillet 1997 portant réorganisation de l'administration	2002 2005 1999 2008	2007* 2010	Legislative text provided in FR. Legislative text provided in FR. Legislative text provided in FR. Legislative text provided in FR. Legislative text provided in FR.

[96] At http://www.llv.li/pdf-llv-dss-dpa-fl_en_2009-11-30.pdf
[97] At http://www.llv.li/pdf-llv-dss-dpo-fl_en_2009-11-30.pdf

	pénitentiaire			
	La loi du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police et de l'Inspection générale de la Police à certains traitements de données à caractère personnel mis en oeuvre par des personnes morales de droit public et portant modification du Code d'instruction criminelle et de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police	2009		Legislative text provided in FR.
	Le règlement grand-ducal du 2 octobre 1992 relatif à la creation et à l'exploitation d'une banque de données nominatives de police générale [**Règlement grand-ducal du 9 août 1993 modifiant le règlement grand-ducal du 2 octobre 1992 relatif à la creation et à l'exploitation d'une banque de données nominatives de police générale, Mémorial A – N° 65 du 20 août 1993]	1992	1993**	Legislative text provided in FR.
	Règlement grand-ducal du 1er août 2007 autorisant la création et l'exploitation par la Police d'un système de vidéosurveillance des zones de sécurité	2007		Legislative text provided in FR.
	Règlement ministériel du 27 septembre 2007 portant désignation des zones de sécurité soumises à la vidéosurveillance de la police grand-ducale	2007		Legislative text provided in FR.
	Règlement grand-ducal du 22 juillet 2008 portant exécution de l'article 48-24 du Code d'instruction criminelle et de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police	2008		Legislative text provided in FR.
	Règlement ministériel du 10 novembre 2009 portant désignation des zones de sécurité soumises à la vidéosurveillance de la police grand-ducale	2009		Legislative text provided in FR.
Macedonia	Law on Police (Official gazette of Republic of Macedonia no. 114/06 and 6/09) Law on Internal affairs (Official gazette of Republic of Macedonia no. 92/09, 35/10 and 36/11) Law on Aliens (Official gazette of Republic of Macedonia no. 35/2006, 66/2007, 117/2008, 92/2009 and 156/10) Law on Border Control (Official gazette of RM no. 171/10)			No texts provided.

	Law on National Criminal Intelligence Data Base (Official gazette of Republic of Macedonia no. 120/09)			
Malta	Data Protection (Processing of Personal Data in the Police Sector) Regulations (Subsidiary Legislation 440.05)	2004		Text provided in EN.
Monaco	Loi n°1.165 du 23 décembre 1993 relative à la protection des informations nominatives modifiée par la loi n° 1353 du 8 décembre 2008, entrée en vigueur le 1er avril 2009 Ordonnance souveraine n°2.230 du 19 juin 2009 fixant les conditions d'application de la loi n° 1.165 modifiée Loi du 8 décembre 2008 de Ratification de la Convention 108	1993 2009 2008	2008	
Montenegro	Law on Personal Data Protection Law on Police Law on Ratification of Police Cooperation in South-East Europe Convention Law on Border Control Law on National Security Agency Law on Personal Data Protection Law on International Legal Assistance in Criminal Matters	2008 2005 2008 2009 2005 2008 2008		No texts provided.
Netherlands	The Police Data Act (applicable from 1 January 2008. Until 1 January 2008 the Police Files Act was applicable.) Data Protection Act (Wet bescherming persoonsgegevens) The Intelligence and Security Services Act (applicable to the processing of data by the General Intelligence and Security Service (AIVD).	2007 2002		Legal texts provided in DUTCH (not available in EN or in FR)
Portugal	Article 35 of the Constitution of the Portuguese Republic Law 57/98 on criminal identification Law 67/98 on the protection of personal data Decree-Law 381/98 on the legal regime of the criminal identification Decree-Law 352/99 on Criminal Police computer files Decree-Law 93/2003 on the cooperation between the Criminal Police and the tax	 1998 1998 1998 1999 2003	2005	No texts provided.

	administration on the access and processing of tax information considered relevant to the criminal investigation			
	Decree-Law 35/2004 on the activity of private security	2004		
	Law 41/2004 that implements into the national legal order the European Parliament and of the Council Directive 2002/58/EC, of 12 July, concerning the processing of personal data and the protection of privacy in the electronic communications sector	2004		
	Law 1/2005 on the use of video-cameras by the police forces in public places of common use	2005		
	Law 109/2007 that approves the Law on Cybercrime	2007		
	Law 5/2008 that approves the creation of a database of DNA profiles	2008		
	Law 73/2009 related to the conditions and procedures to be applied in order to set up a criminal data integrated system, pursuant to the Law on Home Security	2009		
	Law 74/2009 on data and criminal information exchanged between the authorities of the EU Member States	2009		
Serbia	Law on Personal Data Protection	2008		Text provided in EN.
	Law on Security - Intelligence Agency	2002		No text provided.
	Law About the Military Security Agency and Military Intelligence Agency	2009		No text provided.
Slovak Republic	Act No. 428/2002 Coll. on Protection of Personal Data (as further amended)	2002		No texts provided.
	Act No. 171/1993 Coll. on the Police Force (as further amended)	1993		
	Act No 46/1993 Coll. on the Slovak Intelligence Service (as further amended)	1993		
	Ordinances of the MoI SR.			
Slovenia	Personal Data Protection Act – Consolidated version	2007		Text provided in EN translation.
	The Police Act – Consolidated version	2009		Text provided in EN translation.[98]
	The Slovene Intelligence and Security Agency Act - Consolidated version	2006		Text provided in EN translation.

[98] Please note that only minor amendments from 2009 to the Police Act are not included in the English version, which has no effect on the topic researched.

Sweden	Personal Data Act (1998:204)	1998		Legislative text provided in EN.
	Personal Data Ordinance (1998:1191)	1998		No text.
	Police Data Act (1998:622)	1998		No text.
	Police Data Ordinance (1999:81)	1999		No text.
	Police Data Act (2010:361)[99]	2010		Legislative text provided in EN.
	Police Data Ordinance (2010:1155)[100]	2010		No text.
	Criminal Records Act (1998:620)	1998		No text.
	Criminal Records Ordinance (1998:1134)	1999		No text.
	Register of Suspected Persons Act (1998:621)	1998		No text.
	Register of Suspected Persons Ordinance (1999:1135)	1999		No text.
	Schengen Information System Act (2000:344)	2000		No text.
	Schengen Information System Ordinance (2000:836)	2000		No text.
	Act (2010:362) on the Police General Investigative Database[101]	2010		No text.
	Ordinance (2010:1157) on the Police General Investigative Database[102]	2010		No text.
	Secret telephone surveillance, secret wire-tapping and secret camera surveillance, Chapter 27 of the Code of Judicial Procedure, enacted in 18 July 1942, entered into force 1 January 1948.[103]	1942	1995	No text provided.
	Secret Room Surveillance Act (2007:978), enacted on 22 November 2007, entered into force on 1 January 2008	2007		No text provided.
	Video Surveillance Act (1998:150) enacted on 2 April 1998, entered into force on 1 July 1998.	1998		No text provided.
Switzerland (Lois federales)	Loi fédérale sur la protection des données (LPD, Recueil systématique des actes législatifs fédéraux (RS): 235.1)	1992		Text available online in FR.[104] Official translation provided.
	Echange de lettres des 7 mars 2006/22	2006–7		Text available online in FR.

[99] Will enter into force on 1 March 2012.
[100] Will enter into force on 1 March 2012.
[101] Will enter into force on 1 March 2012.
[102] Will enter into force on 1 March 2012.
[103] The rules about technical surveillance have been amended several times since they were first introduced (secret wire-tapping in 1948, secret telephone surveillance in 1989 and secret camera surveillance in 1995).
[104] All legislative texts saved in .pdf format to my hard-drive.

	novembre 2007 entre la Suisse et l'Office européen de police Europol concernant l'extension de l'Accord du 24 septembre 2004 entre la Confédération suisse et l'Office européen de police aux domaines de la criminalité figurant dans le présent échange de lettres (RS 0.362.21)			
	Arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'Union européenne sur la reprise de la décision-cadre 2006/960/JAI relative à la simplification de l'échange d'informations entre les services répressifs (Développement de l'acquis de Schengen) (Projet) 8149	2008		Text available online in FR.
	Arrêté fédéral portant approbation et mise en œuvre de l'échange de notes du 14 janvier 2009 entre la Suisse et l'Union européenne sur la reprise de la décisioncadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (RS 0.362.380.041)	2009		Text available online in FR.
	Loi fédérale sur l'échange d'informations Schengen (LEIS ; RS 362.2), prise en application de la décision-cadre 2006/960/JAI du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'UE	2009		Text available online in FR.
	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS 120)	1997		Text available online in FR.
	Ordonnance sur les mesures de police administrative et les systèmes d'information de l'Office fédéral de la police (OMSI, RS 120.52)	2009		Text available online in FR.
	Ordonnance du DFJP sur les champs de données et les droits d'accès au système ISIS (O ISIS, RS 120.31)	2007		Text available online in FR.
	Loi fédérale sur les systèmes d'informations de police de la Confédération (LSIP; RS 361)	2008		Text available online in FR.
	Loi fédérale sur la police[105] (LPol) en projet qui remplacera les dispositions relatives aux	2009		*[106]

[105] Le projet de loi fédérale sur les tâches de police de la Confédération (LPol) a été mis en consultation en été 2009. Le Conseil fédéral a décidé d'attendre de disposer du rapport clarifiant la répartition des compétences dans le domaine de la sécurité intérieure avant d'arrêter la suite de la procédure concernant les travaux d'élaboration d'une loi fédérale sur les tâches de police de la Confédération.

	traitements des données personnelles par les autorités de police éparpillées dans diverses lois fédérales (cf. LMSI, LSIP, LEIS et autres)			
	Ordonnance sur le système de recherches informatisées de police (Ordonnance RIPOL; RS 361.0)	2008		Text available online in FR.
	Ordonnance sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC, RS 121.2)	2009		Text available online in FR.
	Accord du 26 octobre 2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (avec annexes et acte final, RS 0.362.31)	2004		Text available online in FR.
	Arrêté fédéral portant approbation et mise en œuvre des accords bilatéraux d'association à l'Espace Schengen et à l'Espace Dublin (RS 362)	2004		
	Décision du Conseil du 5 juin 2008 sur l'application à la Confédération suisse des dispositions de l'acquis de Schengen relatives au système d'information Schengen (2008/421/CE)	2008		
	Développements de l'acquis Schengen, comme par ex. Arrêté fédéral du 13 juin 2008 portant approbation des échanges de notes entre la Suisse et l'Union européenne concernant la reprise des bases légales visant l'adaptation du système	2008		*[107]
Ukraine	Law #2297-VI 01.06.2010 "On Protection of Personal Data" (in force from 01.01.2011)	2010		No texts provided.
	Law #2438-VI 06.07.2010 "On Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flows'' (in force from 01.01.2011)	2010		
	Law № 565-XII "On Militia" of 20.12.1990	1990		
	Law № 2657-XII "On Information" of	1992		

[106] * projet LPol, FF 2009 7680 du 08.12.2009: http://www.admin.ch/ch/f/gg/pc/ind2009.html

[107] * Feuille fédérale, FF, 2008 4821, Recueil officiel, RO, 2008 5111, http://www.admin.ch/ch/f/ff/index.html

	2.10.1992 (new wording entered into force 10.05.2011) Law № 2939-VI "On Access to Public Information" of 13.01.2011 Law № 2135-XII "On Operative and Investigative Activities" of 18.02.1992 Law № 80/94-BP "On Information Protection in Information and Telecommunication Systems " of 5.07.1994 Law № 3855-XII "On State Secret" of 21.01.1994 President's Decree "On the Statute of the State Service of Ukraine on personal data protection" of 06.04.2011 N 39/2011 (in force since 18.04.2011) Decree of the Cabinet of Ministers of Ukraine "On approval of the Statute of the State register of the personal data bases and the rules of its procedure" of 25.05.2011 N616 (in force since 21.06.2011) Decree of the Ministry of Internal Affairs of Ukraine of 09.06.2011 "On adoption of the List of data which belong to the confidential information in the system of the Ministry of Internal Affairs"	2011 1992 1994 1994 2011 2011 2011		
United Kingdom	UK Data Protection Act 1998 UK Human Rights Act 1998 The Regulation of Investigatory Powers Act 2000 Anti Social Behaviour Act 2003 Protection of Vulnerable Groups Act and Public Protection.	1998 1998 2000 2003 2007		Text available. Text available. Text available.

Annex C: Tables

Table 2
Specific definitions of "personal data for police purposes"

	Q.4 How does the law of your country define personal data "for police purposes"? (R87(15) 'Scope and definitions'; Explanatory Memorandum para. 22)
Bosnia & Herzegovina	"Processing of personal data in the police services means the processing of personal data carried out by the police authorities to prevent and combat crime and maintain public order." Law on Police Officials of Bosnia and Herzegovina, Article 33.a. (1).
Finland	Act 761/2003 on the Processing of Personal Data by the Police does not provide for a definition as such but according to section 1, the Act applies to the automatic and other processing of personal data needed for the performance of duties as referred to in section 1 of the Police Act (493/1995), where the personal data constitutes or is intended to constitute a personal data file or part thereof.
France	«qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique» ; «ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.» [concerning state security, defence or public security'; 'or that concern the prevention, investigation, detection or prosecution of criminal offences or the enforcement of criminal convictions or security measures] L'article 26 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par la loi N° 2004-501 du 6 août 2004.
Germany	Personal data, as far as their storage or use is necessary for fulfilling the tasks of the police authorities. Section 7 subsection 1 of the Federal Criminal Police Office Act et.al.
Italy	Section 53 of the Personal Data Protection Code, which is part of a chapter addressing "Processing operations by the police", refers specifically to "the processing of personal data that is carried out either by the Data Processing Centre at the Public Security Department or by the police with regard to the data that are intended to be transferred to said centre under the law, or by other public bodies or public security entities for the purpose of protecting public order and security, the prevention, detection or suppression of offences as expressly provided for by laws that specifically refer to such processing". Section 53 of the Personal Data Protection Code.
Malta	"for Police Purposes" means all the tasks which the police (or other public entities, authorities or bodies exercising police powers) must perform for the prevention and suppression of criminal offences or the maintenance of public order;" Subsidiary Legislation 440.05 – Data Protection (Processing of Personal Data in the Police Sector) Regulations, Article 2.
Monaco	Toute donnée collectée dans le cadre de l'ordonnance souveraine n°765 du 13 novembre 2006 modifiée fixant les missions de la police, dans le respect de la loi n° 1.165 modifiée [All data collected as part of the Sovereign Order No. 765 of 13 November 2006 fixing the objectives of policing, in accordance with Law No. 1165 as amended.]
The Netherlands	"(a) police data: any information relating to an identified or identifiable natural person that is being processed in the exercise of the police task; (b) police task: the tasks, meant in the articles 2 and 6 of the Police Act 1993." Article 1 Police Data Act.
Portugal	Articles 3 and 8(2/3) of the Law 67/98, of 26 October: any information, regardless of its nature and irrespective of its support, including sound and image, related to an identified or identifiable person; is considered an identifiable person, whoever may be directly or indirectly identified through reference to an ID number or to one or more specific elements pertaining to his/her physical, physiologic, psychical, economical, cultural or social identity; The processing of personal data related to suspicions of illegal activities, to criminal offences, administrative offences and to decisions on penalties, security measures, fines and ancillary sanctions to be applied may be authorized by CNPD, once the rules on data protection and the safeguard of the information are observed, whenever such processing is deemed necessary for the pursuit of the legitimate purposes of the competent person and insofar as the rights,

	freedoms and guarantees of the data subject do not prevail; The processing of personal data for police investigation purposes should be restricted to what is strictly necessary to prevent a real danger or to repress a certain offence from occurring; such processing may be done in the course of the duties foreseen in the organic statute or in any other legal provision or yet on the terms of an agreement or international convention of which Portugal is part.
Slovakia	Art 69 (1), 69(2) of the Act No. 171/1993 on the Police Force: The Police Force processes information pursuant to this Act and to special Acts as well as personal data collected during fulfilment of the Police Force's duties including information and personal data provided from the abroad within the extent necessary for the fulfilment of those duties. If required for fulfilment of the duties, the Police Force is authorized to prepare audio, visual and other records of public accessible areas; visual or other records of police action or police activity course.
Sweden	All personal data is defined as all kinds of information that directly or indirectly may be referable to a natural person who is alive. The definition of "police purposes": Police Data Act, chapter 2, section 7: "Personal data may be processed if necessary in order to 1. anticipate, prevent or detect criminal activities; 2. investigate or take action against an offence, or 3. fulfil obligations ensuing from international commitments." Cf. Also chapter 2 section 2 of the Police Data Act (2010:361) referring to sec 3 Personal Data Act (1998:204)
Switzerland	«La LPD définit les données personnelles comme étant « toutes les informations qui se rapportent à une personne identifiée ou identifiable».Art. 3 lit. a LPD (section 1). [The Federal Act of 19 June 1992 on Data Protection defines personal data as "all information relating to an identified or identifiable person."] Art. 3 (a) LPD. «La LSIP prévoit que « [l]es systèmes d'information de police sont mis en œuvre pour permettre aux autorités exerçant des fonctions de poursuite pénale, de police et de maintien de la sécurité intérieure d'accomplir leurs tâches.» [The Federal Act of 13 June 2008 on the Information Systems of the Police of the Confederation provides that "police information systems are implemented to enable the authorities exercising functions of criminal prosecution, police and maintenance of internal security to perform their duties.] Art.3 al.1 LSIP.] «[…] [L]es autorités fédérales de police sont habilitées à traiter des données sensibles et des profils de la personnalité et à les communiquer aux autorités cantonales de police et de poursuite pénale ainsi qu'à d'autres autorités suisses et étrangères. Les données personnelles peuvent être traitées dans la mesure où elles s'avèrent nécessaires à l'exécution de tâches légales.» ["[...] The federal police are authorised to process sensitive data and personality profiles and communicate them to the cantonal police and law enforcement and other authorities in Switzerland and abroad. Personal data can be processed to the extent they are necessary to perform legal tasks."] Art. 3 al.2 LSIP. «La base légale pour le traitement des données personnelles dans la LMSI prévoit que «[d]ans le cadre de mesures de protection de personnes et d'immeubles […], les organes de sûreté peuvent également traiter les informations nécessaires pour garantir la sécurité de personnes, d'organisations ou de manifestations menacées.» [The legal basis for the processing of personal data in the Federal Act of 21 March 1997 establishing measures for the maintenance of internal security (LMSI) provides that "in the context of measures to protect people and building [...], the organs of security can also process information the necessary information to ensure the safety of persons, organisations or events threatened."] Art. 3 al. 4 LMSI. «Le code de police en projet prévoit une base légale expresse pour le traitement des données personnelles: «Fedpol [Office fédéral de la police] traite les informations nécessaires aux mesures de protection de personnes et de bâtiments […]». Art. 75 Lpol. [The Federal Act on Police planned to replace the provisions governing the processing of personal data by law enforcement agencies scattered throughout various federal statutes (LPol) provides an express legal basis for the processing of

	personal data: “Fedpol [Federal Police Office] processes the information necessary for the measures of protection of persons and buildings [...]”. Art.75 LPol.] «La LEIS entend par informations « tous les types de données dont disposent les autorités de poursuite pénale ». [For the purposes of the Federal Act of 12 June 2009 on the Schengen information exchange (LEIS, SR 362.2), taken under the Framework Decision 2006/960/JHA 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (LEIS) information shall mean “all types of data available to the prosecuting authorities.”] Art. 2 al. 1 LEIS.
The former Yugoslav Republic of Macedonia	The Law on Police stipulates in Article 66 that the police collects, process, analyses, use, evaluates, transfers, stores and erases data, process personal data under conditions and means with this Law and keeps archive for personal and other data. Personal data essential for detection and prevention of criminal offences and misdemeanours, as well as for detection and apprehension of the perpetrators.

Table 3
The responsible body or controller of the file

	Q.5 Who in your country is the “responsible body” (authority, service or other public body) which is competent according to national law to decide on the purpose of an automated file, the categories of personal data which must be stored and the operations which are to be applied to them (i.e. the controller of the police files)? *(R(87)15 ‘Scope and definitions’; Explanatory Memorandum para. 25)*
	The overwhelming majority of countries responded that the controller is the Ministry of the Interior or the Police themselves.

Table 4
Countries extending principles of R(87)15 to manual processing

	Q.6 Has your country extended the principles contained in Recommendation R(87)15 to personal data undergoing manual processing? *(R(87)15 ‘Scope and definitions’; Explanatory Memorandum para. 26–27)*
Yes	30 countries surveyed / 28 responded ‘yes’.
No	The Netherlands
Unclear	Serbia

Table 5
Aim of manual processing of personal data by police

	Q.7 If not, does manual processing of data take place? What is the aim of such processing? *(R(87)15 ‘Scope and definitions’; Explanatory Memorandum para. 26–27)*
The Netherlands	“Manual processing will presumably only take place in the form of notes taken down by the police on the road, but as most notes will be taken down electronically this will be rare nowadays.”

Table 6a
Extending R(87)15 beyond natural persons

	Q.8 Has your country extended the principles contained in Recommendation R(87)15 to data relating to groups of persons, associations, foundations, companies, corporations or any other body

	consisting directly or indirectly of individuals, whether or not such bodies possess legal personality? *(R(87)15 'Scope and definitions'; Explanatory Memorandum para. 28)*
Yes	Albania, Austria, Bosnia and Herzegovina, Croatia, Estonia, Hungary, Liechtenstein, Monaco, Switzerland and Ukraine.
Yes, but only if such bodies possess legal personality	Montenegro, Sweden and UK
No	Andorra, Cyprus, Czech Republic, Finland, Germany, Ireland, Italy, Lithuania, Luxembourg, the Netherlands, Portugal, Slovak Republic and Slovenia
Unclear answers	Malta, Serbia and the former Yugoslav Republic of Macedonia
No answer	France

Table 6b

Andorra	**L'article 7 de la Loi 15/2003 de protection de données personnelles exclu du cadre de la Loi les données de personnes physiques liées à leur activité professionnelle ou commerciale, dans les circonstances suivantes :** **a) Données de personnel de personnes juridiques ou d'établissements commerciaux ou professionnels, lorsque les informations liées à la personne physique font uniquement référence à son appartenance à l'entreprise ou à l'établissement, ou à leur qualité professionnelle dans l'entreprise ou l'établissement.** **b) Données de personnes physiques appartenant à des collectifs professionnels, à condition que les données fassent uniquement référence à l'activité professionnelle de la personne et à son appartenance à un collectif professionnel donné.** **c) Données de professionnels autonomes ou d'établissements professionnels ou commerciaux, lorsque les données font uniquement référence à leur activité professionnelle ou commerciale.** [Article 7 of Law 15/2003 on the protection of personal data excludes from its scope the data of physical persons related to their commercial or professional activities, in the following circumstances: a) personal data of legal persons or commercial establishments or professionals, when the information related to the natural person refers only to that individual's belonging to the business or establishment, or to their professional capacity in the business or the establishment. b) Data of individuals belonging to professional groups, provided that the data only make reference to the professional activity of the individual and to his belonging to a given professional group. c) Data of independent professionals or professional or commercial establishments, where the data refer only to their professional or commercial activity.]
Finland	Act 761/2003 mainly provides for the processing of personal data. The processing of data relating to the categories referred to in this question is mainly covered by the Act on the Openness of the Government Activities (621/1999).

Table 7
Countries extending R(87)15 to data collected for state security purposes

	Q.9 Has your country extended any of the principles of R(87)15 to the collection, storage and use of personal data for purposes of state security? *(R(87)15 'Scope and definitions'; Explanatory Memorandum para. 29)*

Yes	Albania, Croatia, Czech Republic, Estonia, Finland, France, Germany, Hungary, Italy, Liechtenstein, Luxembourg, Monaco, Montenegro, Portugal, Slovenia, Sweden, Switzerland, Ukraine and UK
State security purposes are 'not excluded'	Austria, Cyprus
No	Andorra, Bosnia & Herzegovina, Ireland and Malta
No, but processing of personal data for state security is regulated by a separate law	The Netherlands, Slovak Republic
Unclear answer/no response	Lithuania, Serbia, and The former Yugoslav Republic of Macedonia.

Table 8
General-purpose or Purpose-specific ISA for police data

	Q.10 Principle 1.1: What is the name of the independent supervisory authority outside the police sector which is responsible for ensuring respect for the principles contained in Recommendation R(87)15? *(R(87)15 Principle 1.1; Explanatory Memorandum para. 31–33)*
Albania	Commissioner for the Personal Data Protection, www.kmdp.al
Andorra	Agence de protection des données de la Principauté d'Andorre, www.apda.ad
Austria	Data Protection Commission (Datenschutzkommission), https://www.dsk.gv.at/DesktopDefault.aspx?alias=dsken
Bosnia and Herzegovina	Personal Data Protection Agency in Bosnia and Herzegovina
Croatia	Croatian Personal Data Protection Agency, www.azop.hr
Cyprus	Office of the Cypriot commissioner for personal data protection, www.dataprotection.gov.cy
Czech Republic	Office for personal data protection, www.uoou.cz
Estonia	Estonian data protection agency, www.aki.ee
Finland	Office of the Data Protection Ombudsman, www.tietosuoja.fi
France	CNIL - Commission Nationale de l'Informatique et des Libertés, www.cnil.fr/
Germany	The Federal Commissioner for Data Protection and Freedom of Information, http://www.bfdi.bund.de/EN/Home/homepage_node.html
Hungary	Parliamentary Commissioner for Data Protection and Freedom of Information, http://abiweb.obh.hu/abi/
Ireland	Data Protection Commissioner, www.dataprotection.ie
Italy	Garante per la Protezione dei Dati Personali, http://www.garanteprivacy.it/
Liechtenstein	Data Protection Office of the Principality of Liechtenstein, www.dss.llv.li
Lithuania	Lithuanian data protection agency, www.ada.lt
Luxembourg	Commission nationale pour la protection des données, www.cnpd.lu/de
Macedonia	Data Protection Commission
Malta	Data Protection Commission, www.dataprotection.gov.mt
Monaco	CCIN - Commission de contrôle des informations nominatives, www.ccin.mc
Montenegro	Personal Data Protection Agency
Netherlands	Dutch Data Protection Agency, www.cbpweb.nl
Portugal	Portuguese Data Protection Agency, www.cnpd.pt
Serbia	Commissioner for Information of Public Importance and Personal Data Protection
Slovak Republic	Data Protection Authority, www.dataprotection.gov.sk
Slovenia	Information Commissioner, www.ip-rs.si
Sweden	Swedish Data Inspection Board, www.datainspektionen.se The Swedish Commission on Security and Integrity Protection, www.sakint.se
Switzerland	Le Préposé fédéral à la protection des données et à la transparence (PFPDT), www.leprepose.ch / www.edoeb.admin.ch

	[The Federal Data Protection and Information Commissioner (FDPIC)] Les autorités de protection des données des cantons sont chargées de la surveillance des données personnelles traitées par les autorités (notamment polices) cantonales et communales. [The data protection authorities of the cantons are responsible for the protection of personal data processed by the cantonal and communal authorities (including the police).].
Ukraine	The State Service of Ukraine on Personal Data Protection
United Kingdom	Information Commissioner's Office, www.ico.gov.uk

Table 9
Where some form of Privacy Impact Assessments are carried out

	Q.11 Principle 1.2: Is a privacy/data protection impact assessment undertaken when new technical means for data processing are introduced, to ensure that their use complies with the spirit of existing data protection legislation? *(R87(15) Principle 1.2; Explanatory Memorandum para. 34)*
Yes	Albania; Bosnia and Herzegovina; Estonia; France; Liechtenstein; Luxembourg; Monaco; Portugal; Slovak Republic; Sweden; The former Yugoslav Republic of Macedonia; Ukraine.
No	Andorra, Austria, Croatia, Germany, Ireland, Italy, Lithuania, Malta, the Netherlands, Slovenia, Switzerland.
No information	Hungary.
No answer	Cyprus, Finland, Serbia.
Unclear answer	Czech Republic, Montenegro.

Table 10
Countries where other reasonable measures are taken

	Q.12 If a privacy/data protection impact assessment is not undertaken, what other reasonable measures are taken to ensure compliance? *(R87(15) Principle 1.2; Explanatory Memorandum para. 34)*
Andorra	**Des évaluations de l'incidence sur la protection des données et de la vie privée sont réalisées à travers de consultations à l'agence andorrane de protection des données ainsi qu'aux autorités judiciaires du parquet.** [Assessments of the impact on data protection and privacy are carried out through consultations with the Andorran agency for data protection and the judicial authorities of the prosecution.]
Austria	**Austria has instituted an "Advisory Data Protection Council" at the Federal Chancellery.[108] The Data Protection Council has the power to advise government on measures affecting data protection.**
Cyprus	In Cyprus the Commissioner for the Protection of Personal Data may monitor the implementation of any law relating to the processing of personal data[109] and has the power to grant or withhold "license for combination."[110]
Germany	I. New technical means for processing personal data can only be introduced on the basis of relevant legislation. In order to ensure conformity with existing data protection legislation, the legislator will involve the Federal Commissioner for Data Protection and Freedom of Information, among others. Section 21 of the Joint Rules of Procedure of the Federal Ministries II. Further processing of personal data by the Federal Criminal Police Office with special technical means, such as automated data files, requires a special legal basis specifying the purpose of such processing („Opening order") irrespective of whether it is done in the context of threat prevention or

[108] § 41 para.1 of the Federal Act concerning the Protection of Personal Data - DSG 2000.

[109] Section 18(1) of Law 138(I)/2001.

[110] Section 8 of Law 138(I)/2001.

	criminal prosecution. To ensure compliance with data protection requirements, the law stipulates that opening orders relating to terrorism-related threat prevention measures must include: 1. the name of the data file; 2. the legal basis and purpose of the data file; 3. the group of individuals on whom data are being stored; 4. the type of personal data to be stored; 5. the types of personal data serving to open the data file; 6. the delivery or entry of the data to be stored; 7. the preconditions under which personal data stored in the data file are to be transferred to which recipients and using which procedure; 8. the time limits within which data must be reviewed and length of storage; 9. the logging procedure. Any opening order requires the consent of the Federal Ministry of the Interior as the supervisory authority for technical matters (Section 34 subsection 1 of the Federal Criminal Police Office Act). The Federal Commissioner for Data Protection and Freedom of Information shall be consulted before the order opening a data file is adopted. Section 34 of the Federal Criminal Police Office Act The following applies to data processing for the purpose of criminal prosecution: In an opening order the controller of the data file shall determine for each automated data file: 1.the name of the data file; 2. the legal basis and purpose of the data file; 3. the group of individuals whose data will be processed in the data file; 4. the type of data to be processed; 5. the delivery or entry of the data to be processed; 6. the preconditions under which personal data processed in the data file are to be transferred to which recipients and using which procedure; 7. the time limits within which data must be reviewed and length of storage. Section 483 et seqq. of the Code of Criminal Procedure The establishment of an automated procedure enabling the transmission of personal data by retrieval requires the prior consent of the Federal Ministry of the Interior and the prior notification of the Federal Commissioner for Data Protection and Freedom of Information. Section 488 subsection 2 of the Code of Criminal Procedure
Hungary	Inspections and recommendations.
Ireland	The Garda Síochána liaise with the office of the Data Protection Commissioner for advice and guidance when necessary and Garda employees logging onto the Garda national police database, PULSE, must acknowledge their obligations under data protection legislation.
Italy	Any processing that is more likely to be prejudicial to data subjects –with particular regard to genetic and/or biometric databases, location-based processing, databases relying on specific information processing techniques, and the introduction of certain types of technology - must be compliant with such measures and arrangements as may be set forth by the *Garante* to safeguard data subjects following a prior checking procedure (DPC, section 55).
Switzerland	La LPD et l'Ordonnance fédérale y relative (OLPD) exigent que les mesures techniques et organisationnelles de sécurité et de protection des données personnelles traitées et des réseaux ou systèmes mis à disposition soient actuelles et adéquates pour assurer la confidentialité, la disponibilité et l'intégrité des données. Il est nécessaire d'intégrer les exigences techniques et organisationnelles dès le début du développement d'un projet informatique. [The Federal Act of 19 June 1992 on the protection of data (LPD) and the Federal Ordinance relating thereto (OLPD) require that measures ensuring technical and organizational security and protection of data processed and of networks or systems available be up-to-date and adequate to ensure the confidentiality, availability and integrity of data. It is necessary to integrate the technical and organizational requirements early in the development of an IT project.]

Table 11a
Obligatory consultation of the DPA in case of automated processing

	Q.13 Principle 1.3: Is the "responsible body" obliged to consult the supervisory authority in advance in any case where the introduction of automated processing methods raises questions about the application of R(87)15? *(R87(15) Principle 1.3; Explanatory Memorandum para. 35)*
Yes	Bosnia Herzegovina; Cyprus; Estonia; France; Germany; Finland; Hungary; Liechtenstein; Luxembourg; Monaco; Portugal; Slovak Republic.
Yes, in specified circumstances or cases	Italy; Lithuania; Sweden.
Yes (with exceptions)	Austria.
No	Albania; Andorra; Croatia; Czech Republic; Ireland; the Netherlands; Slovenia; Switzerland; The former Yugoslav Republic of Macedonia; Ukraine; UK.
No answer	Malta; Serbia.
Unclear	Montenegro.

Table 11b

Andorra	Le règlement de l'agence andorrane de protection des données du 09 juin 2010, dans son article 25 établit les fonctions consultatives de l'agence : 1. prononcer les instructions et recommandations nécessaires pour adapter les traitements des données personnelles aux principes de la législation en vigueur en matière de sécurisation de données personnelles ; 2.émettre des rapports, à caractère de conseil, dans le cas où ils seraient demandés, sur les projets de loi, les projets de dispositions normatives élaborées par le Gouvernement en vertu d'une délégation législative, les projets de règlements ou des dispositions à caractère général touchant la sécurisation de données à caractère personnel ; 3.émettre ses opinions sur d'autres lois ou règlements qui touchent la vie privée des personnes physiques et les traitements et la sécurité des données à caractère personnel. À la pratique des consultations et rapports sont élaborés chaque année par l'agence andorrane de protection des données. [The Regulation of 9 June 2010 0f the Andorran Agency for Data Protection, at Article 25, establishes the advisory functions of the agency: 1. to pronounce the necessary instructions and recommendations to adapt the processing of personal data to the principles of the legislation in force in the matter of the security of personal data; 2. to issue reports, advisory in nature, in the event they are requested, on bills, draft normative standards developed by the Government pursuant to legislative delegation, draft regulations or provisions of a general character affecting the security of personal data; 3. to issue its opinions on other laws or regulations that affect the privacy of individuals and the treatment and the security of personal data. In practice consultations and reports are prepared annually by the Andorran Agency for Data Protection.]
Finland	The supervisory authority is consulted by means of informing the establishment of the relevant data files. Permanent personal data files (data systems) are established by amending the relevant legislation, and the supervisory authority is heard in the course of the legislative procedure in respect of the entire Government bill, particularly the provisions on data protection (including details of the new data files or information system). In respect of temporary or manually maintained personal data files for nationwide use as referred to in section 6, the decision on establishing a file and any significant alteration to it shall be notified to the Data Protection Ombudsman no later than one month before the file is established or altered (section 8(2) of Act 731/2003). Under section 36 of the Personal Data Act, the controller shall notify the Data Protection Ombudsman of automated data processing by sending a description of the file to that authority.
Germany	It is mandatory to involve the Federal Commissioner for Data Protection and Freedom of Information both in a legislative procedure (e.g. for introducing new

	technical data processing powers) and for opening automated data files.
Italy	In Italy any processing that is more likely to be prejudicial to data subjects must be compliant with such measures and arrangements as may be set forth by the *Garante* to safeguard data subjects following a prior checking procedure.[111] Moreover, the Prime Minister and all Ministers are required to seek advice from the *Garante* when drafting regulatory instruments and/or administrative decisions that are liable to impact on the matters regulated by the Personal Data Protection Code.[112]
Liechtenstein	Art. 20 Para. 2 Data Protection Ordinance: The responsible authorities ***shall*** notify the data protection officer or, if there is none, the Data Protection Office without delay of all projects for the automated processing of personal data so that data protection requirements can be taken into account immediately. The German (applicable) version is formulated in a way, that it is mandatory for the responsible authority to consult the Data Protection Office.
Switzerland	L'organe fédéral responsable (en l'espèce fedpol) a l'obligation légale de soumettre à son conseiller à la protection des données (service juridique de fedpol) tous ses projets de traitements automatisés de données personnelles dès le début de leur développement et à défaut au PFPDT. De plus, l'organe fédéral a l'obligation légale de déclarer les fichiers à l'autorité de contrôle, le PFPDT, pour enregistrement. A cet égard, le PFPDT n'a toutefois pas le pouvoir d'autoriser ou de refuser un nouveau système d'information ou l'introduction de nouveaux procédés de traitement avant leur mise en place. Dans ce sens il ne s'agit pas d'une notification systématique. Cela étant, le PFPDT est consulté lorsque le traitement implique la création ou la modification de bases légales (Art. 11a LPD et Art. 20 OLPD). Observation: Il s'agit d'une réglementation générale de protection des données valable pour tous les domaines, non seulement les traitements de données à des fins de police. De plus, en pratique, le PFPDT est consulté dans le cadre du processus législatif fédéral lors qu'il y a adoption ou modification d'une loi ou d'une ordonnance fédérale qui concerne des aspects de protection des données. [The responsible federal agency (in this case fedpol) has a legal obligation to submit to their data protection advisor (fedpol legal service) all projects of automated processing of personal data from the beginning of their development and failing this, to the Federal Data Protection and Information Commissioner - FDPIC (Le Préposé fédéral à la protection des données et à la transparence – PFPDT). In addition, the federal body has a legal obligation to notify files to the supervisory authority, the FDPIC, for registration. In this respect, the FDPIC has not the power to authorise or to refuse a new information systems or the introduction of new means of data processing prior to implementation. In this sense, it is not a routine notification. However, the FDPIC is consulted when the processing involves the creation or a modification in the legal bases. (Comment: This is a general regulation of data protection valid for all areas, not only data processing for police purposes.)[113] In Switzerland, moreover, in practice, the PFPDT is consulted in the federal legislative process when a federal law or ordinance on aspects of data protection is adopted or amended.]
Canton of Basel-Stadt	§ 13 IDG Preliminary assessment (not yet in force) 1 If, because of the nature of the processing or of the data, the processing is likely to pose particular risks for the rights or the freedom of the person concerned, this processing must be submitted to the data protection officer for a preliminary check. 2 The data protection officer will produce an evaluation in the form of a recommendation in accordance with § 46. § 13 Gesetz vom 9. Juni 2010 über die Information und den Datenschutz, Informations- und Datenschutzgesetz, IDG.

Table 12

111 Section 55 of the Personal Data Protection Code.

112 Section 154(4) of the Personal Data Protection Code.

113 Art. 11a LPD et Art. 20 OLPD.

PIA not legally required but mandatory practice

	Q.14 If not legally obliged, is such consultation considered to be a mandatory practice? *(R87(15) Principle 1.3; Explanatory Memorandum para. 35)*
Yes	Czech Republic; The former Yugoslav Republic of Macedonia.
Implemented in practice	Ireland; Slovenia; Switzerland.
No	Croatia; Lithuania; Ukraine.
No answer	Albania; Malta; Serbia; UK.

Table 13a
Obligation to notify permanent automated police files to DPA

	Q.15 Principle 1.4: Is there an obligation in your country to notify permanent automated police files to the supervisory authority? *(R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 36–38)* *Q.16 If yes, what should the notification specify?* *(R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 36–38)*
No	Albania (police purposes exempted); Estonia; Germany; Italy; Luxembourg; the Netherlands; Slovak Republic; Sweden
Yes	Andorra, Austria; Bosnia Herzegovina; Cyprus; Finland; France (although the notion of permanent files doesn't exist in French law); Germany, Hungary; Ireland; Liechtenstein; Lithuania; Macedonia; Malta; Monaco; Portugal; Serbia; Slovenia; Switzerland; Ukraine; UK
Qualified yes	Croatia
Unclear	Czech Republic
No answer	Montenegro

Table 13b

Italy	Notification is only mandatory in respect of the processing operations mentioned in section 37 of the Code. However, section 53 requires the Minister for Home Affairs to specify, by a decree, any non-occasional processing operations for police purposes that are performed with the help of electronic tools along with the respective controllers. Additionally, section 175 of the Code requires the *Garante* to be informed of any processing operation that is carried out to feed information acquired in the course of administrative activities into the DPC of the police as well as in order to establish connections/links between the DPC and other databases.
Luxembourg	According to Article 12 (1) (a) of the Law of 2 August 2002, the treatments provided for in Article 17 are exempted from the preliminary formalities.
The Netherlands	But automated police files must be in conformity with art. 8, 9, 10, 12, 13 Police Data Act.
Sweden	The legal basis for the automated file is pursuant to specific legislation.
Croatia	Records on personal data filing systems maintained by the authorised state bodies within a framework of personal data processing activities for the purposes of state security, defence and the prevention of occurrences determined in the National Security Strategy of the Republic of Croatia as security risks (corruption, organized crime, terrorism) do not have to be compiled in the Register.

Table 14
Obligation to notify manual police files to supervisory authority

	Q.17 Is there an obligation in your country to notify manual police files to the supervisory authority and, if so, what should the notification specify? *(R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 38–39)*
No	Albania; Estonia; Germany; Lithuania; Luxembourg; Monaco; the Netherlands; Slovak Republic; Sweden

Yes	Andorra, Bosnia and Herzegovina; Cyprus; Finland; France; Hungary; Ireland; Liechtenstein; Macedonia; Malta; Slovenia; Switzerland; Ukraine; UK
Qualified Yes	Austria; Croatia; Italy
Unclear answers	Czech Republic, Portugal and Serbia

Table 15
Central requirement to which manual police files must conform

	Q.18 If not, has a general description been drawn up at central level to which manual police files are required to conform? (R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 38–39)
Albania	No answer
Estonia	Yes [no further details provided.]
Germany	General requirements applying to the processing of personal data in (manual) data files are governed by the Federal Criminal Police Office Act and the Statutory Instrument on the Types of Data which may be stored under Sections 8 and 9 of the BKAG. Section 7 et seqq. of the Federal Criminal Police Office Act in conjunction with the Statutory Instrument of 4 June 2010, Federal Law Gazette I 2010, p. 716. I 2010, S. 716.
Lithuania	No
Luxembourg	No answer
The Netherlands	No
Slovak Republic	Yes. Registering of investigation files is stipulated by Criminal Proceedings, Art. 29 of the Act No 428/2002 Coll., Notice of the Ministry of Justice of the Slovak Republic No. 618/2055 on creating a file by law enforcement bodies during criminal proceedings and by courts; Registering of minor offences´ files, operative files – internal legal acts; Registering of manual registry, e.g. searching for things, operative-tactical registry – the procedure is stipulated by internal acts.
Sweden	No. Manual registers, if any, are very few.

Table 16
Obligation to create & notify own description of manual file

	Q.19 If a police force does not comply with this general description, would it be obliged to make its own description and to notify it to the supervisory authority? (R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 38–39)
Albania	No answer
Estonia	No
Germany	On grounds of the principle of the rule of law the Federal Criminal Police Office is obligated to abide by the Federal Criminal Police Office Act. Hence, there is no possibility to derogate from legal requirements (see Q.18). Art. 20 (3) of the Basic Law for the Federal Republic of Germany
Hungary	Yes [No further info provided]
Lithuania	According to Article 30(1) of the LLPPD the data controller and data processor must implement appropriate organisational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing and must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc.). This obligation is mandatory upon the controllers of the police files (including with regard to manual files), but there is no obligation to notify such document to the State Data Protection Inspectorate of the Republic of Lithuania.
Luxembourg	No answer
The Netherlands	No answer
Sweden	No. Manual registers, if any, are very few

Table 17
Other ways of extending principles of R(87)15 to manual police files

	Q.20 Are the principles laid down in R(87)15 extended to manual police files in any other ways? *(R87(15) Principle 1.4 first sub-paragraph; Explanatory Memorandum para. 38–39)*
Albania	Yes [no further details]
Estonia	Yes
Hungary	Yes [no further details provided]
Lithuania	According to Article 1(2) of the LLPPD, this law shall regulate relations arising in the course of the processing of personal data by automated means, and during the processing of personal data by other than automated means in filing systems: lists, card indexes, files, codes, etc. The Law shall establish the rights of natural persons as data subjects, the procedure for the protection of these rights, the rights, duties and liability of legal and natural persons while processing personal data. So the LLPPD is fully applicable to the manual police files, since they always constitute filing system.
Luxembourg	No answer.
Monaco	cf. art 24.1 précité les traitements manuels doivent respecter les principes généraux de la loi n°1.165 modifiée [cf. art 24.1 manual processing must respect the general principles of amended Law No. 1.165]
The Netherlands	No
Sweden	'The Personal Data Act (1998:204) and Police Data Act (2010:361) also applies to other (than data as is wholly or partly automated) processing of personal data, e.g. personal data in manual files, if the data is included in or is intended to form a part of structured collection of personal data that is available for searching or compilation according to specific criteria. Ch 1 sec 2 Police Data Act (2010:361)'

Table 18
Obligation to notify ad hoc files

	Q.21 Principle 1.4: Is there any obligation in your country to notify ad hoc files which have been set up at the time of particular inquiries? *(R87(15) Principle 1.4 second sub-paragraph; Explanatory Memorandum para. 40–42)*
No	Albania; Bosnia and Herzegovina; Germany; Ireland; Italy; Luxembourg; Monaco; Slovak Republic; Sweden; Macedonia; Ukraine.
Yes	Andorra, Austria; Cyprus; Estonia; Finland; France; Hungary; Liechtenstein; Lithuania; Malta; the Netherlands; Slovenia; Switzerland.
Qualified Yes	Croatia; UK.
Unclear answer	Czech Republic, Portugal
No answer	Montenegro, Serbia

Table 19
Conditions and laws for notifying ad hoc files

	Q.22 If yes, in accordance with what conditions/national legislation is this done? *(R87(15) Principle 1.4 second sub-paragraph; Explanatory Memorandum para. 40–42)*
Andorra, Austria, Croatia, Cyprus, Germany, Liechtenstein, Lithuania, Slovenia, Switzerland	No differentiation between permanent and ad hoc files, including for purposes of notification.
Estonia	It has to be according to law and necessary for the purpose.
Finland	The notification of ad hoc files is based on section 8(2) of Act 731/2006.
France	'The notion of ad hoc files does not exist in French law. At the time of the creation of police processing, it must be notified according to the ordinary legal rules.'
Hungary	Act LXIII on the Protection of Personal Data and Publicity of Data of Public

	Interest
Malta	No answer.
The Netherlands	'Art 9 Police Data act: The purpose of every ad hoc police file must be laid down within a week. The privacy officer is obliged to keep a registration of the purposes of the ad hoc files following art 34 (2) Police Data Act.'
UK	'If ad hoc files are established as new categories of data then they should form part of the annual notification procedure. (DPA Part III, s.18 and 20.)'

Table 20
Collection of data not limited to that necessary for prevention or suppression of specific offence

	Q.23 Principle 2.1: Are there instances of collection of personal data for police purposes which is not limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence? *(R87(15) Principle 2.1; Explanatory Memorandum para. 43)*
No	Andorra, Czech Republic, Italy, Liechtenstein, Luxembourg, the Netherlands, Macedonia, Portugal and Slovenia and Ukraine.
Yes	Austria, Bosnia and Herzegovina, Croatia, Cyprus, Estonia, Finland, France, Hungary, Ireland, Monaco, Slovak Republic, Sweden and Switzerland.
Unclear/irrelevant answer	Albania, Lithuania, Montenegro and Serbia.
No answer	Malta and UK.
Germany	The terms "prevention of a real danger" and "the suppression of a specific criminal offence" are unclear. Therefore, we are only able to provide general information.

Table 21
Countries authorising wider police powers to gather information

	Q.24 If yes, is such collection the subject of specific national legislation clearly authorising wider police powers to gather information? *(R87(15) Principle 2.1; Explanatory Memorandum para. 43)*
Austria, France, Finland, Sweden and Switzerland	Provided details substantiating their claim of appropriate specific national legislation (Austria,[114] France,[115] Finland,[116] Sweden[117] and Switzerland[118])

[114] § 21 para. 2 and § 54 of the Federal Act on the Organisation of Security Administration and the Exercise of Security Police Services (Security Police Act – Sicherheitspolizeigesetz).

[115] For e.g. Article 17-1 de la loi du 21 janvier 1995. Moreover, certain legislative texts (law n° 2006-64 of 23 January 2006 on the fight against terrorism, law n° 2011-267 on direction and programming relative to internal security…) authorise the processing of personal data or provide a specific legislative framework. However, these texts do not provide supplementary or expanded powers to the police services. The general provisions of the law of 6 January 1978 complete the specific legislative provisions.

[116] Apart from police data systems, Act 761/2006 provides for a Data System for Administrative Matters, and the police have access to the Emergency Response Centre Data System and the Register of Aliens. In addition, the police obtain data retrieved from certain registers referred to in section 13 of Act 761/2003 subject to details to be agreed on with the keeper of the register in question, and may obtain data from certain registers referred to in section 14 of the Act in accordance with the provisions of the relevant specific legislation. Ref Emergency Response Centres Act (157/2000) and Act on the Register of Aliens (1270/1997). The access of the police to such registers and the use of data retrieved from those registers are governed by the provisions of Act 761/2003. The collection of data to be included in those registers is governed by the provisions of specific legislation (see the lists in sections 13 and 14 of the Act).

[117] Specific regulations, mainly in the Police Data Act (2010:361).

[118] Art. 2 Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS 120); Art. 11 Loi fédérale du 13 juin 2008 sur les systèmes d'informations de police de la Confédération (LSIP ; RS 361); Art. 81 al.1 Loi fédérale sur la police (LPol) en projet qui remplacera les dispositions relatives aux traitements des données personnelles par les autorités de police éparpillées dans diverses lois fédérales (cf. LMSI, LSIP, LEIS et autres).

Bosnia and Herzegovina	Provided a reference to – Law on State Investigation and Protection Agency ("Offizial Gazzete BaH" No.27/04, 63/04, 35/05 and 49/09), Article 3, paragraph (1) prescribes the general police powers to gather information.
Croatia	Responded 'yes' but provided no reference to any law.
Cyprus	Responded 'yes' and referred to sections 9 and 10 of the Police Law (L .73(I)/2004) dealing with criminal records.
Estonia	Responded 'yes' and referred to 'Estonian Road Administration, Estonian Tax and Customs Board, Prisons Department of Ministry of Justice.'
Germany	Pursuant to the Federal Criminal Police Office Act, the BKA may only store data if this is necessary to fulfil its tasks. Which data may be stored by the Federal Criminal Police Office (BKA) is governed by law.
Hungary	No response.
Ireland	The Garda Síochána Act 2005: Emphasis on purpose.[119]
Monaco	La police monégasque adopte des mesures préventives , induites par la particularité d'un territoire exiguë et dont les frontières sont ouvertes. Ex: les fiches d'hôtel ; les requêtes en naturalisation (traitement régalien de souveraineté tel que prévu par l'art 15 de la Constitution et non soumis aux dispositions de la loi n° 1.165). [The police of Monaco adopt preventive measures, induced by the peculiarity of a tiny territory whose borders are open. E.g. hotel forms; petitions for naturalization (processing of sovereignty as provided by Article 15 of the Constitution and not subject to the provisions of Law No. 1165).] Cf Ordonnance souveraine n°765 du 13 novembre 2006 relative à l'organisation et au fonctionnement de la direction de la sûreté publique et art 9 et 10 de l'ordonnance n. 3.153 du 19/03/1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté en ce qui concerne les fiches d'hôtel et art 5 de la loi n°1155 du 18 décembre 1992 relative à la nationalité. [Cf. Sovereign Ordinance No. 765 of 13 November 2006 on the organization and functioning of the Directorate of Public Security and art 9 and 10 of Ordinance no. 3.153 of 19/03/1964 on the conditions of entry and residence of foreigners in the Principality with regard to hotel forms and art 5 of Law No. 1155 of 18 December 1992 on Nationality.]
Montenegro	Responded 'yes' and referred to the Law on Police.[120]
Slovak Republic	Art. 1 of the Act No. 171/1993 Coll. defines the scope of activities of the Police Force.

Table 22
Data subjects notified of their data collected without their knowledge

	Q.25 Principle 2.2: According to existing records, on how many occasions have data subjects been informed where data concerning them have been collected and stored without their knowledge and have not been deleted as soon as the object of the police activities was no longer likely to be prejudiced? *(R87(15) Principle 2.2; Explanatory Memorandum para. 44–45)*
No cases	Albania, Austria, Croatia, Cyprus, France, Italy, Monaco, Portugal, Slovak Republic and Slovenia.
No information	Andorra, Bosnia and Herzegovina, Czech Republic, Estonia, Finland, Germany, Hungary, Ireland, Liechtenstein, Lithuania, Luxembourg, Malta, Montenegro, the Netherlands,

[119] Section 4.2 of the Garda Code of Practice states the following: "An Garda Síochána may only keep data for purposes that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with the purpose. An individual has a right to question the purpose for which An Garda Síochána holds his/her data and An Garda Síochána must be able to identify that purpose. An Garda Síochána holds information for a variety of purposes. Much of this information is held for the investigation, detection and prevention of offences while other information such as the Keyholders Register, Administrators of Neighbourhood Watch Schemes, and the Electoral Register for instance are held for the performance of functions of a public nature and can only be used for these purposes."

[120] Official Gazette of Montenegro 28/05, 86/09 and 88/09. Law adopted on 05 May 2005, and entered into effect on 13 May 2005.

	Serbia, Switzerland, Sweden, Ukraine and the UK.
Macedonia	"The Police officials are not bound to report to the data subject."

Table 23a
Rules regulating collection of data by technical surveillance/automated means

	Q.26 Principle 2.3: Which are those laws/specific provisions which provide for collection of data by technical surveillance or other automated means? Please append text. (R87(15) Principle 2.3; Explanatory Memorandum para. 46–47) *Q.27 Are those laws/specific provisions accompanied by adequate guarantees against abuse? If yes, kindly provide examples of such adequate guarantees. (R87(15) Principle 2.3; Explanatory Memorandum para. 46–47)*
Albania, Andorra, Austria, Germany, Ireland, Monaco, Sweden and UK	Referred to their law regulating interception
Austria, Germany, Hungary, Ireland, Liechtenstein, Slovenia, Sweden, Switzerland and UK	Referred to their laws regulating covert surveillance
Austria, Italy, Liechtenstein, Luxembourg, Montenegro, Slovenia, Sweden and Switzerland	Referred to their regulation of video surveillance

Table 23b

Andorra	"En Principauté d'Andorre la collecte de données par des moyens techniques de surveillance ou d'autres moyens automatisés n'est possible que dans le cadre de procédures judiciaires et sous le contrôle du juge d'instruction. Ces dispositions sont prévues dans le la Loi qualifiée de modification du Code de procédure pénale, du 10 décembre 1998, publiée au bulletin officiel le 7 janvier 1999 et qui est entrée en vigueur le même jour de sa publication et La Loi 10/2005, du 21 février, qualifiée de modification du Code de procédure pénale, publiée au bulletin officiel le 23 mars 2005 et qui est entrée en vigueur six mois après sa publication. (art. 87) [In Andorra the collection of data by technical surveillance or other automated means is only possible within the framework of judicial procedures and under the supervision of the investigating judge. These provisions are described in the Act to amend the Code of Criminal Procedure, of 10 December 1998, published in the Official Gazette on 7 January 1999 and which came into force on the same day of its publication and Law 10/2005, of 21 February, qualified for amending the Code of Criminal Procedure, published in the Official Bulletin on 23 March 2005 and which came into force six months after its publication (Art. 87).] Pour certains délits et par exemple pour les écoutes téléphoniques le juge d'instruction à l'obligation de communiquer à la personne mise sous surveillance qu'elle à fait l'objet de cette mesure." [For certain crimes and for example for wiretapping the investigating judge has got the duty to disclose to the person put under surveillance that s/he was the subject of this measure.] "Des garanties constitutionnelles sont établies dans la Constitution de la Principauté d'Andorre dans les articles 9 à 15 de ce texte." [Constitutional guarantees established in the Constitution of

	the Principality of Andorra in articles 9-15 of this text.] D'autre part la Principauté à adopté la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 22 décembre 1995 (publiée au bulletin officiel le février 1996 et en vigueur un mois après sa publication) qui en application de l'article 3 de la Constitution à été intégré directement lors de son adoption dans l'ordre juridique de la Principauté. [In addition the Principality has adopted the Convention for the Protection of Human Rights and Fundamental Freedoms of December 22, 1995 (published in the official bulletin in February 1996 and in force one month after its publication) which, pursuant to Article 3 of the Constitution, has been directly integrated following its adoption in the legal system of the Principality.] Le Code pénal de la Principauté prévoit entre autres des délits qui punissent les abus qui pourraient être commis dans ce cadre comme par exemple l'obtention ou utilisation illicites de données personnelles automatisées (article 184), les écoutes illégales ou autres conduites similaires (article 183) et d'autres délits prévus dans le chapitre premier du titre X «Délits contre l'intimité et l'inviolabilité du domicile». [The Criminal Code of the Principality provides *inter alia* for crimes that punish the abuses that may be committed in this context such as the illicit obtaining or use of automated personal data (Article 184), illegal wiretapping or other similar conduct (Article 183) and other offenses provided for in chapter I of Title X "Offences against privacy and inviolability of the home."] Le Code pénal prévoit également dans le chapitre 2 du titre XXI «Infidélité dans la garde de documents et violation du secret » diverses infractions pénales applicables à ces cas d'espèce lorsqu'ils sont commis par des fonctionnaires dont ceux de police. [The Criminal Code also provides in Chapter 2 of Title XXI "Infidelity in the custody of documents and breach of confidentiality" various criminal offences applicable to such cases when committed by public officials including the police.] Des jugements ont été adoptés par les tribunaux andorrans sur la base de la jurisprudence de la Cour Européenne des Droits de l'Homme dans plusieurs de ces domaines, le dernier cas par exemple concernant l'assistance de l'avocat dès la première heure de détention.» [Judgments have been adopted by the Andorran courts on the basis of the jurisprudence of the European Court of Human Rights in several of these areas, the most recent case for example concerning the assistance of legal counsel from the first hour of detention.]
Austria	Legal provision for instances of collection of data by technical surveillance or other automated means. § 21 para. 3 of the Federal Act on the Organisation of Security Administration and the Exercise of Security Police Services (Security Police Act – Sicherheitspolizeigesetz) provides: "(3) Security authorities shall be responsible for the observation of groupings if, in view of their existing structures and expectable developments in their surroundings, it has to be expected that criminal offences will be committed causing severe danger to public security, in particular, violence motivated by ideologies or religious beliefs (extended potential danger identification)." The specific instances in which automated collection of data may take place for purposes others than the prevention of a real danger or the suppression of a specific criminal offence are regulated in § 54 of the Security Police Act. The exercise of the relevant powers described in its legislation is subject to legal supervision by the "Legal Protection Commissioner", a specific independent control institution.[121] Depending on the specific legal provision under which the specific instance of compiling of personal data or surveillance takes place, the security authorities may be obliged to notify the Legal Protection Commissioner,[122] to inform the Federal Minister of the Interior, who shall in turn give the Legal

[121] The applicable legal safeguards are *inter alia* set out in § 91c of the Federal Act on the Organisation of Security Administration and the Exercise of Security Police Services (Security Police Act – Sicherheitspolizeigesetz).

[122] § 91c. (1)

	Protection Commissioner the opportunity to comment thereon within three days,[123] or to obtain authorisation from the Legal Protection Commissioner through the Federal Minister of the Interior.[124] Furthermore, processing is subject to supervision by the Independent Data Protection Commission under the Federal Act concerning the Protection of Personal Data (DSG 2000).
Bosnia and Herzegovina	Provisions of the Code of Criminal Procedure on special investigative procedures and the conditions for their application.
Cyprus	Law regulating the use of cameras by the police for the detection and prosecution of traffic offences.
Estonia	Referred to its Surveillance Act[125] but provided no further details thereon
Finland	Referred to the provisions of Chapter 3 of their Police Act and to the Coercive Measures Act (450/1987) with regard to the entry of data retrieved by means of telecommunications interception or interception into personal data registers. The response from Finland states that these laws also provide adequate guarantees against abuse.
Germany	The following provisions of the BKA Act apply to the prevention of threats posed by international terrorism: Section 20 (g) (Special means of data collection); Section 20 (h) (Special provisions on the use of technical equipment in or from homes); Section 20 (k) (Covert intrusion into information technology systems); Section 20 (m) (Collection of telecommunications traffic data and usage data); Section 20 (n) (Identification and localisation of mobile telecommunications cards and terminal devices). Section 20 g of the Federal Criminal Police Office Act Section 20 h of the Federal Criminal Police Office Act Section 20 k of the Federal Criminal Police Office Act Section 20 m of the Federal Criminal Police Office Act Section 20 n of the Federal Criminal Police Office Act The following provisions apply in the area of criminal prosecution: - Section 100a of the Code of Criminal Procedure (Conditions regarding Interception of Telecommunications), in the version of Art. 1 of the Act of 21 December 2007 (Federal Law Gazette I, p. 3198); - Section 100 c of the Code of Criminal Procedure (Measures Implemented without the Knowledge of the Person Concerned [Use of technical means in private homes]), introduced by Art. 3 of the Act of 15 July 1992 (Federal Law Gazette I, p. 1302); - Section 100f Code of Criminal Procedure (Private speech outside homes), in the version as promulgated in Art. 1 no. 1 Act of 24 June 2005 (Fed. Law Gazette I, p. 1841); - Section100g Code of Criminal Procedure (Collection of telecommunications traffic data), introduced by Art. 1 no. 1 in conjunction with Art. 2 no. 1 of the Act of 20 Dec. 2001 (Fed. Law Gazette I, p. 3879); - Section 100h Code of Criminal Procedure (Further measures without the knowledge of the person concerned), in the version of Art. 1 no. 11 of the Act of 21 Dec.2007 (Fed. Law Gazette I, p 3198); - 100i StPO (Measures involving mobile telecommunications terminal devices), in the version of Art. 1 no. 11 of the Act of 21 Dec. 2007 (Fed. Law Gazette I, p 3198).

123 § 91c. (2) Actual use of image and sound recording devices or the actual use of the data processing shall be implemented only after expiry of this period or after submission of corresponding comments by the Legal Protection Commissioner.

124 § 91c. (3)

125 Available at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30011K7&keel=en&pg=1&ptyyp=RT&tyyp=X&query=j%E4litustegevuse

	Section 100a of the Code of Criminal Procedure Section 100 c of the Code of Criminal Procedure Section 100 f of the Code of Criminal Procedure Section 100 g of the Code of Criminal Procedure Section 100 h of the Code of Criminal Procedure Section 100 i of the Code of Criminal Procedure Surveillance with technical means or the use of powers for extended technical surveillance is possible only under narrowly defined conditions. The following provisions for example apply to surveillance of private homes under Section 20 (h)of the Federal Criminal Police Office Act (key procedural safeguards are indicated in **bold**) [unofficial English translation]: (1) With a view to responding to an **imminent threat to the existence or security of the state, or to the life, limb or freedom of a person or to property items of considerable value the preservation of which is required in the interest of the general public**, the Federal Criminal Police Office (BKA) may covertly use technical equipment in or from homes in order to 1. eavesdrop on and record private speech of a person a) who is responsible pursuant to sections 17 or 18 of the Act on the Federal Police, b) for whom concrete preparatory acts alone or along with other specific facts justify the reasonable assumption that he/she will commit offences pursuant to section 4a subsection 1 sentence 2, or c) who is a contact of a person mentioned in letter a or b or a person accompanying the latter, and 2. take photographs and make image recordings of this person if **the response to the threat is otherwise futile or considerably more difficult.** (2) **The measure may only target a person as referred to in subsection 1 and be carried out only in his/her home. The measure may be carried out in homes of other persons only, if specific facts suggest that** **1.** **a person as referred to in subsection 1 no. 1 letter a or b is staying there and** **2.** **the measure, if carried out only in the home of this person, will not result in a response to the threat mentioned in subsection 1.** The measure may also be carried out if other persons are unavoidably affected. (3) Measures as mentioned in subsection 1 may only be **ordered by a court at the request of the President of the Federal Criminal Police Office or his/her deputy.** In case of imminent danger, the measures may also be ordered by the President of the Federal Criminal Police Office or his/her deputy. In this case, the court decision shall be obtained subsequently and without delay. If the order issued by the President of the Federal Criminal Police Office or his/her deputy is not confirmed by the court within three days, it shall cease to be effective. (4) The order shall be issued in writing. **The order shall specify** **1.** **the name and address of the target person of the measure, if possible,** **2.** **the home/residential premises to place under surveillance,** **3.** **type, scope and duration of the measure and** **4.** **the essential reasons for it.** **The order shall be limited to a maximum period of validity of one month. The duration may be extended by not more than one month each time, if the prerequisites referred to in subsections 1 and 5 continue to exist, taking into account the information obtained. If the prerequisites for**

	the order do not exist any more, the measures taken on the basis of the order shall be stopped immediately. (5) **The measure referred to in subsection 1 may only be ordered and carried out if it can be assumed, based on facts regarding especially the type of premises to be placed under surveillance and the relationship between the target persons of the surveillance, that the surveillance will not cover statements considered to belong to the core area of the private sphere. The eavesdropping and observation referred to in sentence 1 shall be suspended immediately if facts revealed during surveillance suggest that contents considered to belong to the core area of the private sphere are covered. If doubts exist in this respect, only automatic recording may be continued. Automatic recordings as referred to in sentence 3 shall be submitted without delay to the court having ordered the measure with a view to obtaining a decision on whether the data may be used or have to be deleted. If the eavesdropping and observation have been suspended in accordance with sentence 2, the measure may be continued subject to the terms of sentence 1. Information from the core area of the private sphere which has been obtained by a measure pursuant to subsection 1 may not be used. Any recordings of it shall be deleted immediately. The fact that the data were recorded and deleted shall be documented. The documentation may be used exclusively for the purpose of data protection supervision. It shall be deleted as soon as it is no longer required for this purpose, but no later than at the end of the calendar year following the year of documentation.**
Italy	In a decision addressing video surveillance issues dated 8 April 2010,[126] the Italian *Garante* (the Italian Data Protection Authority) dealt with the data protection aspects related to the use of CCTV and other types of video surveillance for public security purposes. Moreover, according to section 55 of the Personal Data Protection Code,[127] any processing that is more likely to be prejudicial to data subjects – with particular regard to genetic and/or biometric databases, location-based processing, databases relying on specific information processing techniques, and the introduction of certain types of technology – must be compliant with such measures and arrangements as may be set forth by the Garante to safeguard data subjects following a prior checking procedure in pursuance of section 17 of the Code.
Liechtenstein	See Art. 33, 34 and 34a PA
Lithuania	Law on Operational Activities of the Republic of Lithuania (Official Gazette, 2002, No. 65-2633), as well as to their Code of Criminal Procedure.
Luxembourg	Guarantees against abuse (as referred to in Q.27) are provided by having controls exercised by the "Article 17" authority, the supervisory authority specifically charged with overseeing the processing of data for police purposes.
Malta	Reg. 5(3) of S.L. 440.05 "The collection of personal data by technical surveillance or other automated means can be performed for police purposes, or in accordance with any law" but no reference to any specific law/provision provided.
Monaco	Projet de loi portant réforme des Codes pénal et de procédure pénale en matière de corruption et de techniques spéciales d'enquête, telles la sonorisation et la fixation d'images de certains lieux ou véhicules, actuellement déposé au Conseil national article 60-10 du Code de procédure pénale (CPP) prévoyant les enregistrements audiovisuels des auditions en garde à vue. Art 106 et suivants du CPP relatifs aux interception, enregistrement et transcription de correspondances par voie de télécommunications ou de communications électroniques Art 268-3 du CPP sur les enregistrements audiovisuels d'auditions de mineurs ou majeurs incapables. [Bill to reform the Penal Code and Code of Criminal Procedure on corruption and special investigative techniques, such as sound and image fixing of certain places or vehicles, currently deposited in the National Council; Article 60-10 of the Code of Criminal Procedure providing audio-visual recordings of the hearings in custody; Art 106 et seq. of the Code of Criminal Procedure relating to interception, recording and transcribing correspondence by means of telecommunications or electronic

126 Available, also in English, at http://www.garanteprivacy.it/garante/doc.jsp?ID=1734653

127 Personal Data Protection Code, Legislative Decree no. 196 dated 30 June 2003, available in English at http://www.garanteprivacy.it/garante/document?ID=1219452

	communications; and Article 268-3 of the Code of Criminal Procedure on audiovisual recordings of hearings of minors or incapacitated adults.]
The Netherlands	Referred generically to the Police Data Act.
Sweden	The use of automated means to carry out secret telephone surveillance, secret wire-tapping and secret camera surveillance is determined pursuant to specific legislation in the Code of Judicial Procedure[128] by the court upon request of a prosecutor for a short, specified period of time. The supervisory authority is the Swedish Commission on Security and Integrity Protection, www.sakint.se. With regard to video surveillance under the Video Surveillance Act,[129] such surveillance normally requires a permit from the County Administrative Board.
Switzerland	Oui, ces lois et dispositions spécifiques sont assorties de garanties adéquates. Les moyens spéciaux de recherche d'informations (comme la surveillance de la correspondance par poste et télécommunications à titre préventif, l'observation de personnes dangereuses dans des lieux pas librement accessibles, y compris au moyen d'appareils techniques, et la perquisition secrète de systèmes informatiques) ne peuvent être employés que dans les domaines du terrorisme, du service de renseignements politiques ou militaires prohibé et du commerce illicite de substances radioactives et ce, uniquement en cas de menaces concrètes. De plus, l'utilisation de ces moyens est soumise à une double approbation : l'examen judiciaire par le Tribunal administratif fédéral et le contrôle sous l'angle de la politique de l'Etat par les deux membres du gouvernement fédéral, chefs respectifs des départements fédéraux concernés (justice et police ainsi que militaire). [Yes, these laws and specific provisions are accompanied by adequate safeguards. Special means of finding information (such as monitoring of communication by post and telecommunications as a preventive measure, observing of dangerous people in places not readily accessible, including through technical devices, and the secret search of information systems) can only be employed in the fields of terrorism, [du service de renseignements politiques ou militaires prohibé][translation?] and illegal trade in radioactive substances and only in case of concrete threats. Furthermore, the use of these means is subjected to a dual approval: judicial review by the Federal Administrative Court and control from the angle of policy of the State by two members of the federal government, heads of the relevant federal departments (justice and police, as well as military).] In *Switzerland*, in the Canton of Basel-Stadt, with regard to guarantees against abuse in the case of video surveillance, the responsible body has to set up a rule book in cooperation with the data protection supervisor. Furthermore, the data protection supervisor can launch an assessment of the actual systems, files etc.
UK	Referred to "DPA1998; RIPA2000".

Table 24
Prohibition of collection of sensitive data – variations on a theme

	Q.28 Principle 2.4: Does the law of your country prohibit the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law, unless absolutely necessary for the purposes of a particular inquiry? (R87(15) Principle 2.4; Explanatory Memorandum para. 48)

[128] Enacted in 18 July 1942, entered into force 1 January 1948. The rules about technical surveillance have been amended several times since they were first introduced (secret wire-tapping in 1948, secret telephone surveillance in 1989 and secret camera surveillance in 1995).

[129] (1998:150), enacted on 2 April 1998, entered into force on 1 July 1998.

Generally prohibited [with exceptions and/or other special provisions generally applicable to all sensitive data]	Albania, Bosnia and Herzegovina, Croatia, Cyprus, Finland, France, Germany, Liechtenstein, Luxembourg, Portugal, Sweden.
Generally prohibited 'unless absolutely necessary for the purposes of a particular inquiry'	Lithuania, Malta, Montenegro.
Generally prohibited unless explicitly provided for in law	Switzerland [With regard to data collected for police purposes, the Swiss Federal Act does not distinguish between sensitive and other data. It considers all police data as sensitive and provides restrictive provisions for all processing of police data].
Generally prohibited with exceptions provided for in law	Slovakia, The former Yugoslav Republic of Macedonia, Ukraine.
Generally prohibited [with no mention of exceptions]	Andorra, Estonia, Hungary, Ireland, Italy, Monaco, the Netherlands.
'Not explicitly authorised'	Austria [with regulation for when sensitive data is processed].
No [and no further information provided]	Czech Republic.
Unclear answers	Serbia, Slovenia.

Table 25
Collection of sensitive personal data solely for intrinsic properties

	Q.29 According to existing records, on how many occasions has data on individuals been collected solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law? (R87(15) Principle 2.4; Explanatory Memorandum para. 48)
No cases	Albania, Andorra, Croatia, Cyprus, Irleand, Monaco, Slovenia and Sweden.
No records available	Austria, Bosnia and Herzegovina, Germany, Hungary, Lithuania and the Netherlands, Slovakia, Ukraine.
No information provided	Czech Republic, Estonia, France, Finland, Italy, Liechtenstein, Luxembourg, Montenegro, Portugal, The former Yugoslav Republic of Macedonia, United Kingdom.

Table 26
Determining absolute necessity for the purposes of a particular inquiry

	Q.30 How was/is the question of "absolute necessity for the purposes of a particular inquiry" determined? (R87(15) Principle 2.4; Explanatory Memorandum para. 48)
Estonia	"It means that no other way is possible."
France	"According to Art 6 of the law of 6 January 1978, the data collected must be "adequate, relevant and not excessive" with regard to the purposes of the processing. The processing must also fall within the framework of derogations provided for in Article 8 of this law."
Ireland	"This is determined on a case by case basis."
Monaco	"*Toute donnée recueillie, doit l'être conformément à la Constitution, aux lois et règlements en vigueur, loyalement et proportionnellement. Elle doit pouvoir alimenter une procédure judiciaire.*" [Any data collected must be in accordance with the Constitution, laws and regulations, fairly and proportionately. It must be able to supply a legal proceeding.]
Sweden	"By interpretation of law."

Table 27
Measures in place to ensure limited and accurate data

	Q.31 Principle 3.1: What measures are in place to ensure that, as far as possible, the storage of personal data for police purposes is limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law? (R87(15) Principle 3.1; Explanatory Memorandum para. 49–51)
Majority of countries	General principles of data processing, including accurate and not excessive storage of data.
Some cases	Legal obligation upon the police to assess the accuracy or reliability of data.
Estonia, France, Germany, Ireland, the Netherlands, Sweden, and Switzerland	Internal controls.
Estonia, France, Germany, Ireland, Portugal, Sweden, Switzerland, and UK	Controls exercised by audits and/or spot checks carried out by the supervisory authorities.
Ireland	The Garda Information Service Centre (GISC) has a key role in ensuring the accuracy of data collected and stored for policing purposes. Details of the role of the GISC in ensuring accuracy of data are set out in Section 4.5 of the Garda Síochána Data Protection Code of Practice.

Table 28
Countries employing categorisation to improve accuracy of personal data

	Q.32 Principle 3.2: The Explanatory Memorandum refers to 'a system of data classification'. In your country, are different categories of data stored by police authorities distinguished in accordance with their degree of accuracy or reliability? (R87(15) Principle 3.2; Explanatory Memorandum para. 52)
Yes	Albania, Bosnia and Herzegovina, Croatia, Estonia, Finland, Hungary, Malta, the Netherlands [but only regarding data processed by the Criminal Intelligence Unit], Portugal, Slovak Republic, Slovenia, Sweden, Switzerland, The former Yugoslav Republic of Macedonia.
No	Andorra, Austria, Cyprus, France, Germany, Ireland, Lithuania, Luxembourg, Monaco, Ukraine.
Unclear or no information	Czech Republic, Italy, Liechtenstein, Serbia and UK.

Table 29
Measures to improve data quality by distinguishing fact from opinion

	Q.33 In particular, do the police authorities of your country distinguish data based on facts from data based on opinions or personal assessments? (R87(15) Principle 3.2; Explanatory Memorandum para. 52)
Yes	Albania, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, Hungary, Liechtenstein, Malta, the Netherlands [but only regarding data processed by the Criminal Intelligence Unit], Portugal, Slovak Republic, Slovenia, Sweden, Switzerland, The former Yugoslav Republic of Macedonia and UK.
No	Andorra, Austria, France, Germany, Ireland, Luxembourg, Monaco, Ukraine.
Unclear or no	Finland, Italy, Liechtenstein, Lithuania and Serbia.

answer	

Table 29b

Andorra	Le service de Police dispose d'un contrôle exhaustif sur l'enregistrement de données personnelles ainsi que sur leur consultation par les fonctionnaires habilités. Ainsi lorsqu'un fonctionnaire enregistre des données il doit être habilité pour le faire, le système enregistre les modifications réalisées ainsi que le nom de la personne qui les à faites. Selon les données enregistrées une deuxième vérification est réalisée par le service chargé des archives. / Compte tenu de l'exposé antérieurement nous ne faisons pas de différence en fonction du degré d'exactitude ou de fiabilité. [The Police Department has a comprehensive control over the recording of personal data as well as over their consultation by authorized officials. So when an official records data he must be empowered to do so, the system saves the changes made as well as the name of the person who made them. Based on the recorded data, a second audit is conducted by the department in charge of records. Given the previous statement, Andorra does not make distinctions in the degree of accuracy or reliability.] Non, compte tenu que les données fondées sur des opinions ou sur des appréciations personnelles ne peuvent être inclues dans des fichiers de police. [Data based on opinions or personal assessments should not be included in police files.]
Finland	The Act on the Processing of Personal Data by the Police (Act 761/2003) draws a distinction between different categories of data files, depending on the type of data (not on the reliability of the data). An assessment of the reliability of the information provider and the accuracy of the information is attached with the registered data, where possible.
Germany	German law does not make any distinction relating to accuracy and reliability of data categories. However, the accuracy and reliability of information obtained is constantly verified during criminal investigations or any measure taken to respond to a threat. German law stipulates that inaccurate data must be deleted, corrected or blocked. Under German law, differentiation depending on the degree of accuracy and reliability is reflected in the requirement that the data storing body must be identifiable in case of data based on opinions or personal assessments.
Ireland	Data controlled by An Garda Síochána can be broken down into a number of categories such as data of a personal nature, data of a non-personal nature, data of a sensitive personal nature, data required for policing purposes, administration data and the Gardaí have procedures in place which allow them to take corrective action where inaccurate or unreliable data is identified.
Liechtenstein	Data processed in connection with crime prevention (Art. 2 Para. 1 Subpara. d) or within the scope of State security (Art. 2 Para. 2) in information systems are to be kept separately from the other information systems. See: Art. 34b Para. 6 PA
Monaco	Seules les données dont la fiabilité est avérée sont conserves. [Only data whose reliability has been proved are preserved.]

Table 30
Data collected for administrative purposes

	Q.34 Principle 3.3: Do the police authorities of your country store data which has been collected for administrative purposes (for example, information on firearms certificates granted, lost property, etc) and are to be stored permanently, in a separate file? (R87(15) Principle 3.3; Explanatory Memorandum para. 53–54)
Yes	Albania, Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Liechtenstein, Luxembourg, Monaco, the Netherlands, Portugal, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, Ukraine.
No	Malta, Slovak Republic, Slovenia
No information	UK

Unclear answer	Lithuania, Serbia

Table 31
Where administrative data is subject to special regime for police data

	Q.35 Is such administrative data also subject to the special regime for police data? (R87(15) Principle 3.3; Explanatory Memorandum para. 53–54)
Yes	Albania, Croatia, Cyprus, Czech Republic, Estonia, Finland, Liechtenstein, Luxembourg, Monaco, Portugal, Switzerland, The former Yugoslav Republic of Macedonia.
No	Andorra, Austria, Bosnia and Herzegovina, France, Ireland, Italy, Malta, the Netherlands, Slovak Republic, Sweden, Ukraine, UK.
No information	Hungary, Lithuania, Slovenia
Unclear answer	Serbia

Table 31b

Ireland	Administrative data is subject to the Data Protection Acts and the Garda Síochána Data Protection Code of Practice, 2006.
UK	The Data Protection Act 1998 covers all processing of personal data.

Table 32
Where data collected for police purposes is used for other purposes

	Q.35bis Principle 4: Are there instances in which personal data collected and stored by the police for police purposes (the prevention and suppression of criminal offences or the maintenance of public order) are used for any other purpose? (R87(15) Principle 4; Explanatory Memorandum para. 55)
No (without exception)	Albania, Andorra, Bosnia Herzegovina, Estonia, France, Italy, Luxembourg, Malta, Portugal, Switzerland and Ukraine.
Yes, but only in accordance with law	Austria, Croatia, Cyprus, Finland, Germany, Liechtenstein, Lithuania, Slovak Republic, Sweden.
Yes	Hungary, Ireland, Monaco, UK
Inconclusive answer	The former Yugoslav Republic of Macedonia
No answer	Montenegro

Table 32b

Ireland	For vetting and security clearance purposes, for example for vetting for people applying for public sector posts, posts involving the care of minors, etc
Monaco	Contrôle de la délivrance des permis de travail. [monitoring the issuing of work permits.]
UK	Disclosure of criminal records and police information on potential employees to prospective employers.

Table 33
When communication between police bodies is permissible

	Q.36 Principle 5.1: In what circumstances is the communication of data between police bodies to be used for police purposes permissible? (R87(15) Principle 5.1; Explanatory Memorandum para. 56)
Andorra	The communication of data between police bodies occurs mostly within the framework of INTERPOL. Other applicable juridical frameworks include international as well as bilateral cooperation agreements.

Austria	To domestic authorities, so far as this is explicitly provided for by law or is an essential condition precedent for the recipient to safeguard a task conferred on him by law.
Bosnia and Herzegovina	Regulated by agreement signed by the police authorities.
Croatia	On the user's written request if this is necessary for carrying out tasks encompassed by the user's legal activity as defined by law.
Cyprus	Communication is regulated by internal regulations.
Estonia	Police bodies may only process the data that is related to their duties.
Finland	It is permissible subject to the conditions provided for in sections 17 and 18 of the Act on the Processing of Personal Data by the Police (761/2003), including also research and planning as well as training.
France	The rules are particular to each processing and within the framework of the legal powers of the police services.
Germany	The Federal Criminal Police Office may transmit personal data to other Federal and Land police forces, if this is necessary for the accomplishment of its tasks or of those of the recipient. Section 10 (1) of the Federal Criminal Police Office Act.
Ireland	Data may be communicated to other police bodies for legitimate policing functions: See section 4.3 of the Garda Code of Practice in relation to communication of data.
Italy	There does not appear to be any specific provision in this respect.
Liechtenstein	The National Police Force may disclose data to offices of the national administration, administrative authorities, the courts and the Swiss border guard authority if this is necessary for the performance of their duties as prescribed by law or the preconditions stated in Art. 23 of the Data Protection Act are met.
Lithuania	In the manner prescribed by laws...on a lawful basis for the exercise of the functions of police bodies.
Luxembourg	Luxembourg has only got one police authority. ["Le Grand-Duché du Luxembourg n'a qu'une seule autorité de police à savoir la Police Grand-Ducale."]
Malta	Where there exists a legitimate interest for such communication within the framework of the legal powers of police bodies (which would appear to be a typical example of "cut & paste syndrome" found in some states hurriedly adapting or adopting new regulatory instruments in order to comply with the acquis on accession to the European Union.)
Monaco	Dans le strict cadre du domaine judiciaire : procédure, recherches… L'échange obéit donc aux règles édictées en matière de collaboration internationale, soit par commission rogatoire, soit au travers d'Interpol et Europol. [Within the strict framework of the legal field: procedures, research ... The exchange obeys the rules laid down in international collaboration, either by letters rogatory or through Interpol and Europol.]
The Netherlands	Police data will be made available by the controller to persons who have been authorised by himself or by another controller for the processing of police data, insofar as they need the data for the execution of their duty.
Portugal	In accordance with the Law 73/2009, of 12 August, that also enshrines the principle of necessity.
Slovak Republic	Regulated by internal acts.
Sweden	See Ch 2 sec 16 Police Data Act (2010:361) ["A translation of the Swedish Police Data Act will be finalised during summer. We will send it to you as soon as possible."]
Switzerland	In accordance with the Loi fédérale sur les systèmes d'informations de police de la Confédération (LSIP ; RS 361).[130]
The former Yugoslav Republic of Macedonia	The circumstances are determined in article 34 of the Law on Personal Data Protection: "The controller shall reveal the personal data to a user upon the user's written request, if needed for performing matters within legally determined competencies of the user. / The written request referred to in paragraph 1 of this Article has to contain the reasons, legal basis for usage of the personal data and personal data category being requested".
Ukraine	Police bodies can communicate data either with the consent of the data subject or in cases determined by law, and only in the interests of national safety, economic

[130] Art. 3 al.2 LSIP.

	welfare and human rights. (Law on Personal Data Protection, Article 14)
UK	Under the DPA 1998 it is up to data controller to decide if it is necessary and reasonable in all the circumstances to share information, either on a case-by-case basis or by implementing a data sharing agreement for a more long term arrangement.
Albania, Czech Republic, Serbia and Slovenia	Unclear/insufficient responses
Montenegro, Hungary	No answer

Table 34
Legal requirement for police to have legitimate interest in obtaining data

	Q.37 Does it require the police authorities to have a "legitimate interest" in obtaining the data? (R87(15) Principle 5.1; Explanatory Memorandum para. 57)
Yes	Albania, Andorra, Austria, Bosnia and Herzegovina Croatia, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Liechtenstein, Lithuania, Malta, Monaco, the Netherlands, Portugal, Slovak Republic, Slovenia, Sweden, Switzerland, the Former Yugoslav Republic of Macedonia, Ukraine and UK.
NA	Italy and Luxembourg.
Unclear	Czech Republic and Serbia.

Table 35
Types of legitimate interest required by police to obtain data

	Q.38 If it is required that the receiving police authority possess a "legitimate interest" in obtaining the data, how is such a "legitimate interest" for such communication to be determined? (R87(15) Principle 5.1; Explanatory Memorandum para. 57)
Andorra	L'intérêt légitime est apprécie par le département de coopération international du service de police de la Principauté qui a comme fonction l'échange de données en matière pénale et reçoit les demandes étrangères ou élabore les demandes dirigées à d'autres services de police étrangers. Cette coopération se réalise principalement par le canal INTERPOL. Seules des autorités de police peuvent adresser des demandes d'information. [The legitimate interest is assessed by the department of international cooperation of the police of the Principality that has the function of data exchange in criminal matters and receives foreign requests or elaborates the requests directed to other foreign police agencies. This cooperation is achieved mainly through INTERPOL. Only law enforcement agencies can submit requests for information.]
Austria	The fulfilment of a task conferred to an authority by the law constitutes a legitimate interest.
Estonia	The processor who provides data determines the legitimate interest. The obtaining party has to give reasons.
Finland	The data must be necessary for the performance of duties referred to in section 1 of the Police Act. Other types of data may only be communicated for certain purposes explicitly provided for in sections 17 and 18 of the Act on the Processing of Personal Data by the Police (761/2003). A corresponding requirement of a specific purpose is also included in sections 6 and 7 of the Personal Data Act.
France	Recipients of data must justify a legal right or be expressly mentioned in the regulating act creating the processing.
Germany	The transmission of data is permissible only if this is necessary for the accomplishment of the tasks of either the Federal Criminal Police Office or the Federal and Land police forces. Section 10 (1) of the Federal Criminal Police Office Act.
Ireland	The existence of a 'legitimate interest' is determined by the provision of background and investigative information on the personal data being shared or sought, and by the use of appropriate channels, evaluation and handling codes, and conventions.
Liechtenstein	Necessary for the performance of their duties as prescribed by law.
Lithuania	As laid down in the law – Article 5 of the Law on Legal Protection of Personal Data No. I-1374.

Malta	The Law Enforcement Authority submitting the request must be lawfully empowered in line with its functions to request similar information. Such requests are normally evaluated by the receiving body on a case-by-case basis. In cases of routine data exchanges, specific Memoranda of Understanding (MoU) may also be in place to regulate the procedure.
Monaco	La police sera soit saisie par un magistrat lui ordonnant de diligenter une enquête, soit amenée à intervenir dans un cadre juridique exigeant le recueil des données. [The police will be seized by a magistrate ordering them to undertake an investigation, be required to intervene in a legal framework requiring the collection of data.]
The Netherlands	That they need the data for the execution of their duty.
Portugal	The provision of data and information is restricted to what is considered relevant and necessary for prevention and criminal investigation purposes in a given case.
Serbia	"If the processing is necessary for doing legal job within its jurisdiction of certain general legal act."
Slovenia	If performing police duties in accordance with the law.
Sweden	Pursuant to law.
Switzerland	La législation spéciale de police prévoit expressément que seules les données personnelles peuvent être traitées dans la mesure où elles s'avèrent nécessaires à l'exécution de tâches légales. (Art. 3 al. 2 in fine LSIP) [The special police legislation expressly provides that only personal data may be processed insofar as they are necessary for the performance of legal duties. (Art. 3 para. 2 LSIP)]
The former Yugoslav Republic of Macedonia	If needed for performing matters within legally determined competencies of the user.
Ukraine	If permitted in cases determined by law, and only in the interests of national safety, economic welfare and human rights.
UK	In general terms, in the UK legitimate interest means that there should be no law specifically prohibiting such processing. Legitimate interests, in the specific context of the Data Protection Act 1998, means that any legitimate interest pursued by the Police or third party in conjunction with the Police, should only be initiated without prejudicing the rights and freedoms or legitimate interests of the data subject.

Table 36
Is any oversight mechanism in place?

	Q.39 Is any oversight mechanism in place? *(R87(15) Principle 5.1; Explanatory Memorandum para. 57)*
Yes	Albania, Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Liechtenstein, Lithuania, Monaco, the Netherlands, Portugal, Slovak Republic, Slovenia, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Ukraine and UK.
No	Malta.
NA	Italy and Luxembourg.
Unclear	Serbia.
No information	Czech Republic.

Liechtenstein	Art. 29 DPA: The Data Protection Office shall supervise compliance by authorities with this Act and other regulations relating to data protection. The government shall be exempted from such supervision. [Explanation: By exempting the Government from supervision solely the Government itself (in German "Regierung") with its 5 members and the associated departments are exempt from supervision. The National Police, court etc. bodies are considered public authorities over which the data protection office generally has the power of supervision. Regarding the National Police the Data Protection Office is the supervisory authority in regard of data protection.

Table 37
Sub-categories of processing where communication of data is permissible

	Q.40 Principle 5.2: In what circumstances is the communication of police data to other public bodies (e.g. social security authorities, inland revenue authorities, immigration control, customs authorities etc.) permissible? (R87(15) Principle 5.2.i; Explanatory Memorandum para. 58–61)
ONLY if explicitly provided for by law	Austria, Croatia, Estonia, Finland, France, Italy, Lithuania, Monaco, Ukraine.
Legal basis & authorisation of supervisory authority ONLY	Albania, Malta, Slovenia.
Legal basis & judicial authorisation ONLY	Andorra, Ireland, Luxembourg, Sweden.
Legal basis & Ministerial authorisation ONLY	The Netherlands.
Legal basis , authorisation of supervisory authority & other cases	Cyprus.
Legal basis, judicial authorisation & other cases	Bosnia and Herzegovina, Portugal, Switzerland.
Legal basis, judicial authorisation & authorisation of supervisory authority	Slovak Republic.
Legal basis, Ministerial authorisation & other cases	UK.
Legal basis & other cases	Germany, Hungary, Liechtenstein.
Based on agreements with public bodies who require the data for the performance of their tasks	One case (social security) in Andorra, Montenegro, The former Yugoslav Republic of Macedonia.

Table 37b

Germany	According to Section 10 (2) the Federal Criminal Police Office may transmit personal data to authorities and public bodies other than those mentioned in subsection 1 if this is provided for in other legal provisions or necessary 1. to accomplish its tasks pursuant to this Act, 2. for purposes of criminal prosecution, execution of sentences, imprisonment and clemency proceedings, 3. for purposes of threat response, or 4. to avert serious infringements of the rights of individuals, and if this is not in contradiction to the purposes of the criminal proceedings. “Other legal provisions” for the transmission of personal data are for example section 18 (1) BVerfSchG Section 10 subsection 2 BKAG

Table 38
Clear legal obligation to communicate data to other public bodies

	Q.41 Are there instances in your law of a clear legal obligation on the police authorities to communicate data to any other public bodies? Please append the text of the relevant law. (R87(15) Principle 5.2.i.a; Explanatory Memorandum para. 60)
Yes	Austria, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, France, Germany, Hungary, Luxembourg, Monaco, the Netherlands, Portugal, Slovenia, Sweden, Switzerland and UK.
No	Andorra, Finland, Ireland, Liechtenstein and Lithuania, Ukraine.
No answer	Italy
Unclear	Albania, Serbia, Slovak Republic, The former Yugoslav Republic of Macedonia.

Table 38b

Finland	Section 19 of Act 761/2003 provides for the authorities to which the police may communicate data registered in the police data files (except for the Europol Data System and the National

	Schengen Information System) as well as for the purposes for which the data may be communicated, the wording of the provisions of Act 761/2003 does not impose an obligation. Legislation concerning certain other authorities provides for the right of those authorities to obtain data from the police in specific circumstances.
Germany	Yes, Section 18 of the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (BVerfSchG) stipulates: "The authorities of the Federation, of the federal institutions of public law, the public prosecutors' offices and, subject to the public prosecutors' authority to give instructions as regards subject matters, the police authorities, the authorities of the customs investigation service and other customs offices performing tasks under the Federal Police Act, on their own initiative, shall notify the Federal Office for the Protection of the Constitution or the state offices for the protection of the constitution of the information, including personal data, having come to their knowledge, indicative of activities threatening security or intelligence activities carried out on behalf of a foreign power or efforts within the area where this Act applies which by use of violence or preparation thereof are directed against the interests protected by this Act as defined in section 3, subsection 1, no. 1, 3 and 4. Obligations to transfer information under the Military Counterintelligence Act or the Federal Intelligence Service Act beyond those defined in sentence 1 shall not be affected. Sentence 1 shall not apply to the transfer of information between authorities of the same federal state. Section 18 BVerfSchG.
Ireland	There is no absolute obligation under Irish law unless subject to a court order.
Switzerland	«La communication de données personnelles de police à d'autres organes publics est autorisée dans la mesure où cela est nécessaire pour obtenir les renseignements dont ils ont besoin et pour motiver leurs demandes d'entraide administrative ainsi que pour les assister dans l'accomplissement de leurs tâches légales. Art. 3 al.2 LSIP, Art. 19 LPol projet Les autorités de police peuvent communiquer des données à d'autres autorités suisses ou étrangères (p. ex. autorités de police, douanières, assumant des tâches relevant du droit des étrangers) en vue de l'accomplissement de leurs tâches légales ou de l'exécution d'obligations internationales. Art. 15 LSIP & Art. 7 RIPOL Ordonnance Plusieurs services publics ont accès à des systèmes d'information de police, en fonction de leurs finalités, pour l'accomplissement de certaines de leurs tâches légalement prévues (par exemple autorités de migration, de poursuite pénale et de circulation routière au SIS). Art. 16 LSIP Egalement communication à des services de contrôle internes à l'administration pour l'accomplissement de leurs tâches légales ainsi que pour leurs travaux de maintenance et de programmation. cf. supra et Art. 5 LSIP» [The communication of police data to other public bodies is permitted to the extent necessary to obtain the information they need and to motivate their requests for administrative assistance and to assist them in performing their legal tasks. The police authorities may communicate data to other Swiss and foreign authorities (for e.g. law enforcement, customs, taking on tasks relevant to the law on aliens) in view of the accomplishment of their legal duties or of the execution of international obligations. Several public services have access to police information systems, in accordance with their purpose, for the accomplishment of certain of their tasks as provided for in law (for e.g. migration authorities, law enforcement and traffic to the SIS. Also communication to controls services internal to the administration for the accomplishment of their legal tasks and for their maintenance work and programming.]

Table 39
Where DPA authorise communication of data to other public bodies

	Q.42 Are there instances in which the supervisory authority may authorise such a communication of data by the police authorities to any other public bodies? (R87(15) Principle 5.2.i.a; Explanatory Memorandum para. 60)
Yes	Albania, Cyprus, Malta, Slovak Republic, The former Yugoslav Republic of Macedonia.
No	Andorra, Austria, Bosnia and Herzegovina, Croatia, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Monaco, the Netherlands, Portugal, Slovenia, Sweden, Switzerland, Ukraine and UK.
Don't know	Czech Republic.
Unclear	Serbia.

Table 39b

Cyprus	The communication of police data to other public bodies is permissible after a licence for the combination of filing systems is issued by the Commissioner in accordance with section 8 of the Processing of Personal Data (Protection of Individuals) Law of 2001 (Law 138(I)/2001).
Ireland	While there is no legislative provision for such an authorisation, however the Gardaí routinely seek advice from the Office of the Data Protection Commissioner on such matters.

Table 40
Other authorities empowered to authorise communication of data

	Q.43 Is any other authority empowered to authorise the police authorities to communicate data to any other public bodies? *(R87(15) Principle 5.2.i.a; Explanatory Memorandum para. 60)*
Yes	Andorra (l'autorité judiciaire [judicial authority]), Bosnia and Herzegovina (judicial authority), Hungary (no details provided), Luxembourg (judicial authority), the Netherlands (the Minister of Security and Justice), Portugal (judicial authority), Slovak Republic (judicial authority), Slovenia (Information Commissioner), Sweden (judicial authority), Switzerland (the federal police office responsible for the processing of police data in the framework of police files and judicial authority) and UK (Home Secretary).
No	Albania, Austria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Ireland, Liechtenstein, Lithuania, Malta, Monaco, The former Yugoslav Republic of Macedonia, Ukraine.
No answer	Italy.
Unclear	Serbia.

Table 41
Other circumstances where communication is authorised

	Q.44 Are there any other circumstances in which the police authorities of your country are authorised to communicate data to other public bodies (apart from when there exists a clear legal obligation or authorisation)? *(R87(15) Principle 5.2.i.b and 5.2.ii; Explanatory Memorandum para. 61–62)*
Yes	Bosnia and Herzegovina, Cyprus, Hungary (no details provided), Ireland, Malta, Portgual, Switzerland, the former Yugoslav Republic of Macedonia and UK.
No	Albania, Andorra, Austria, Croatia, Estonia, Finland, France, Germany, Lithuania, Luxembourg, Monaco, the Netherlands, Slovak Republic, Slovenia, Sweden, Ukraine.
NA	Liechtenstein.
Unclear	Czech Republic, Italy and Serbia.

Table 41b

Cyprus	Communication of non sensitive police data to other public bodies may be permissible in accordance with sections 5(2)(a) (processing is necessary for compliance with a legal obligation to which the controller is subject), 5(2)(c)(processing is necessary in order to protect the vital interests of the data subject), 5(2)(d) (processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority vested in the controller or a third party to whom the data are communicated;) and 5(2)(e) (processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the personal data are communicated, on condition that such interests override the rights, interests and fundamental freedoms of the data subjects) of The Processing of Personal Data (Protection of Individuals) Law 138(I)/2001. Communication of sensitive police data to other public bodies is permissible if any one of the conditions of section 6(2) of the Law is fulfilled, particularly, the condition set out in section 6(2)(g) of the Law: s. 6(2)(g) processing is necessary for the purposes of national needs or national security, as well as criminal and reform policy, and is performed by a service of the Republic or an Organisation or Foundation authorized for this purpose by a service of the Republic and relates to the detection of crimes, criminal convictions, security measures and investigation of mass

	destructions;
Ireland	Section 8 of the Data Protection Act 1988 (as amended by section 9 of the 2003 Act) lifts the restrictions on the processing (including communication) of personal data in circumstances where processing is in the interests of the data subject or in the general public interest e.g. where the life of a person could be compromised by not disclosing personal data. It is a matter for the Garda Síochána to decide on a case by case basis as to whether the data can be provided on any such basis.

Table 42
Provisos to authority to transmit police data to other public bodies

	Q.45 Are there any provisos to this authority being granted? *(R87(15) Principle 5.2.i.b and 5.2.ii; Explanatory Memorandum para. 61–62)*
Yes	Bosnia and Herzegovina, Malta (S.L. 440.05 Reg. 8(4)), Hungary (no details provided) and Portugal (Law 67/98, Article 6).
No	Andorra, France, Lithuania, Luxembourg, Monaco, Switzerland, Ukraine.
NA	Austria, Croatia, Estonia, Finland, Germany, Liechtenstein, Slovak Republic and Sweden.
No answer	Albania, Italy, the Netherlands and Slovenia.
Unclear	Cyprus, Czech Republic and Serbia.

Table 43
Existence of oversight mechanisms

	Q.46 Is any oversight mechanism in place with regard to determinations of authorisation to communicate data to other public bodies? *(R87(15) Principle 5.2.i.b and 5.2.ii; Explanatory Memorandum para. 61–62)*
Yes	Bosnia and Herzegovina, Cyprus, Hungary, Ireland, Liechtenstein, Lithuania, Malta, the Netherlands, Switzerland and UK (but not of authorisations).
No	Andorra, Croatia, France, Luxembourg ,Portugal, Slovak Republic, Ukraine.
NA	Austria, Estonia, Germany, Monaco and Sweden.
No answer	Albania, Finland, Italy and Slovenia, the former Yugoslav Republic of Macedonia.
Unclear	Czech Republic and Serbia.

Table 43b

Andorra	Vu qu'il n'y a pas de communication excepté disposition légale ou autorisation judiciaire un mécanisme de contrôle n'est pas nécessaire. Pour la communication à la sécurité sociale (qui dans le cadre d'un accident de circulation avec des blessés est informée de l'identité et des circonstances lorsqu'une personne physique peut être responsable civil pour pouvoir diriger une demande judiciaire contre celle-ci) celle-ci est expressément prévue par l'accord bilatéral et un contrôle est effectué lors de celle-ci par le fonctionnaire qui réalise la communication et par son supérieur. [Since there is no communication except for statutory provision or judicial authorization, a control mechanism is not necessary. For the communication to social security (that in the context of a traffic accident with casualties is informed of the identity and the circumstances where a natural person may be civilly responsible for directing a judicial claim against such.), such is expressly provided for by the bilateral agreement and a check is performed by the official who makes the communication and by his superior.]

Table 44
When communication to other public bodies has been exceptionally permitted

	Q.47 According to existing records, on how many occasions has communication to other public bodies been exceptionally permitted, in a particular case?
On average 2 per year	**Switzerland: «Aucune réponse à cette question ne peut être fournie en l'absence d'un temps de référence donné. En moyenne deux fois par an, tout système d'information de**

	police de la Confédération confondu.» [No response to this question can be given in the absence of a time-frame of reference. On average twice a year, considering all police information systems of the Confederation.]
No cases	**Croatia; Malta; Portugal, Slovak Republic.**
No information	**Bosnia and Herzegovina; Cyprus; Czech Republic; Hungary; Lithuania; Luxembourg; Serbia; Ukraine.**
NA	**Austria; Germany; Ireland; Liechtenstein; Monaco; Sweden.**
No answer	**Albania; Andorra; France; Italy; Montenegro; the Netherlands; Slovenia; the former Yugoslav Republic of Macedonia; UK.**

Table 45
When communication of police data to private parties is permissible

	Q.48 Principle 5.3: In what circumstances is the communication of police data to private parties permissible? (R87(15) Principle 5.3; Explanatory Memorandum para. 58, 63–64)
No (Absolutely Not)	Albania, Andorra, France
Only if there is a clear legal obligation/authorisation	Austria, Estonia, Hungary
Only clear legal obligation/authorisation & supervisory authority:	Slovenia
Only clear legal obligation/authorisation & judicial authority	Luxembourg, Sweden, UK
Clear legal obligation/authorisation and other circumstances circumscribed by law	Croatia, Germany, Liechtenstein, Lithuania, Switzerland.
Legal obligation/authorisation	Malta, Slovak Republic, The former Yugoslav Republic of Macedonia
Legal obligation/authorisation and consent	Ukraine
Legal obligation/authorisation, authorisation by the AG, other	Cyprus
Court authorisation, other cases	Bosnia and Herzegovina
As provided in the police code of practice	Ireland
Only at the request of the data subject	Italy
Only on the basis of consent	Portugal
No answer	Finland

Table 45b

Germany	In accordance with Section 10 subsection 3 of the Federal Criminal Police Office Act, the Federal Criminal Police Office Act may also transmit personal data to non-public bodies if this is provided by other legislation or if it is necessary for 1. the accomplishment of its tasks pursuant to the Federal Criminal Police Office Act, 2. purposes of criminal prosecution, the execution of a sentence or to issue pardons for state crimes, 3. purposes of threat prevention or 4. the prevention of serious harm to the rights of individuals provided the purposes of criminal prosecution do not prevent such transmission. If there is reason to believe that the transmission of data pursuant to subsection 3 would jeopardize the purpose on which the collection of the data was based, the Federal Criminal Police Office must request the consent of the agency that supplied the data to the Federal Criminal Police Office Act (Section 10 subsection 4 of the Federal Criminal Police Office Act). Section 10 subsections 3 and 4 of the Federal Criminal Police Office Act
Switzerland	«La communication de données de police à des tiers privés n'est autorisée que dans des cas ponctuels et à des conditions restrictives :

	- cf. art. 14 décision-cadre 2008/977/JAI : consentement de l'autorité compétente, aucun intérêt spécifique légitime de la personne concernée ne s'y oppose et la communication est essentielle soit pour l'exécution d'une tâche légalement confiée, soit pour la prévention et la détection d'infractions pénales, soit pour la prévention d'un danger immédiat et sérieux pour la sécurité publique, soit pour la prévention d'une atteinte grave aux droits des personnes (Art. 14 DC 2008/977/JAI) - lorsque ces tiers ont besoin de ces données pour l'accomplissement de leurs tâches. (Art. 19 lit.f LSIP) Une telle communication est réglementée pour chaque système d'information de police, en principe par voie d'ordonnance. Par ex. dans l'ordonnance relative au système de recherches informatisées de police (RIPOL), une telle communication n'est pas expressément interdite ni exclue ; l'ordonnance prévoit que la communication de données à des tiers doit être assortie d'une remarque précisant que les données doivent être traitées de manière confidentielle et qu'elles ne peuvent être transférées à d'autres intéressés. (Art. 7 (al.5) RIPOL Ordonnance) Dans la LMSI (sécurité intérieure), « la communication de données personnelles à des particuliers n'est autorisée que : - si elle est dans l'intérêt indubitable de la personne concernée et que celle-ci ait donné son accord ou que les circonstances indiquent que ce dernier eût été sûrement donné; - si elle est nécessaire afin d'éviter un danger grave immédiat; - si elle est nécessaire pour motiver une demande de renseignements. » (Art. 17 al. 2 LMSI)» [The communication of police data to private parties is allowed only in specific cases and under restrictive conditions: -cf. Art. 14 Framework Decision 2008/977/JHA: consent of the competent authority, no legitimate specific interests of the data subject prevent transmission and transfer is essential for the performance of a task lawfully assigned or for the prevention and detection of criminal offences, or for the prevention of an immediate and serious threat to public security, or for the prevention of serious harm to the rights of individuals; -where such third parties need this data to carry out their tasks. Such communication is regulated for each police information system, in principle by ordinance. For eg. Under the ordinance on the system of computerised searches of the police (RIPOL), such communication is not expressly prohibited or excluded; the Ordinance provides that the communication of data to third parties must be accompanied by a note specifying that the data must be processed confidentially and that they may not be transferred to other interested parties. In the LMSI (internal security), "the communication of personal data to individuals is only allowed: -if it is undoubtedly in the interest of the person concerned and that this person has given his or her consent or the circumstances indicate that such consent would have certainly been given; -if it is necessary to avoid an immediate, serious danger; -if it is necessary to justify a request for information."]

Table 46
Clear legal obligation of police to communicate data to private parties

	Q.49 Are there instances in your law of a clear legal obligation on the police authorities to communicate data to any private parties? Please append the text of the relevant law. *(R87(15) Principle 5.3; Explanatory Memorandum para. 63–64)*
No	Andorra, Bosnia and Herzegovina, Cyprus, Czech Republic, Estonia, France, Germany, Monaco, Ukraine.
None reported (i.e. no categorical "No" response)	Lithuania, Malta, Portugal
Yes	Austria, Croatia, Hungary, Ireland, Liechtenstein, Luxembourg, the Netherlands, Slovak Republic, Slovenia, Sweden, Switzerland, UK.
No answer	Finland, Italy, The former Yugoslav Republic of Macedonia
Not clear	Serbia

Table 47
Where DPA may authorise communication of data to private parties

	Q.50 Are there instances in which the supervisory authority may authorise such a communication of data by the police authorities to any private parties? (R87(15) Principle 5.3; Explanatory Memorandum para. 63–64)
No	Albania, Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, France, Germany, Hungary, Ireland, Liechtenstein, Lithuania, Luxembourg, the Netherlands, Portugal, Sweden, Switzerland, Ukraine, UK
Yes	Malta, Slovak Republic
No answer	Finland, Italy, Slovenia
Not clear	Serbia, The former Yugoslav Republic of Macedonia

Table 48
Where other authorities are empowered to authorise communication

	Q.51 Is any other authority empowered to authorise the police authorities to communicate data to a private party? (R87(15) Principle 5.3; Explanatory Memorandum para. 63–64
No	Albania, Austria, Croatia, Czech Republic, Estonia, France, Germany, Ireland, Liechtenstein, Lithuania, Malta, Monaco, Portugal, Switzerland, The former Yugoslav Republic of Macedonia, Ukraine.
Yes	Andorra (judicial authority), Bosnia and Herzegovina (judicial authority), Cyprus (Attorney General), Hungary (no specification), Luxembourg (judicial authority), the Netherlands (Minister of Security and Justice), Slovak Republic (judicial authority), Slovenia (Information Commissioner), Sweden (judicial authority), UK (judicial authority).
No answer	Finland, Italy
Not clear	Serbia

Table 48b

Switzerland	«La loi ne prévoit pas de mécanisme de contrôle spécifique sur ce point. Elle spécifie seulement quelles autorités sont autorisées à traiter quelles catégories de données et dans quelles finalités. Conformément aux principes généraux de protection des données, « les organes fédéraux ne sont en droit de communiquer des données personnelles que s'il existe une base légale […] ou à l'une des conditions suivantes : - le destinataire a, en l'espèce, absolument besoin de ces données pour accomplir sa tâche légale ; - la personne concernée y a, en l'espèce, consenti ; - la personne concernée a rendu ses données accessibles à tout un chacun et ne s'est pas formellement opposée à la communication ; - le destinataire rend vraisemblable que la personne concernée ne refuse son accord ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes; dans la mesure du possible, la personne concernée sera auparavant invitée à se prononcer ; […] - [également si] la communication répond à un intérêt public prépondérant. […]» (Art. 19 LPD) [The law makes no provision for a specific control mechanism on this point. It only specifies which authorities are authorised to process which categories of data and for what purposes. In conformity with the general principles of data protection law, "federal bodies may disclose personal data if there is legal basis for doing so [...] or if: -the data is indispensable to the recipient in the individual case for the fulfilment of his statutory task; -the data subject has consented in the individual case; -the data subject has made the data generally accessible and has not expressly prohibited disclosure; or --the recipient demonstrates credibly that the data subject is withholding consent or blocking disclosure in order to prevent the enforcement of legal claims or the safeguarding of

	other legitimate interests; -the data subject must if possible be given the opportunity to comment beforehand.; [...]; - [so also] if there is an overriding public interest in its disclosure. [...]]

Table 49
Other circumstances where communication to private parties is authorised

	Q.52 Are there any other circumstances in which the police authorities of your country are authorised to communicate data to private parties (apart from when there exists a clear legal obligation or authorisation)? *(R87(15) Principle 5.3; Explanatory Memorandum para. 63–64)*
No	Albania, Andorra, Austria, Croatia, Estonia, France, Germany, Ireland, Lithuania, Luxembourg, the Netherlands, Slovak Republic, Slovenia, Ukraine.
Yes	Bosnia and Herzegovina, Cyprus, Finland, Hungary, Liechtenstein, Malta, Portugal, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, UK.
No answer	Czech Republic, Italy
Not clear	Serbia

Table 49b

Finland	For the purposes of background checks referred to in section 21 of the Act on the Processing of Personal Data by the Police (Act 761/2003), a private corporation and foundation, whose seat, central administration or main operative unit is located in Finland, and a foreign corporation or foundation that has a registered branch in Finland, may apply for a basic background check on persons seeking an office or position, persons to be admitted to a position or training, or persons who are performing an office or position. However, the data is communicated to the Security Police that is responsible for carrying out the background checks.

Table 50
Where communication to private parties has been exceptionally permitted

	Q.53 According to existing records, on how many occasions has communication to private parties been exceptionally permitted, in a particular case?
Monaco	11 over the last 3 years (2009 – 2011)
No cases	Austria, Croatia, Germany, Slovak Republic, Slovenia, Switzerland
No data provided	Bosnia and Herzegovina, Cyprus, Czech Republic, Estonia, Hungary, Ireland, Lithuania, Luxembourg, Malta, the Netherlands, Portugal, Serbia, Sweden, Ukraine, UK
No answer provided	Albania, Andorra, Finland, France, Italy, The former Yugoslav Republic of Macedonia
Not Applicable	Liechtenstein

Table 51
Where communication to foreign authorities is restricted to police bodies

	Q.54 Principle 5.4: Is communication of data to foreign authorities restricted to police bodies? *(R87(15) Principle 5.4; Explanatory Memorandum para. 65–69)*
Yes	Albania, Austria, Croatia, France, Ireland, Liechtenstein, Luxembourg, Malta, the Netherlands, Slovenia.
Police bodies and judicial authorities	Andorra, Germany, Monaco Germany - Transnational data transfers are permissible only to police and judicial authorities and to other public bodies responsible for the prevention or prosecution

	of crime in other countries as well as to intergovernmental and supranational bodies dealing with the prevention and prosecution of crime (see Section 14 of the Federal Criminal Police Office Act). / Within the EU, under Section 14 (a) of the Federal Criminal Police Office Act data may be transmitted to police and judicial authorities and to other public bodies responsible for the prevention or prosecution of crime.
No, but only in accordance with specific legal acts	Estonia, Lithuania, Portugal, Sweden.
No	Cyprus [the Commissioner issued 9 licenses for the transmission of data to third countries' nationals, requested for claims before a Court relating to road accidents they had been engaged in during their stay in Cyprus]. Finland - There are provisions governing the communication of data to the competent foreign authorities in the Act on the Processing of Personal Data by the Border Guard (579/2005) and in the Customs Act (1466/1994). In addition, section 22 of the Data Protection Act provides for the conditions of transfer of data to non-member states. Personal data may be transferred to outside the European Union or the European Economic Area only if the country in question guarantees an adequate level of data protection. That condition is based on Directive 95/46/EC. Hungary (no details provided). Slovak Republic (no details provided). Switzerland - Law enforcement authorities in the broad sense: not only police authorities, but also prosecuting authorities, migration authorities, road traffic authorities, civilian and military justice authorities, authorities of execution of sentences. The former Yugoslav Republic of Macedonia (no details provided). Ukraine (no details provided)
No (no further details)	Bosnia and Herzegovina.

Table 52
Legal provision for communication of data by a police force to a foreign authority

	Q.55 Is there clear legal provision under national or international law [including bilateral and multilateral international agreements] enabling the communication of data by your police authority to foreign authorities? *(R87(15) Principle 5.4.a; Explanatory Memorandum para. 65–69)*
Yes	Albania, Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, Portugal, Serbia, Slovak Republic, Slovenia, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, UK.
No	Ukraine (?)

Table 53
Communication to foreign authorities where no clear legal provision exists

	Q.56 In the absence of such a provision, in what other circumstances may your police authorities communicate data to foreign authorities?

	(R87(15) Principle 5.4.b; Explanatory Memorandum para. 65–69)
NA*	Albania, Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany,Hungary, Italy, Liechtenstein, Lithuania, Luxembourg, Monaco, the Netherlands, Portugal, Serbia, Slovak Republic, Slovenia, Sweden.
Germany	Data may be transmitted only if provided for by law.
Ireland	Only with the approval of the Commissioner of An Garda Síochána.
Malta	"if the communication is necessary for the prevention of a serious and imminent danger, or necessary for the suppression of a serious criminal offence."
Switzerland	"En l'absence d'une obligation légale (de droit international ou national), le soutien et la communication de données personnelles sont accordés en règle générale selon le principe de réciprocité." [In the absence of a legal obligation (under national or international law), support and communication of personal data are generally granted on the basis of the principle of reciprocity.]
The former Yugoslav Republic of Macedonia,	As an exception to the Article 31 paragraphs 1 and 2 of this Law, the personal data transfer may be performed in the following cases: - if the personal data subject is explicitly consent to the data transfer ; - the transfer is necessary for signing or realization of the contract concluded in the interest of the personal data subject, between the controller and a third party; - the transfer is necessary for protection of the public interest or for the public safety; - the transfer is necessary for determining or meeting individual legal interests; - the transfer is necessary for protection of the life or the essential interests of the personal data subject and - the transfer is performed out of publicly available personal data collections or personal data collections available to a person who shall render his/her legal interest probable, in a scope determined by law. (Article 33) (sic.)
UK	"If no explicit statutory duty exists to facilitate the sharing of information, police forces and foreign third parties (either private entities or other public/law enforcement authorities) can facilitate the sharing of information following the Information Commissioner's Data Sharing Code of Practice."

Table 54
Existence of oversight mechanisms for communication to foreign authorities

	Q.57 Is any oversight mechanism in place with regard to determinations of circumstances warranting the communication of data to foreign authorities? *(R87(15) Principle 5.4; Explanatory Memorandum para. 65–69)*
Andorra	L'intérêt légitime est apprécié par le département de coopération international du service de police de la Principauté qui a comme fonction l'échange de données en matière pénale et reçoit les demandes étrangères ou élabore les demandes dirigées à d'autres services de police étrangers. Cette coopération se réalise principalement par le canal INTERPOL. Seules des autorités de police peuvent adresser des demandes d'information. [The legitimate interest is assessed by the department of international cooperation of the police of the Principality that has the function of data exchange in criminal matters and receives foreign requests or elaborates the requests directed to other foreign police agencies. This cooperation is achieved mainly through INTERPOL. Only law enforcement agencies can submit requests for information.] Le mécanisme de contrôle en vigueur existant consiste à la centralisation des demandes reçues et effectuées à travers du département de coopération international qui détermine quelle autorité de police effectue la demande, quel est le canal utilisé, quel est l'objet de la demande, quelle est la qualité des données, quelles données sont nécessaires pour satisfaire la demande, et quelle est la finalité de celle-ci. Finalement un responsable de ce département supervise et autorise ces communications. / Si l'autorité de police a effectué une demande de données que le service de police ne peut satisfaire elle est informée des motifs. [The control mechanism in force

	consists of the centralization of requests received and carried out through the department of international cooperation which determines which police authority is making the request, what is the channel used, what is the purpose of the request, what is quality of the data, what data are necessary to meet the request, and what is the purpose thereof. Finally an official of this department oversees and authorizes such communications. / If the police authority has made a data request that the police cannot meet, it is informed of the reasons.]
Cyprus	Requires licence issued by DP Commissioner.
Finland	The safeguards under the Act on the Processing of Personal Data by the Police (Act 761/2003). In addition, the Act includes special provisions concerning the right of access to data included in the Europol Data System and the Schengen Information System as well as in the data file maintained by the technical support function of the Schengen Information System.
Germany	The general principles of data protection supervision also apply to data transmission to foreign countries.
Ireland	Oversight mechanisms are operated with Interpol and Europol's headquarters. The Europol National Unit is also subject to inspection by national Data Protection Authorities, and periodic inspections have taken place. The Garda Síochána also has internal audit and professional standards mechanisms in place and is independently overseen by both an Inspectorate and an Ombudsman Commission with legislative basis and high levels of access to data.
Monaco	La communication de données de police par la police monégasque, s'opère par le canal Interpol ou Europol ou sous couvert de la hiérarchie judiciaire. [Data communication by the police of Monaco operates through the Interpol or Europol channels or under the cover of the judicial hierarchy.]
Sweden	The Central Security Log, inspections carried out by the National Police Board, ordinary supervision by the Data Inspection Board and the Swedish Commission on Security and Integrity Protection, extraordinary supervision by the Parliamentary Ombudsman or the Chancellor of Justice.
Switzerland	«Oui. la loi générale de protection des données (LPD) prévoit qu'en principe la communication transfrontière de données n'est pas autorisée en l'absence d'une législation assurant un niveau de protection adéquat. A cet égard le PFPDT évalue régulièrement le niveau des législations étrangères de protection des données et publie une liste des Etats dans lesquels il estime que le niveau de protection des données est suffisant.» [Yes. The general law of data protection (LPD) provides that in principle cross-border communication of data is not permitted in the absence of legislation that guarantees an adequate level of protection. In this respect the PFPDT regularly assesses the levels of foreign laws on data protection and publishes a list of States in which it considers that the level of data protection is adequate.]

Table 55
When data is communicated to foreign authorities in absence of legal provision

	Q.58 According to existing records, on how many occasions have your police authorities communicated data to foreign authorities in the absence of a clear legal provision under national or international law permitting such communication? *(R87(15) Principle 5.4; Explanatory Memorandum para. 65–69)*
No cases	Albania, Andorra, Austria, Croatia, Germany, Ireland, Malta, Monaco, Slovak Republic, Slovenia, Sweden.
No data provided	Bosnia and Herzegovina, Czech Republic, Estonia, Finland, France, Hungary, Italy, Liechtenstein, Lithuania, Luxembourg, the Netherlands, Portugal, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Ukraine, UK.
Specific number of cases provided	Cyprus: The Commissioner has issued 9 licenses for the transmission of data to third countries' nationals, requested for claims before a Court relating to road accidents they had been engaged in during their stay in Cyprus.

Table 55b

Germany	Never, because it is unlawful to transfer data without a legal basis.
Switzerland	«Aucune réponse à cette question ne peut être fournie en l'absence d'un temps de référence donné. Lorsque des données sont transmises à une autorité étrangère en l'absence d'une autorisation légale, cette communication est annoncée au PFPDT conformément à la loi.» [It is not possible to provide an answer to this question in the absence of a given time-frame of reference. When data are transmitted to a foreign authority in the absence of legal authorization, this communication is announced to the PFPDT in accordance with the law.]

Table 56
Circumstances justifying communication of data in absence of legal provision

	Q.59 What circumstances justified such a communication? *(R87(15) Principle 5.4; Explanatory Memorandum para. 65–69)*
NA	Albania, Andorra, Austria, Bosnia and Herzegovina, Croatia, Czech Republic, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, Portugal, Serbia, Slovak Republic, Slovenia, Sweden, The former Yugoslav Republic of Macedonia, Ukraine, UK.
Switzerland	«Traités internationaux de coopération policière ; convention d'application de l'accord de Schengen (CAAS).» [International treaties for police co-operation; Convention implementing the Schengen Agreement.]

Table 57
Information required by countries when requests for communication are received

	Q.60 Principle 5.5.i: What information does your country require to be included when requests for communication of data are made to the police authorities? *(R87(15) Principle 5.5.i; Explanatory Memorandum para. 70–72)*
	Q.61 In particular, is it a requirement that requests for communication of data be justified, i.e. that they include the reason for the request and its objective? *(R87(15) Principle 5.5.i; Explanatory Memorandum para. 70–72)*
	Q.62 Are there any specific provisions contained in national legislation or in international agreements applicable to your country in regard to requests for communication of data? *(R87(15) Principle 5.5.i; Explanatory Memorandum para. 70–72)*
	When faced with a request for information from another country, the countries surveyed all seem to require indications as to the body or person requesting the data as well as the reason for the request and its objective and an indication of the data being requested. It is clear from the responses received that, unsurprisingly, much exchange of police data takes place within the framework of cooperation agreements (including Schengen, Prüm, the European Convention on Mutual Assistance in Criminal Matters etc.) and international police organisations, such as Europol and Interpol.
Germany	There exist explicit legal provisions defining requirements for data communication with EU Member States. Pursuant to Section 14 a subsection 2 of the Federal Criminal Police Office Act, the transmission of personal data may only take place if the request contains at least the following information: 1. name and address of the requesting authority, 2. designation of the offence for the prevention of which the data are required, 3. facts of the case on which the request is based, 4. designation of the purpose for which the data are requested, 5. connection between the purpose for which the information or intelligence is requested and the person who is the subject of this information, 6. details of the identity of the person concerned if the request relates to a known person, and 7. reasons for assuming that relevant information and intelligence is available in Germany.

	Beyond this, there is no other legal provision governing the contents of a request for data transmission. In any case, it must be clear from the request that the applicable legal requirements for the requested data transmission are fulfilled. These may vary (see Section 10 of the Federal Criminal Police Office Act for intra-national data exchange and Section 14 for data exchange in the framework of international cooperation), but always take account of the principle of necessity. Section 14a (2) of the Federal Criminal Police Office Act. The requirement that requests for communication of data be justified is explicitly regulated in Section 14 a subsection 2 of the Federal Criminal Police Office Act. In all other cases, this follows indirectly from the fact that the general principle of necessity applies.

Table 58
Countries with structures in place to verify quality of data communicated

	Q.63 Principle 5.5.ii: Do your police authorities have structures in place whereby, at the latest at the time of their communication, the quality of data is verified? (R87(15) Principle 5.5.ii; Explanatory Memorandum para. 73–75)
Yes	Albania, Andorra, Croatia, Estonia, Finland, Germany, Ireland, Luxembourg, Malta, Portugal, Slovenia, Sweden, Switzerland.
No specific structure reported, but principles apply	Austria, Cyprus, France, Italy, Liechtenstein, Lithuania, the Netherlands, Slovak Republic, UK.
The DPA has got no information	Hungary
No	Monaco
Unclear answer	Bosnia and Herzegovina, Czech Republic, Serbia, The former Yugoslav Republic of Macedonia, Ukraine.

Table 58b

Andorra	Police data of the Principality do not contain personal appreciations or opinions.
Germany	Pursuant to Section 32 (1) of the Federal Criminal Police Office Act, the Federal Criminal Police Office shall rectify personal data stored in data files if they are incorrect. When handling individual cases and at prescribed intervals, the Federal Criminal Police Office checks whether stored personal data need to be rectified or deleted (Section 32 (3) of the Federal Criminal Police Office Act).Section 31 (1) of the Federal Criminal Police Office Act Section 32 (3) of the Federal Criminal Police Office Act
Ireland	Internal supervisory functions; internal audit; Professional Standards Unit; and role of National Criminal Intelligence Unit.

Table 59
Countries with structures in place to check data based on personal opinions

	Q.64 Do your police authorities have structures in place whereby, in all communications of data, judicial decisions, as well as decisions not to prosecute, are indicated and data based on opinions or personal assessments checked at source before being communicated? (R87(15) Principle 5.5.ii; Explanatory Memorandum para. 73–75)
Yes	Albania, Estonia, France, Liechtenstein, Malta, Portugal, Switzerland.
No	Andorra, Croatia, Germany, Ireland.

No specific structure, but general principles apply	Austria, Cyprus, the Netherlands, Slovak Republic, Sweden.
No information	Hungary, Lithuania, Slovenia, UK.
Unclear/irrelevant answer	Bosnia and Herzegovina, Czech Republic, Monaco, Serbia, Ukraine.
No answer	Finland, Italy, The former Yugoslav Republic of Macedonia

Table 59b

Andorra	The police services of the Principality do not systematically dispose of judicial data and therefore communicate that the data transmitted are police data.
Germany	Judicial decisions including decisions to dismiss criminal proceedings can be accessed by persons authorized to access the central register; however, this has no immediate effect on any transmission of data. Whether data are based on personal opinions or assessments refers to the question of accuracy of such data. Insofar it is referred to the general obligation of the Federal Criminal Police Office to verify the accuracy of data.
Ireland	Details of convictions and acquittals are public information. Decisions not to prosecute are not and are not communicated internationally.
Luxembourg	«Toute décision prise au niveau des tribunaux n'est mentionnée qu'avec l'autorisation expresse du Parquet Général. Les données transmises se basent en outre uniquement sur des décisions officielles évitant ainsi toute opinion ou appréciation personnelle.» [All decisions taken at the level of the courts are not mentioned except with the express authorisation of the Prosecutor General. Besides, the data communicated are based solely on official decisions, thus avoiding all opinion or personal appreciation.]

Table 60
Strategies required by law for accuracy of police data

	Q.65 What strategy does the law require in case data which are no longer accurate or up to date are to be or have been communicated? (R87(15) Principle 5.5.ii; Explanatory Memorandum para. 73–7
The communicating body should inform as far as possible all the recipients of the data of their non-conformity	Austria, Croatia, Estonia, Finland, Germany, Liechtenstein, Lithuania, Malta, Monaco, the Netherlands, Slovak Republic, Sweden, Switzerland.
Andorra	Data which are no longer accurate or up to date are not communicated taking into account that only data that have been re-verified are communicated by the department of international cooperation.
Ireland	Where rectification or updating of data materially modifies the data, the data controller must notify any person to whom the data were disclosed during the previous 12 months unless such notification proves impossible or involves disproportionate effort.
Liechtenstein	Incorrect recordings are to be corrected ex officio. The National Police Force must inform a foreign security authority or organization when personal data which have been communicated were incorrectly or unlawfully processed and are therefore to be corrected or deleted. Art. 34i Para. 1 PA and Art. 35 Para. 6 PA
No requirement	Italy, Luxembourg.
Unclear answer	Albania, Bosnia and Herzegovina, Cyprus, Czech Republic, France, Portugal, Serbia, Slovenia, The former Yugoslav Republic of Macedonia, Ukraine, UK.

Table 61
Countries with safeguards in place regarding use for specified purpose

	Q.66 Principle 5.5.iii: Are any safeguards in place to ensure that data communicated to other public bodies, private parties and foreign authorities are not used for purposes other than those specified in the request for communication? *(R87(15) Principle 5.5.iii; Explanatory Memorandum para. 76–77)*
Yes (Legal principle, legal provision or data is transferred on this condition)	Albania, Austria, Bosnia and Herzegovina, Cyprus, Estonia, Finland, Germany, Ireland, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Slovak Republic, Sweden, Switzerland, The former Yugoslav Republic of Macedonia
Yes (further safeguards)	Andorra, Croatia, Germany, Portugal, UK(sanction).
Yes (no further info provided)	Hungary
No	The Netherlands, Slovenia, Ukraine.
Unclear answer	Czech Republic, Serbia.
No answer	France, Italy.

Table 61b

Andorra	«La Loi du 29 décembre 2000 de coopération pénale internationale et de lutte contre le blanchiment d'argent ou de valeurs produit de la délinquance internationale, publiée au bulletin officiel le 24 janvier 2001 et entré en vigueur 6 mois après sa publication établit dans les articles 5 et 6 des protections visant à ce que les données communiquées ne soient utilisées qu'aux seules fins établies dans la demande. / D'autre part les services de police lors d'une demande de données par un service de police étranger communiquent dans le texte de la réponse la formule suivante «Ce document est destiné à l'usage exclusif du destinataire dans le but désigné ou pour les besoins policiers. Il ne peut être porté à la connaissance de tiers qu'avec l'autorisation expresse de l'expéditeur, l'expéditeur se réserve le droit de se renseigner sur l'utilisation de cette information» / Concernant les communications entre services de police ou avec les autorités judiciaires étrangères celles-ci se réalisent à travers du canal INTERPOL qui garantie ces principes.» [The law of 29th December 2000 on international criminal cooperation and the flight against money laundering or of securities that are the product of international crime establishes protections in its articles 5 and 6 so that data communicated are used only for the purposes set forth in the request. On the other hand the police services, following a data request by a foreign police service, communicate in the text of the answer the following formula "This document is intended for the exclusive use of the recipient for the designated purposes or for policing needs. It may not be made known to third parties without the express permission of the sender, the sender reserves the right to learn about the use of this information". With regard to communications between law enforcement agencies or with foreign judicial authorities they are realized through the channel of INTERPOL that guarantees these principles.]
Croatia	e.g. At the request of the competent authority which has transferred the data, the recipient reports on the usage of the received data and the results accomplished.
Germany	First of all, data are transmitted only if necessary (see answers to questions 60 and 61). This helps minimize the risk that the data are processed for other than the agreed purpose. The legal provisions governing data transfers to foreign countries are even stricter: Pursuant to Section 14 subsection 7 sixth sentence of the Federal Criminal Police Office Act personal data may not be transmitted if there is reason to assume that their transmission would be contrary to the objectives of a German law. Moreover, the recipient is obligated by law to use the data solely for the purpose for which they were transmitted (Section 10 subsection 6 first sentence of the Federal Criminal Police Office Act). In the event of data being transmitted to non-public bodies or bodies abroad they must be advised of this obligation (Section 10 subsection 6 third sentence; Section 14 subsection 7 fourth sentence of the Federal Criminal Police Office Act). Data used unlawfully for other than the originally agreed purpose may generally not be used as evidence in court proceedings relating to that other purpose.

	Section 14 (7) of the Federal Criminal Police Office Act Section 10 (6) of the Federal Criminal Police Office Act
Ireland	Handling codes are applied to all data exchanged internationally, limiting its further use and dissemination. Reference must always be made back to the sending authority for specific written permission to use data for purposes other than originally specified.
Portugal	The National Authority for Data Protection is endowed with powers of authority; as such it may block, erase or destroy data and temporarily or permanently prohibit the processing of personal data, including those contained in open networks for data transmission from computer servers located in Portuguese territory (article 22(3/b) of the Law 67/98, of 26 October).
UK	Any processing of personal data pursued by the data controller which is found to be in breach of the principles (in this case likely to be beyond the purposes specified either to the data subject at the time of collection or in any written data sharing agreement between the data controller and third party) outlined the UK Data Protection Act 1998 and therefore not legitimate, can be determined by the Information Commissioner and enforced by several sanctions – such as Civil Monetary Powers up to £500,000 or by the Courts.

Table 62
Requests made for data collected for one purpose to be used for other purpose

	Q.67 According to existing records, have requests ever been made by other public bodies, private parties or foreign police authorities to use the communicated data for purposes other than those specified in the request for communication?
Yes	Ireland, Switzerland.
No	Albania, Andorra, Austria, Croatia, Cyprus, Liechtenstein, Luxembourg, Malta, Monaco, Portugal, Slovak Republic, Slovenia, Sweden, The former Yugoslav Republic of Macedonia.
No data provided	Bosnia and Herzegovina, Czech Republic, Estonia, Finland, France, Germany, Hungary, Italy, Lithuania, the Netherlands, Ukraine.
Unclear answer	Serbia

Table 62b

Ireland	For example, Europol periodically discovers links with new investigations, and requests that the sending country allows their data to be shared with a different investigative group.
Switzerland	«Des demandes du FBI ou d'autres autorités analogues sont adressées en moyenne deux fois par an à fedpol afin d'obtenir toutes les données des systèmes d'information de police de la Confédération relatives à une personne d'une nationalité déterminée.» [On an average of twice a year the Swiss Federal Police receives requests from the FBI or analogous entities with a view to obtaining all available data linked to a person of a given nationality.]

Table 63
Requests acceded to (for data to be used for other purposes)

	Q.68 If yes, to how many of those requests has the communicating police body acceded?
NA	Albania, Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Hungary, Italy, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, Portugal, Slovak Republic, Slovenia, Sweden, The former Yugoslav Republic of Macedonia, Ukraine.
Ireland	While specific data are not available, however the majority would be acceded to if clear justification is provided.
Switzerland	None.

Table 64
Clear legal provision authorising interconnection of files

	Q.69 Principle 5.6: Is there any clear legal provision in the laws of your country that authorises any interconnection of police files with files held for different purposes (for e.g. social security bodies, passenger lists kept by airlines, trade union membership files, etc.)? Please append text. *(R87(15) Principle 5.6; Explanatory Memorandum para. 78–79)* *Q.70 If so, does the clear legal provision state the conditions under which interlinkage can take place?* *(R87(15) Principle 5.6; Explanatory Memorandum para. 78–79)*
No	Albania, Andorra, Hungary, Ireland, Liechtenstein, Lithuania, Monaco, Portugal, Slovak Republic, Slovenia, Sweden, Switzerland, Ukraine.
Yes	Austria, Croatia, Cyprus, Czech Republic, Estonia [no reference provided], Finland, France, Germany, Italy [no specific provisions indicated], Luxembourg, Malta, The former Yugoslav Republic of Macedonia, UK.
No definite response provided	Bosnia and Herzegovina.
No answer	The Netherlands.
Unclear	Serbia.

Table 64b

Finland	Under section 13(3) of Act 761/2003, before data is supplied to the police with the aid of a technical interface, the police shall present an account of data security in the manner referred to in section 32(1) of the Personal Data Act.
Germany	For example and in particular Section 1 of the Act on Setting up a Standardized Central Counter-Terrorism Database of Police Authorities and Intelligence Services of the Federal Government and the Länder (Antiterrordateiengesetz, ATDG). Section 1 of the Act on Setting up a Standardized Central Counter-Terrorism Database of Police Authorities and Intelligence Services of the Federal Government and the Länder (Antiterrordateiengesetz, ATDG) This standardized central counter-terrorism database is run by the Federal Criminal Police Office (BKA), the Federal Police Central Bureau (BPOLD), the Land Criminal Police Offices (LKA), the Federal and Land Offices for the Protection of the Constitution, the Military Counter-Intelligence Service (MAD), the Federal Intelligence Service (BND) and the Customs Criminological Office (ZKA).
Ireland	Data must be sought from such external files in the context of an actual investigation of a crime or potential crime.
Luxembourg	Under Article 34-1 of the amended law of 31 May 1999 on the Police and the General Inspectorate of Police, the police has direct access, in the performance of its duties, by a computer system, to some other state files. Some of these files (e.g. general register of natural and legal persons, file of road vehicles) are interconnected with the general file of the police.
Switzerland	Fedpol operates a network of information systems for police only. Fedpol also operates, in collaboration with the cantons, a system of computerised searches of persons and objects to which access is granted to different types of authorities, among others also to migration authorities (cf Art. 15 LSIP).[131]

Table 65
Where supervisory body may grant authorisation for interconnection of files

[131] Art. 9ss,15 LSIP; Art. 78 LPol projet.

	Q.71 May the supervisory body grant authorisation for the interconnection of files with files held for different purposes, and if so, is such authorisation limited to particular purposes? *(R87(15) Principle 5.6; Explanatory Memorandum para. 78–79)*
Andorra	L'organe de contrôle peut autoriser une mise en relation de fichiers avec des fichiers utilisés à des fins différents mais cette autorisation sera uniquement accordée à des fins particulières qui doivent être de conformité à une disposition légale. [The supervisory body may authorise a linking of files with files used for different purposes, but that authorisation will be granted only for specific purposes which must be in conformity with a statutory provision.]
Yes, not merely 'for the purposes of an inquiry into a particular offence'	Cyprus, Estonia.
Yes (no further specific info as to limitation 'for the purposes of an inquiry into a particular offence')	France, Luxembourg, Malta, Portugal.
No	Germany, Ireland, Monaco, Slovak Republic, Ukraine.
Unclear	The former Yugoslav Republic of Macedonia.

Table 66
Occasions when interconnection of files has been authorised by DPA

	Q.72 According to existing records, on how many occasions and in what instances has the interconnection of files with files held for different purposes been authorised by the supervisory body? *Q.73 What limited purposes, if any, was this authorisation granted for?*
None	Malta
No further information provided	Estonia, France, Luxembourg, Portugal.
Specific information	*Cyprus:* The Commissioner has issued 6 licenses permitting the combination of the Police's filing system with the respective systems of the Department of Population Registry, the Department of Road Transport, the Asylum Service, the Ministry of Foreign Affairs, The Customs and Excise Department and the National Guard. *Andorra:* Cette autorisation à été donnée une seule fois sur la base d'un règlement. / Lors de l'organisation des jeux des petits États européens, la finalité était de garantir la sécurité de l'Etat et consistait à la communication aux services de police des personnes qui se logeaient dans des établissements hôteliers. [This authorization was given only once on the basis of a regulation. / When organizing the Games of the Small States of Europe, the purpose was to ensure state security and consisted in the communication to the police services of persons lodging in hotels.]

Table 67
How many police systems are accessible on-line even if in a secure fashion

	Q.74 How many of your police systems are accessible on-line even if in a secure fashion? *(R87(15) Principle 5.6; Explanatory Memorandum para. 80)*
Albania	There are 8 police systems accessible on-line at the Albanian State Police.
Andorra	Aucun fichier de police n'est consultable par d'autres institutions. Compte tenu que la police andorrane est composée par un seul service celui-ci ne dispose que d'un seul système et

	sa consultation est contrôlée par un programme qui permet de savoir qui consulte quoi, ainsi que d'établir des catégories d'utilisateurs. [No police file may be consulted by other institutions. Taking into account that the police of Andorra are composed of a single service, it disposes of a single system and its consultation is controlled by a programme that allows to know who consults what, as well as to establish categories of users.]
Austria	As a rule, police systems are accessible on-line.
BaH	We don't know.
Croatia	None.
Cyprus	The Police's central filing system is accessible on line by District Police stations and other Units/ Services of the Police through a safe intranet network.
Czech Republic	See http://www.policie.cz/clanek/Police-of-the-Czech-Republic.aspx
Estonia	1 central register contains about 8 sub-information systems.
Finland	All of them, within a secure network.
France	None.
Germany	Police data systems are not available online. The Internet was intentionally excluded as an access to these systems. However, there exists an electronic data network between the Federation and the Länder which is accessible through separate police networks. This data network is run by the BKA as the central agency. The legal basis for this electronic network is Section 11 et seqq. of the Federal Criminal Police Office Act. Section 11 et seqq. of the Federal Criminal Police Office Act.
Hungary	No information provided.
Ireland	The Garda PULSE system.
Italy	Most.
Liechtenstein	None.
Lithuania	There are 7 databases which are accessible on-line.
Luxembourg	Il y a 7 interfaces pour accéder aux bases de données policières.
Malta	The Police general web-site is available on-line.
Monaco	None.
Montenegro	No answer.
The Netherlands	A number of the police systems are on-line accessible. There is no exact overview available.
Portugal	None.
Serbia	(unclear answer)
Slovak Republic	10
Slovenia	3 police records are accessible on-line in limited edition.
Sweden	All the systems are accessible on-line.
Switzerland	Fedpol exploite un réseau de systèmes d'information qui comprend 5 systèmes...Les systèmes sont interconnectés de manière à permettre aux utilisateurs disposant des droits d'accès nécessaires de savoir grâce à une interrogation unique si des personnes ou des organisations figurent dans un ou plusieurs systèmes du réseau. De plus, fedpol exploite d'autres systèmes d'informations de police qui ne sont pas mis en réseau, mais qui sont accessibles en ligne également. [Fedpol operates a network of information systems which includes five systems ... the systems are interconnected to allow users with necessary access rights to know through a single query if people or organizations figure in one or several of the systems on the network. In addition, fedpol operates other police information systems that are not networked, but which are also available online.]
The former Yugoslav Republic of Macedonia,	There are no such systems on the Internet.
Ukraine	None.
UK	The Serious Organised Crime Agency's Elmer database is accessible on-line via the Moneyweb portal.

Table 68
Where domestic legislation permits direct or on-line access to a police file

	Q.75 Does the domestic legislation of your country allow direct access or online access to a file? If yes, does it provide specific safeguards in those cases where direct access or online access to a file is permitted? *(R87(15) Principle 5.6; Explanatory Memorandum para. 80)*
Yes	Albania, Andorra, Austria, Cyprus, Estonia, Finland, France, Germany, Italy, Luxembourg, Slovak Republic, Sweden, Switzerland.
No	Croatia, Liechtenstein, Malta, Monaco, Portugal, The former Yugoslav Republic of Macedonia, Ukraine.
Not specified	Czech Republic, Lithuania, the Netherlands, Serbia, Slovenia.
Unclear	Hungary.

Table 68b

Andorra	L'accès à un fichier en ligne ne peut avoir lieu que lorsque la norme de création le prévoit et que le principe de finalité est respecté, c'est à dire que les données soient utilisées par le destinataire à des fins directement liées aux fonctions légitimes du cédant et du cessionnaire. (art.5.18 du Règlement de l'Agence Andorrane de protection de données.) [Access to an online file can take place only when the creating norm provides for it and when the principle of finality is respected, i.e. that the data is used by the recipient for purposes directly related to the legitimate functions of the transferor and the transferee. (art.5.18 of the Regulation of the Andorran Agency of data protection.)]
Bosnia and Herzegovina	The law contains no provisions which prohibit or allow on-line access to the file.
Germany	Under German law, automated data retrieval processes are admissible only under certain conditions. This is governed by several provisions of the Federal Criminal Police Office Act, e.g. Section 11 subsection 5 and Section 10 subsection 7. A basic prerequisite for the admissibility of automated data retrieval is that the law provides for the manual retrieval of a great number of similar data. Owing to increased risks associated with automated data retrieval the Federal Criminal Police Office Act makes admissibility dependent on a number of additional conditions which are much stricter than those applicable to manual data transmission (individual queries). For example, an automated process for the retrieval of personal data may only be established to perform law enforcement tasks with the approval of the Federal Ministry of the Interior and the Ministries of the Interior and Senate Departments for the Interior at Land level, if this form of data transmission is appropriate because of the large number of transmissions to be made or their particular urgency, taking into account the legitimate interests of the persons concerned. In addition, the Federal Criminal Police Office can set up automated data files containing personal data if this is necessary to fulfil its tasks. For each automated data file containing personal data, which it keeps with a view to fulfilling its tasks, the Federal Criminal Police Office must define the following in an opening order requiring the approval of the Federal Ministry of the Interior: 1. the name of the data file; 2. the legal basis and purpose of the data file; 3. the group of individuals on whom data are being stored; 4. the type of personal data to be stored; 5. the types of personal data serving to open the data file; 6. the delivery or entry of the data to be stored; 7. the conditions under which personal data stored in the data file will be transmitted to which recipients and in which proceedings; 8. the review time limits and the duration of storage; 9. the logging procedure

	The Federal Commissioner for Data Protection and Freedom of Information must be consulted before the order opening a data file is adopted (also see answer to Q 11). Section 11 subsection 5; Section 10 subsection 7; and Section 34 of the Federal Criminal Police Office Act
Slovak Republic	Access read only, not copy; Risk analysis; Security documentation; Rules of personal, premises and industrial security.
Sweden	Swedish legislation allows direct access in specific cases – see e.g. Ch 2 sec 21 Police Data Act (2010:361); With regard to IT-security, pursuant to sec 31 of the Personal Data Act (1998:204) and ch 2 sec 2 of the Police Data Act (2010:361), the controller of personal data shall implement appropriate technical and organisational measures to protect the personal data that is processed.
Switzerland	Switzerland the specific law on police information systems (LSIP) defines expressly and exhaustively, for each information system, the authorities and services (federal, cantonal and foreign) having online access to that system. The law also specifies the purposes for which these data are to be exclusively used.
UK	There is no provision in the UK Data Protection Act 1998 to prohibit such a circumstance. This is in line with the general UK stances of 'that which is not prohibited is by default permitted.'

Table 69
Measures taken by DPA to ensure public is informed of existence of files

	Q.76 Principle 6.1: Does the supervisory authority of your country take any measures so as to satisfy itself that the public is informed of the existence of police files, as well as of the rights of individuals in regard to these files (the requirement of publicity)? *(R87(15) Principle 6.1; Explanatory Memorandum para. 81–82)*
Data controllers obliged to notify a data application to the Data Protection Commission & register publicised	Austria, Bosnia and Herzegovina, Cyprus, Malta, UK.
Otherwise publicising the existence and nature of files	Andorra [publication in Government Gazette], Monaco [publication in Government Gazette]
Register accessible via the Internet	Liechtenstein
Info on website of police/Ministry/Data Protection Authority	Cyprus, Estonia, Finland, Hungary, Ireland, Italy, Liechtenstein, Lithuania, Monaco, Slovak Republic
DPA provide info via media/including website	The Netherlands, Germany, Portugal, Sweden, Switzerland
Organising seminars	Croatia
Other specifics	*Cyprus:* As regards the rights of individuals in regard to [police] files, the Police has adopted a self binding Charter of Citizens' Rights, which is posted on its website and, among other things, informs citizens on how to exercise their rights which are provided for by Law 138(I)/2001.

Table 69b

Andorra	L'article 30 de la Loi 15/2003 de protection de données prévoit obligatoirement que la création, la modification ou la suppression de fichiers de nature publique doit être réalisée au moyen d'une norme de création, qui doit être approuvée par l'entité publique responsable du traitement et qui doit être publiée au Bulletin officiel avant la création, la modification ou la suppression du fichier. / L'approbation de cette norme de création n'est pas nécessaire pour les fichiers de données

	personnelles qui concernent la Sécurité de l'État et investigation et prévention des infractions pénales. [Article 30 of the Data Protection Law 15/2003 provides in a mandatory manner that the creation, modification or deletion of files of a public nature must be performed by means of an establishing norm, which must be approved by the public entity responsible for the processing and which must be published in the Official Gazette before the creation, modification or deletion of the file. The approval of this establishing norm is not necessary for personal data files concerning State Security and investigation and prevention of crimes.]
Germany	As the representative of the general public, the Federal Commissioner for Data Protection and Freedom of Information is involved in the procedure.

Table 70
How requirement of publicity takes ad hoc files into account

	Q.77 In what manner does implementation of the requirement of publicity take account of the specific nature of ad hoc files, in particular the need to avoid serious prejudice to the performance of a legal task of the police bodies? (R87(15) Principle 6.1; Explanatory Memorandum para. 81–82)
NA (no differentiation made between permanent and ad hoc files)	Andorra, Austria, Cyprus, Ireland, Liechtenstein, Monaco, Portugal, Sweden.
Special nature of ad hoc files taken into account	Bosnia and Herzegovina, Estonia, France, Italy, Malta, Switzerland, Ukraine.
Unclear	Czech Republic, Germany, Lithuania, the Netherlands, Serbia, UK.
No answer	Albania, Croatia, Finland, Hungary, Luxembourg, Slovenia, The former Yugoslav Republic of Macedonia.

Table 70b

Ireland	The registration of the Garda Síochána with the Office of the Data Protection Commissioner provides a large amount of detail on files.[132] The entry is not required to include any details that may prejudice the conduct of the functions of the Gardaí.

Table 71
Arrangements for access rights to be exercised by data subject

	Q.78 Principle 6.2: What arrangements does your country provide for the data subject to be able to obtain access to a police file at reasonable intervals and without excessive delay? (R87(15) Principle 6.2; Explanatory Memorandum para. 83–84)
Direct right of access	Albania, Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, Finland, Germany, Hungary, Ireland, Italy, Liechtenstein, Lithuania, Malta, the Netherlands, Portugal, Slovenia, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, Ukraine and the UK.
Indirect right of access	Luxembourg[133]
Both direct and indirect	(France? See ans to Q.87), Monaco (see answer to Q.31)

132 See http://www.dataprotection.ie/registry-details/0315%2FA.htm

133 *Luxembourg* provides an indirect right of access – *via* the article 17 supervisory authority: «Le droit d'accès à un fichier de police ne peut être effectué que de manière indirecte, c'est-à-dire par l'intermédiaire de l'autorité de contrôle article 17. C'est l'autorité qui procède aux vérifications et investigations utiles dans le cadre d'une demande d'accès, elle fait opérer les rectifications nécessaires et informe la personne concernée par la suite que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution (cf. art 17 para (2) de la loi modifiée du 2 août 2002).»

rights of access	
Insufficient information in questionnaire response	Serbia.

Table 71b

Luxembourg	Le droit d'accès à un fichier de police ne peut être effectué que de manière indirecte, c'est-à-dire par l'intermédiaire de l'autorité de contrôle article 17. C'est l'autorité qui procède aux vérifications et investigations utiles dans le cadre d'une demande d'accès, elle fait opérer les rectifications nécessaires et informe la personne concernée par la suite que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution (cf. art 17 para (2) de la loi modifiée du 2 août 2002). [The right of access to a police file may only be exercised in an indirect manner, that is to say via the mediation of the Article 17 supervisory authority. It is this authority that carries out the verifications and investigations within the framework of an access request, makes the necessary rectifications and informs the person concerned that the processing in question contains no data contrary to the conventions, to the law and to its implementing regulations. (Article 17 para (2) of the amended law of August 2, 2002.)]

Table 72
Where system of registration of requests for access to data exist

	Q.79 Does your country operate a system of registration of requests for access to data? (R87(15) Principle 6.2; Explanatory Memorandum para. 84)
Yes	Albania, the Netherlands, Estonia, Hungary, Ireland, Malta, the Netherlands, Slovak Republic, Slovenia, Switzerland (for certain police systems), Ukraine.
No	Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, France, Germany, Liechtenstein, Lithuania, Luxembourg, Monaco, Portugal, Sweden.
Not sure	Czech Republic, UK.
No answer	Finland, Italy, The former Yugoslav Republic of Macedonia.
Other	Bosnia and Herzegovina requires the data controller to operate a system of registration of rejected requests. The Czech Republic reported that while such a requirement is not set in the Police Act, probably some kind of such register is run by the Police because a data subject may only ask for information once in six months.

Table 72b

Andorra	Le service de police demande que la pétition soit faite par écrit et adressées à la direction par la personne intéressée, mais n'enregistre pas ces demandes dans les fichiers détenus par la police. Elles seraient enregistrées dans le fichier de la correspondance mais en aucun cas dans un fichier nominatif de la personne. / Il ne s'agit pas de fichier spécifique mais d'un fichier regroupant toute la correspondance reçue par la direction des services de police. [The Police Department asks that the petition be made in writing and addressed to management by the person concerned, but does not record these requests in files held by the police. They are stored in the file of correspondence but not in a personal file of the person. It is not a specific file but a file containing all correspondence received by the management of police services.]
Ireland	The register is kept as a department record within the meaning of the National Archives Act 1986 which sets out the rules in relation to the keeping and disposal of department records. As a general rule, the Act allows for the retention of a file for 30 years before it is considered for archiving in the Public Archives Office or destruction.
Slovak	Requests are registered according to the internal rules of the Ministry of the Interior of the

Republic	Slovak Republic. In accordance with Art. 69 (14) of Act No 171/1993 Coll. the Police Force shall keep records of every provision and accessibility of personal data for purposes of verification of legitimacy of personal data processing, internal control and assurance of personal data protection and safeguarding.

Table 73
Where registration of access requests are kept separate from other files

	Q.80 If yes, is the register of requests kept separate from the normal criminal files held by the police, and is data deleted from the register after the lapse of a period of time? (R87(15) Principle 6.2; Explanatory Memorandum para. 84)
Yes	Albania, Bosnia and Herzegovina, Estonia, Hungary, Ireland, the Netherlands, Malta, the Netherlands, Slovak Republic, Slovenia, Switzerland, Ukraine.

Table 74
What is required for data subject to obtain access, change or deletion of data

	Q.81 Principle 6.3: What is required of the data subject for her to be able to obtain, where appropriate, rectification or erasure of her data which are contained in a file? (R87(15) Principle 6.3; Explanatory Memorandum para. 85–86)
Albania	Quoted the law declaring that the data subject "has the right to address himself to General Director of State Police" but didn't provide details as to what is required of the data subject to exercise such right
Andorra	Pour exercer le droit de rectification, le responsable peut demander à la personne intéressée qu'elle fournisse les documents nécessaires pour prouver la correction et la réalité des nouvelles données, et il peut rejeter la demande si ces documents n'ont pas été fournis par la personne intéressée ou par son représentant ou s'ils ne prouvent pas la réalité des nouvelles données. [To exercise the right of rectification, the controller may ask the person concerned to furnish the necessary documents to prove the correction and the veracity of the new data, and s/he may reject the application if the said documents have not been provided by the interested person or his/her agent, or if they do not prove the veracity of the new data.]
Austria	Austria also reported that according to their law "Every controller shall rectify or erase data that are incorrect or have been processed contrary to the provisions of this Federal Act ... on a well founded application by the data subject" and that "Insofar as a use of data is not authorised by law, every data subject shall have the right to raise an objection with the controller" but provided no further details as to what is required of the data subject.
Bosnia and Herzegovina	Request to data controller with possibility of filing a complaint with the Personal Data Protection Agency. No further details provided.
Croatia	In Croatia 'right to access, printouts and correction of the data relating to him/her' may happen 'Upon the request of the data subject or that of his/her legal representative or plenipotentiary'. No further details provided.
Cyprus	"The data subject has the right to ask for and receive from the Police without excessive delay and expense the rectification, erasure or blocking of the data". No further details provided.
Czech Republic	'The request has to be done in written form, must be a rightful and cannot be in conflict with the aims of police activities.' No further details provided.
Estonia	'Data subject has to identify himself/herself. Data subject has the right to obtain data regarding him/her, if data is not correct he/she can provide correct data for police to check it or police has to search correct data itself. If erasure of data is requested, police has to check the reason and if there is legitimate reason, erase the data.'

Finland	A data subject who wishes to use the right of access under section 44 of Act 761/2003, must personally make a request to that effect to the keeper of the register or other police unit referred to in subsection 1 of section 44, and to prove his or her identity.
France	A demand must be made to the person responsible for the processing or to the CNIL.
Germany	If it is found that data were stored unlawfully they are corrected, deleted or blocked. This does not require any action on the part of the data subject concerned. Sections 32, 33 BKAG.
Hungary	Request in written form; if the SIS is involved, proper identification is necessary.
Ireland	A data subject has the right to seek to have personal data amended, blocked or erased where it can be shown that it is incorrect. Any such request must be submitted to the Garda Síochána's Data Protection Processing Unit.
Monaco	Selon les possibilités définies par l'exercice du droit d'accès: soit directement auprès du «Maître du fichier»; soit par le biais de la Commission de Contrôle des Informations Nominatives (C.C.I.N.). [Depending on the possibilities defined by the right of access, either directly from the "Master File" or via the supervisory authority (CCIN).]
Italy	Under section 10(5) of Act no. 121/1981, whoever is informed that personal data relating to them are processed in breach of the applicable laws and/or regulations may request the court having jurisdiction on the place where the data controller is established to perform the necessary investigations and order the said data to be rectified, supplemented, erased or anonymised.
Liechtenstein	Any person concerned may demand the correction of incorrect data or the deletion of inadmissible data (Art. 34i Para. 2 PA). Under Art. 11 and 12 of the Data Protection Act, every person may demand information from the National Police Force about police data concerning that person. Art. 34h is reserved (Art. 34g Para. 1 PA). Administrative and formal requirements are specified in Art. 11 DPA and Art. 1 and 2 DPO.
Lithuania	Upon the written, oral or any other request of the data subject.
Luxembourg	«Pour obtenir, le cas échéant, la rectification ou la suppression des données contenues dans un fichier de police, il suffit de saisir l'autorité article 17 par écrit. Après vérification et investigation, c'est l'autorité qui décide si des rectifications s'imposent ou non et en informe la personne concernée.» [In order to obtain, if appropriate, the rectification or suppression of data contained in a police file, it is sufficient to engage the Article 17 authority in writing. After verification and investigation, it is the authority that decides if rectifications should be imposed or not and informs the person concerned.]
Malta	Request in writing.
Montenegro	Data subject may submit a request.
The Netherlands	'Art 25 Police Data Act: a request of rectification.'
Portugal	Declares the right of the data subject…but provides no further details.
Serbia	Provided a reference to the law. No further detail.
Slovak Republic	Providing proof of identity (presenting an ID card or travel document). No further detail provided.
Slovenia	On request of individual who must also provide proof of incompleteness, inaccuracy etc. If request is denied, the data subject may lodge his request before the National Supervisory Body for Protection of Personal Data.
Sweden	Upon a complaint by the data subject. No formal requirements apply but sufficient information in order to find the data in question is necessary.
Switzerland	Il faut que les données traitées soient fausses (inexactes/incomplètes) ou illicites. (Art. 15, 25 LPD) -Art 15 LPD : 1 Les actions concernant la protection de la personnalité sont régies par les art. 28, 28a et 28l du code civil2. Le demandeur peut requérir en particulier que le traitement

	des données, notamment la communication à des tiers, soit interdit ou que les données soient rectifiées ou détruites. 2 Si ni l'exactitude, ni l'inexactitude d'une donnée personnelle ne peut être établie, le demandeur peut requérir que l'on ajoute à la donnée la mention de son caractère litigieux. 3 Le demandeur peut demander que la rectification ou la destruction des données, l'interdiction de la communication, à des tiers notamment, la mention du caractère litigieux ou la décision soient communiquées à des tiers ou publiées. -Art. 25 LPD : 1 Quiconque a un intérêt légitime peut exiger de l'organe fédéral responsable qu'il: a. s'abstienne de procéder à un traitement illicite; b. supprime les effets d'un traitement illicite; c. constate le caractère illicite du traitement. 2 Si ni l'exactitude, ni l'inexactitude d'une donnée personnelle ne peut être prouvée, l'organe fédéral doit ajouter à la donnée la mention de son caractère litigieux. 3 Le demandeur peut en particulier demander que l'organe fédéral: a. rectifie les données personnelles, les détruise ou en empêche la communication à des tiers; b. publie ou communique à des tiers sa décision, notamment celle de rectifier ou de détruire des données personnelles, d'en interdire la communication ou d'en mentionner le caractère litigieux. [It is necessary that the data processed are false (inaccurate/incomplete) or illicit. (Art. 15, 25 LPD) -Art 15 LPD : 1 Actions for the protection of personality are regulated by art. 28, 28a and 28l of the civil code. The applicant may request in particular that the processing of data, including the communication to third parties, be prohibited or that the data be rectified or destroyed. 2 If neither the accuracy, nor inaccuracy of the personal data can be established, the applicant may request that one adds to the data the mention of its contentious nature. 3 The applicant may request that the rectification or destruction of the data, the prohibition on disclosure, to third parties in particular, the mention of the litigious nature or the decision be communicated to third parties or published. -Art. 25 LPD: 1 Anyone who has a legitimate interest may require from the federal body that it: a. refrains from proceeding with an unlawful processing operation; b. removes the effects of an unlawful processing operation; c. notes the unlawful nature of the treatment. 2 If neither the accuracy, nor inaccuracy of the personal data can be proven, the federal agency must add to the data the mention of its contentious nature. 3 The applicant may in particular request that the federal agency: a. rectify, destroy or prevent the communication to third parties of the personal data; b. publishes its decision or communicates it to third parties, including that of rectifying or destroying the personal data, of preventing the communication thereof or of mentioning the litigious nature.] The Canton of Basel-Stadt reported as follows: "Besides the usual means to identify the person requiring rectification etc., i.e. a copy of the identity card, the data subject has no other requirements to fulfil – it must only state its cause, preferably written. It is up to the authority to prove that the contested data are correct and that the data subject's argumentation is wrong."
The former Yugoslav	"Upon the request of the personal data subject..." No further detail provided.

Republic of Macedonia	
Ukraine	The data subject should apply to the owner and provide official documents.
UK	A data subject can either ask the data controller directly for the rectification, blocking, erasure or deletion of their data, but if a data controller fails to comply with this request then a data subject has the right to complain to the Information Commissioner and request that he investigate whether it is likely or unlikely that the data controller has failed to deal with the request appropriately under Section 42 of the DPA.

Table 75
Number of requests received for access, rectification or deletion

	Q.82 According to existing records, how many data subject requests for rectification or erasure of data contained in a police file have been received by the police authorities?
Austria, Bosnia and Herzegovina, Cyprus, Czech Republic, France, Germany, Hungary, Italy, Lithuania, Malta, the Netherlands, Slovak Republic, Sweden, Ukraine, UK.	Don't know
Albania	159
Andorra	none
Croatia	2
Estonia	Hundreds per month
Ireland	Approximately 600 per annum.
Liechtenstein	on average one case per year
Luxembourg	1 or 2 per year
Monaco	Une demande en 2010, laquelle a été satisfaite. [One demand in 2010, which was met.]
Portugal	3 or 4 times in the last 10 years
Slovenia	approx. 5 per year
Switzerland	In 2010 fedpol received 416 requests in all its police information systems.

Table 76
When police data was found to be excessive, inaccurate or irrelevant

	Q.83 According to existing records, on how many occasions were data found to be excessive, inaccurate or irrelevant in application of any of the principles contained in R(87)15?
Don't know	Austria, BaH, Cyprus, Czech Republic, Estonia, France, Germany, Hungary, Italy, Lithuania, Malta, the Netherlands, Slovak Republic, Sweden, Ukraine, UK.
None	Andorra, Croatia, Liechtenstein, Luxembourg, Monaco, Portugal, Slovenia, Switzerland.
Specific Information	*Albania* – some cases (68 requests, of which 39 have been refused). *Ireland* - Due to the large amount of data involved, it is not possible to provide details of the number of occasions on which data were found to be excessive, inaccurate or irrelevant. *UK* - There are 42 cases since 2005 where the Information Commissioner has found in favour of the complainant that the information held by a PA or LEA was inaccurate, excessive or irrelevant.

Table 77
Types of follow-up action re findings of irrelevant, excessive or inaccurate data

	Q.84 What action, if any, was taken or is planned to be taken pursuant to these findings?
Albania	An audit was undertaken, and followed by a report containing recommendations.
Estonia	Effective supervision, arising knowledge and awareness in police sector.
UK	In all 42 cases, remedial action was advised to achieve compliance.

Table 78
Time-frames within which follow-up action is taken

	Q.85 Within what time-frame was such action taken or is expected to be taken?
Albania	Finalised in February 2011.
Andorra	Le responsable du fichier dispose d'un délai maximum d'un mois, à partir du moment où il recevra la demande de la personne intéressée, pour lui communiquer la rectification ou suppression effective des données. [The controller has a maximum period of one month from the moment he receives the request of the interested person, to communicate to him the effective correction or deletion of the data.]
Estonia	1 to 2 years.
Hungary	30 days
Ireland	Data must be either provided or amended, as appropriate, within 40 days. In practice, data are updated and corrected on coming to notice.
Malta	'In the minimum time possible.'
Sweden	'without delay'.
UK	'No specific or average time frame can be conveyed. The case officer will decide this based on the merits of the case.'

Table 79
Instances when rights of access, rectification and erasure were refused

	Q.86 Principle 6.4: In what instances have the rights of access, and thus the rights of rectification and erasure, been refused? Please give examples. (R87(15) Principle 6.4; Explanatory Memorandum para. 87–90)
Andorra	No demand has been made.
Cyprus	'Our Office, so far, has received only one complaint relating to the right for access to Police files. The Police did satisfy the complainant's request but failed to do so within the time frame of four weeks, in line with section 12(3) of the Law. Due to the fact that there was only a delay of few days and given the fact that the Police, in order to satisfy this particular request, had to search for the complaint's data in more than 45 filing systems, some of which were paper filing systems (not automated) the Commissioner decided that in this case it was not necessary to impose to the Police any administrative sanctions.'
Estonia	When the data requested regards ongoing proceedings or surveillance.
France	«Lorsque la sûreté de l'Etat, la défense ou la sécurité publique du traitement sont en cause. Néanmoins, lorsque la CNIL constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause la finalité de ces traitements, elles peuvent être communiquées au requérant (art. 41 loi 6 janvier 1978)» [When the security of the State, defence or public security processing are involved. However, when the CNIL found, in agreement with the controller, that the communication of data contained therein does not affect the finality of these treatments, they may be communicated to the applicant (Art. 41 Law of 6 January 1978)]
Liechtenstein	None.

Monaco	Never.
Switzerland	En 2010, fedpol a refusé, conformément à la loi, dans dix cas d'espèce le droit d'accès, respectivement le droit à l'effacement de données, à des personnes concernées. [In 2010, fedpol refused, in accordance with the law, in ten such cases the right of access, respectively the right to the erasure of data, to the persons concerned.]
UK	'Many cases which we are aware of involve the public wanting to have their criminal record deleted from the Police National Computer (PNC). An example of this can be seen in the case of five people who had minor and/or old convictions but which showed up checks when they applied for employment. They contested that this was irrelevant, excessive and not up to date. However an Information Tribunal found that deletion was not a proportionate response whereas non-disclosure was. See news article http://www.independent.co.uk/news/uk/crime/chief-constables-win-minor-convictions-appeal-1805421.html'

Table 80
Where national law requires police to provide reasoning for restricted access

	Q.87 Principle 6.5: Does the law of your country oblige the police authority to provide the data subject with a reasoned restriction or refusal of the exercise of the data subject's rights to access, rectification or erasure of her data? How are such reasons communicated to the data subject? *(R87(15) Principle 6.5; Explanatory Memorandum para. 91)*
Yes, reason given in writing	Andorra, Austria, Czech Republic, Finland, Germany, Hungary, Ireland, Liechtenstein, the Netherlands, Monaco, Sweden, Switzerland.
Yes, reason 'in an understandable form'	Portugal
Yes	The former Yugoslav Republic of Macedonia, Ukraine
No (cases of Indirect access)	France: «Non. La législation autorise dans certains cas le responsable du traitement à limiter l'exercice du droit d'accès (accès indirect via la CNIL).» [No – in certain cases the legislation authorizes the person responsible for processing to limit the exercise of the right of access (indirect access via the CNIL)] Luxembourg: No – the right of access is not exercised with the police but with the authority established under Article 17.
Cyprus	The law demands a "satisfactory" response: "Section 12(3) of the Law obliges the Police to give to data subjects satisfactory replies. Furthermore, according to section 12(4) of Law 138(I)/2001, pursuant to a Decision of the Commissioner, access to certain files may be waived wholly or partly."

Table 81
When police may refuse to communicate reasons for non-access etc.

	Q.88 In what circumstances may the police refuse to communicate the reasons for a restriction or refusal of the data subject's rights to access, rectification or erasure of data? (R87(15) Principle 6.5; Explanatory Memorandum para. 92)
Andorra	Tout refus d'accès, rectification ou suppression aux données doit être communiqué par le responsable, de manière expresse, à la personne intéressée par écrit, et doit être motivé. [Any refusal of access, correction or deletion of data must be communicated by the controller, in an explicit manner, to the person concerned in writing, and must be justified.]
Cyprus	'The Law does not enable the Police to refuse to communicate to data subjects the reasons for a restriction or refusal of exercising the right to access, rectification or erasure of data.'
Germany	Only if the statement of the actual and legal reasons on which the decision is based would

	jeopardize the purpose pursued by refusing to provide information (usually police purposes), reasons need not be stated for the refusal to provide information. In such cases it should be pointed out to the data subject that he may appeal to the Federal Commissioner for Data Protection or to a court. Section 39 of the Administrative Procedure Act; Section 19 subsection 6 of the Federal Data Protection Act; Section 19 subsection 5 of the Federal Data Protection Act.
Ireland	In circumstances of an ongoing investigation or where security of State issues arise.
Liechtenstein	A file controller may refuse to provide, or restrict or defer the providing of the requested information in cases where: a) a law so provides; b) disclosure of the requested information is prohibited by order of the courts or an authority; or c) he is required to do so due to the overriding interest of a third party. 2) In addition, an authority may refuse to provide, or restrict or defer the providing of the requested information in cases where: a) it is required to do so due to overriding public interests, and in particular in the interests of the internal or external security of the State; or b) the communication of the information may compromise criminal proceedings or other investigative processes. (Art. 12 Para. 1 and 2 DPA)
Monaco	Never
Ukraine	In case the information includes data which belong to the state secret and the requestor has no access to secret documents. (Article 22, 27 of the Law of Ukraine "On State Secret" of 02.10.2003 N1561-12)
Slovenia	'Never, the individual is always notified of the reason.'

Table 82
Where data subject is given information on how to challenge decisions

	Q.89 In either case, is the data subject given information on how to challenge the decision? (R87(15) Principle 6.6; Explanatory Memorandum para. 92)
Yes	Albania, Andorra, BaH, Czech Republic, Estonia, France, Germany, Hungary, Ireland, Liechtenstein, Malta, Monaco, the Netherlands, Portugal, Slovak Republic, Slovenia, Sweden, Switzerland.
Other	*Austria:* 'There is no legal obligation to inform the data subject on the ways and means to challenge the decision.' *Cyprus:* 'The Police's self binding Charter of Citizens' Rights, which is posted on its website does not provide any information regarding the right to appeal to the Commissioner in accordance with the provisions of section 12(3) of the Law.' *UK:* 'This is not a mandatory obligation on Police Authorities but in any response to a subject access request it is recommended practice to refer to the right to contact the Information Commissioner.'

Table 83
Where rights of access, rectification or deletion has been refused

	Q.90 In what sort of real case scenarios has the exercise of such rights been restricted or refused?
Estonia	'For example ongoing surveillance proceedings.'
Malta	'One typical such scenario is that regarding information contained in criminal conducts.'
Ireland	Where it is prejudicial to an ongoing police investigation.
Slovak Republic	If such notification would endanger fulfillment of Police Force tasks according to Art. 2 of the Act No 171/1993 Coll.

Switzerland	«Dans des cas en rapport avec les signalements de la banque de données HOOGAN qui conformément aux bases légales ne doivent pas être effacées et en rapport avec les signalements des systèmes d'information de police RIPOL et SIS dans lesquels une information aurait remis en question le but d'une instruction pénale.» [In cases in connection with the records of the database HOOGAN which in conformity with the legal bases must not be erased and in connection with the records of information systems of the police RIPOL and SIS in which a piece of information would challenge the goal of a criminal investigation.]
UK	'Many cases which we are aware of involve the public wanting to have their criminal record deleted from the Police National Computer (PNC). An example of this can be seen in the case of five people who had minor and/or old convictions but which showed up checks when they applied for employment. They contested that this was irrelevant, excessive and not up to date. However an Information Tribunal found that deletion was not a proportionate response whereas non-disclosure was; Other examples include, however, Mr S. and Marper Vs UK in which a case involving DNA samples where retained on the DNA database for 100 years regardless of the crime in question.'

Table 84
Where law provides for right of appeal to supervisory body or court

	Q.100 Does the law provide for a right of appeal to the supervisory authority or to another independent body (for e.g. a court or tribunal) from a refusal to grant access? R(87(15) Principle 6.6; Explanatory Memorandum para. 92–95)
Yes	Albania, Andorra, Austria, BaH, Croatia, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, Portugal, Serbia, Slovak Republic, Slovenia, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, Ukraine, UK.
Unclear response	Ireland, Italy.

Table 84b

Germany	If no information is provided the data subject can appeal to the Federal Commissioner for Data Protection. Section 39 of the Administrative Procedure Act; Section 19 subsection 6 of the Federal Data Protection Act. If reasons for a restriction or refusal are not given, the data subject may appeal to the Federal Commissioner for Data Protection or to a court. Section 19 subsection 5 of the Federal Data Protection Act. The German legal system provides for the possibility of appeal to the courts.
Ireland	The data subject must be informed of the right to complain to the Data Protection Commissioner. Section 10 of the Data Protection Act 1988 (as amended) provides that the Data Protection Commissioner may investigate, or cause to be investigated, whether the provisions of the Act have been, or are being, or are likely to be complied with in relation to an individual on the basis of a complaint from an individual or on his own volition. If the Commissioner is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter the subject of the complaint, s/he shall notify in writing the individual who made the complaint of his or her decision in relation to it and that the individual may, if aggrieved by the decision, appeal against it to the Court under section 26 of this Act within 21 days from the receipt by him or her of the notification.

Table 85
Where supervisory body is obliged to communicate police data to individual

	Q.101 Is the supervisory authority or other independent body obliged to communicate the data to the individual if there is no justification for refusing

	access? If not, what alternative action could it take? *(R87(15) Principle 6.6; Explanatory Memorandum para. 92–95)*
Yes, the supervisory body is obliged, or allowed, to communicate the data to the individual	Bosnia and Herzegovina, Estonia, Hungary, Monaco, Slovenia, Ukraine.
No, the supervisory authority is not obliged, indeed permitted, to communicate the data	Albania, Andorra, Austria, Croatia, Cyprus, Finland, Germany, Ireland, Malta, the Netherlands, Slovak Republic, Sweden, Switzerland, UK.
Unclear answer	Liechtenstein, Portugal, Serbia.
No answer	Italy, Lithuania.
Other (cases of indirect access)	Luxembourg: «Suivant le principe du droit d'accès indirect, les données ne sont pas communiquées à la personne concernée. Cette dernière est uniquement informée que le traitement ne contient aucune donnée contraire à la loi, aux conventions et aux règlements.» [Following the principle of indirect access, the data are not communicated to the person concerned. The latter is only informed that the treatment contains no data contrary to law, conventions and regulations.] France: «L'hypothèse relève du domaine du juge.» [The hypothesis falls within the domain of the judge.]
Alternative action	If the data controller does not respect the decision of the DPA, alternative action normally involves the DPA having recourse to administrative or judicial action to enforce its decision. E.g. Andorra: S'il n'y a pas de motif de refuser l'accès, soit l'autorité de contrôle soit le tribunal obligerait le service de police à communiquer les données à la personne. [If there is no reason to deny access, either the data protection authority or the court would require the police to communicate the data to the person.] Austria: If the complaint raised by the data subject is successful, the Data Protection Commission's decision has the effect of a declaration that the Data Controller has failed to obey its legal obligation to inform the individual. The Data Controller is then obliged to abide by the decision. Futhermore, § 30 para 6 of the Federal Act concerning the Protection of Personal Data (DSG 2000) applies, which states: "(6) To establish the rightful state, the Data Protection Commission can issue recommendations, unless measures according to §§ 22 and 22a or para 6a are to be taken an appropriate period for compliance shall be set if required. If a recommendation is not obeyed within the set period, the Data Protection Commission shall, depending on the kind of transgression and ex officio, 1. bring a criminal charge pursuant to sects. 51 or 52, or 2. … 3. in case of a transgression by an organ of a territorial corporate body [Gebietskörperschaft], involve the competent highest authority. This authority shall within an appropriate period, not exceeding twelve weeks, take measures to ensure that the recommendation of the Data Protection Commission is complied with or inform the Data Protection Commission why the recommendation is not complied with. The reason may be publicised by the Data Protection Commission in an appropriate manner as far as not contrary to official secrecy." Germany: Generally, the supervisory authority / court obliges the competent body to provide the requested data. Ireland: It is the responsibility of the Garda Síochána to communicate the data. However, if the Data Protection Commissioner finds that the data has not been communicated he can require the Gardaí do so. Section 10 of the Data Protection

	Act 1988 (as amended) provides that if the Data Protection Commissioner is of the opinion that a person has contravened or is contravening a provision of the Act, the Commissioner may issue an enforcement notice requiring the person concerned to take such steps as are specified in the notice, within such time as may be so specified, to comply with the provision. Liechtenstein: - Possibility of an investigation by the Data Protection Office (Art. 29 DPA) - cases of indirect access: Any person may demand a check by the National Police Force as to whether the latter is lawfully processing data about him or her within the scope of State security (Art. 2 Para. 2 PA) or for crime prevention (Art. 2 Para. 1 Subpara. d PA). The Data Protection Office [the supervisory authority] advises the person making the request in an answer which always contains the same wording that either no data concerning such person is being unlawfully processed or, if any errors have been found in the processing of the data, that it has recommended the removal of such errors.

Table 86
Number of appeals to Supervisory Authority regarding non-access to police data

	Q.102 According to existing records, on how many occasions has a denied access request been challenged before the supervisory authority or other independent body?
Ireland	Approximately 6 per year. However, in 2011 nearly 200 complaints were received due to an organised campaign of some 180 complaints on a specific issue.
Italy	No cases have been registered in respect of SIS.
Serbia	'In relation to police authorities somewhere around 10 request for year.'
Slovak Republic	Once.
Switzerland	«Aucune réponse à cette question ne peut être apportée sans temps de référence donné. En 2010, deux décisions de refus de droit d'accès ont été contestées devant le Tribunal administratif fédéral.» [No response to this question can be given without a time reference. In 2010, two decisions refusing access were challenged before the Federal Administrative Court.]
The Netherlands	We know of just one case over which the National Authority for Data Protection has not yet rendered a decision.
UK	Since 2005 (as far as the ICO's records go), the Information Commissioner has received 1100 complaints in the area of Policing and Criminal Records.
No cases	Albania, Andorra, Bosnia and Herzegovina, Croatia, Cyprus, Liechtenstein, Luxembourg, Malta, Monaco, The former Yugoslav Republic of Macedonia
No records	Austria, Estonia, Germany, Hungary, the Netherlands, Slovenia, Sweden, Ukraine.
No answer	Finland, Italy, Lithuania

Table 87
Occasions when supervisory authority decided access refusal not justified

	Q.103 On how many occasions did the supervisory authority or other independent body decide that there was no justification for refusing access, and what action did it take?
Estonia	About 15 cases in last 2 years. Supervisory authority granted access.
Ireland	On an ongoing basis the Office of the Data Protection Commissioner would provide advice to the Gardaí to supply additional data following the review of a complaint. The

	Commissioner has not had to use his legal powers to require such provision as his office receives full cooperation from the Gardaí. The almost unique nature of each complaint received in relation to access means that engagement is almost invariably necessary to tease through issues.
The Netherlands	As regards the Criminal Police and up to now, such has not occurred.
Slovak Republic	The access granted to the data subject was incomplete.
Switzerland	«Aucune réponse ne peut être donnée en l'absence d'un temps de référence donnée. Ni fedpol, ni le PFPDT, n'ont eu connaissance de tel cas ces dernières années.» ["No answer can be given in the absence of a time reference. Niether fedpol, nor the PFPDT, have had knowledge of such cases in recent years. "]
UK	"As stated above, the Information Commissioner has on record since 2005 that his office has investigated 1100 cases of request for assessment against police authorities and of these he has found 273 to compliant unlikely, advising 165 to take remedial action and recommending no remedial action in 108 cases. Various methods have been undertaken to achieve compliance from simply requesting that data original refused to be disclosed be disclosed, to updating procedures to act in accordance with the UK Data Protection Act 1998 or the Information Commissioner's view, or disclosing the information in another format that would not breach the Data Protection Act."

Table 88
Measures taken to ensure that police data is deleted when no longer necessary

	Q.104 Principle 7.1: What measures are taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored? *(R87(15) Principle 7.1; Explanatory Memorandum para. 96)*
Albania	None
Andorra	[no answer]
Austria	Security authorities shall check personal data processed with computer assistance which have remained unchanged for six years as to whether they are not to be corrected or deleted under para (1). In addition, specific rules and time-limits for regular correction and deletion apply to the "Information Collection Center" (a police database established under § 57 of the Security Police Act).
Bosnia and Herzegovina	Unclear (bare reference to a law is provided, but the text of the law is not appended)
Croatia	Unless otherwise prescribed by the law, the data stored in personal data filing system which is kept on the information system of the Ministry of Interior, needs to be erased without any delay... after the lapse of time limits set in Article 26 of this law... and after the lapse of time limits prescribed by the special law (with reference provided to the Law on Police Affairs and Powers, Art. 26 and The Act on Personal Data Protection, Art. 20.)
Cyprus	Section 25 of the Police Law (Law 73(I)/2004) contains specific provisions for the deletion of fingerprints photographs and DNA data. Law 70/1981, which regulates the rehabilitation of convicted persons, contains specific provisions for the deletion of convictions. Law 183(I)/2007, which regulates the retention of telecommunication data for the purpose of investigation of serious crimes, contains specific provisions for the deletion of telecommunication and electronic communication data, collected by the Police from service providers, which are no longer of use to the Police. The State Archives Law of 1991 (Law 208/1991) contains specific provisions for the deletion and/or storage of Police administrative paper files. Police Internal Regulation 1/45 provides for the destruction of Police paper files

	(books, registers, documents). Closed criminal files are stored/ archived but not destroyed.
Czech Republic	The Police are obliged to examine the necessity of all processed personal data at least once every three years; In the case of the register of undesirable persons, once a year or at any time that the Police have any reason to doubt the justification for the inclusion (Article 20 of the Act on the Protection of Personal Data applies). Compliance with the respective provisions was the subject of multiple inspections carried out by the DPA, including those initiated by the complaint lodged by the data subject. Deletion practice (including deletion logs) and occurrence of "old" data is a standard part of on-site inspection procedure. According to the findings by the DPA inspectors standardized deletion procedures are in place as a rule, including bulk deletion in certain files.
Estonia	"There are automated deletion after time period provided by Statutes of Police Database. There is also automated mechanism that erase certain data after criminal or misdemeanour proceeding comes to an end. Manual deletion is also possible and it is always logged."
Finland	Chapter 5 of Act 761/2003 provides for detailed provisions on the deletion and archiving of data included in the various police data files.
France	«Outre les contrôles de la CNIL, des contrôles internes existent, organisés par le responsable du traitement. Selon les cas, le procureur de la République peut s'assurer de l'effacement ou un magistrat peut être spécialement affecté à ce contrôle.» [In addition to the controls of the CNIL, internal controls are organized by the controller. Depending on the case, the prosecutor of the Republic can ensure erasure or a judge may be specially assigned to this control.]
Germany	A decision on whether the data are still needed is taken on the merits of each individual case. Every time data are stored, a time limit is defined within which the data have to be reviewed for relevance and erasure. Section 32 subsections 3 and 4; Section 33 of the Federal Criminal Police Office Act.
Hungary	Generally an automated system is put in place for the deletion but in case the data is not deleted and it comes to the attention of the DPA, it takes the necessary measures.
Ireland	According to the An Garda Síochána Data Protection Code of Practice, all electronic and manual data is retained in line with the Garda Commissioner's policy on records management. For the purpose of retention, data will be categorised into essential and non-essential files. Specific timeframes will be established in respect of the retention of all data contained on such files within the Garda Síochána. / All investigation files and incident records regarding headline and indictable crimes and incidents will be retained for 30 years as departmental records in line with the provisions of the National Archives Act 1986. Decisions in respect of the further retention of such files will be made on a case by case basis following the 30 year period (Section 4.7 of the An Garda Síochána Data Protection Code of Practice).
Italy	No measures specified.
Liechtenstein	Personal data may only be processed for as long as is necessary for the performance of the tasks but at the latest until the expiry of the period of storage fixed by Government ordinance; the data must then be anonymized or destroyed. Art. 34e Para. 1 PA
Lithuania	"Every register or information system has its regulations in which it is determined, when and how (automatically or manually) personal data, if they are no longer necessary for the purposes for which they are stored, are deleted, also, how monitoring is carried out, etc." [unclear whether these regulations are laws or internal regulations.]
Luxembourg	«Suppression automatique par procédure informatique des informations contenues sous forme électronique. Destruction physique des supports papiers.» [Automatic

	removal of information in electronic form by computerised procedure. Physical destruction of paper documents.]
Malta	Declared that reviews take place at regular intervals.
Monaco	Lors de la déclaration du traitement, un délai de conservation est défini. Au terme de celui-ci, les données sont effacées. [When a declaration of processing is made, a retention period is set. When the term expires, the data are erased.]
Montenegro	No answer.
The Netherlands	'The police Data Act provided in a maximum storage time of the data from a half year up to 5 years and an obligation of a check within a certain period.'
Portugal	Retention periods are set up according to the database to which the data belong. No further detail provided as to "measures taken" as such.
Serbia	Unclear response.
Slovak Republic	The Police Force at least once over 3 years verifies whether processed personal data are further necessary for fulfillment of the Police Force tasks – Art. 69(8) of the Act No. 171/1993 Coll. There are provisions of special Acts on the time period for personal data retention in place. Internal Acts stipulate how information and personal data are destroyed.
Slovenia	Technical measures which follow the regulation in relevant laws.
Sweden	Registers are programmed to be deleted automatically after the lapse of a stipulated period of time according to law or ordinance.
Switzerland	«1) Contrôles des blocs de données par l'organe responsable des systèmes d'informations de police (fedpol). 2) De plus, selon les systèmes, avertissement automatique des délais de conservation des données arrivant à échéance (par ex. SIS, ISIS-LMSI). 3) Enfin, l'autorité de surveillance (PFPDT), effectue des contrôles des données traitées et de la gestion de l'organe responsable des traitements de données dans les systèmes d'information de police. (Art. 6 al. 3 LSIP; Art. 27 LPD)» [1) Checks of data blocks by the body responsible for police information systems (fedpol). 2) In addition, according to the systems, automatic warning of delays of conservation of data which have reached their term (eg. SIS, ISIS-LMSI). 3) Finally, the supervisory authority (PFPDT) performs checks of processed data and the management of the body responsible for the processing of data within the police information systems. (Art. 6 para. 3 LSIP, Art. 27 LPD)]
The former Yugoslav Republic of Macedonia	There is a special Commission that decides on the issues of keeping or deleting of particular data.
UK	The Management of Police Information (MOPI) guidance outlines what measures should be taken to ensure that police data is not kept longer than is necessary. It states that information must be retained for at least six years.
Ukraine	Merely quoted the law stipulating when data should be deleted.

Table 89
Countries where rules have been established for time-limitation of police files

	Q.105 Principle 7.2: Has your country established rules aimed at fixing storage (or conservation) periods for the different categories of personal data collected and stored for police purposes? *(R87(15) Principle 7.2; Explanatory Memorandum para. 97–99)*
Yes	Albania, Austria, BaH, Croatia, Cyprus, Czech Republic, Finland, France, Germany, Hungary, Ireland, Luxembourg, the Netherlands, Estonia, Italy, Luxembourg, Monaco, the Netherlands, Portugal, Slovak Republic, Slovenia,

	Sweden, Switzerland, UK.
No	Malta, Ukraine.
Legislation in the pipeline	Italy and Liechtenstein.
Internal regulations	Lithuania, Serbia, UK.
No answer	Andorra, Montenegro

Table 90
Authority responsible for rules determining time-limitation

	Q.106 Who or which authority was responsible for formulating the rules. Please describe the content and application of the said rules. Kindly provide a reference to the rules and attach the relevant text. *(R87(15) Principle 7.2; Explanatory Memorandum para. 98)*
Albania	Laws formulated by the Ministry of Justice and other regulation formulated by the General Directorate of State Police or by the latter in cooperation with the Commissioner for Personal Data Protection
Andorra	[no answer]
Austria	Federal law
Bosnia and Herzegovina	The police authority is responsible for issuing instructions.
Croatia	By law.
Cyrpus	The Law empowers the Council of Ministers to make Regulations on the Commissioner's recommendation.
Czech Republic	By law.
Estonia	Police body, Ministry of the Interior, Data Protection Authority.
Finland	The legislation on police data files is at the responsibility of the Police Department of the Ministry of the Interior.
France	No answer.
Germany	The legislator.
Hungary	"We have got no information, most definitely the Ministry of Justice or Interior."
Ireland	The Code of Practice on Data Protection in the Garda Síochána (from where the said rules emanate) was developed by the Garda Síochána in co-operation with the Office of the Data Protection Commissioner and has been approved by the Data Protection Commissioner under section 13 of the Data Protection Act 1988.
Italy	Legislation in the pipeline by Presidential decree to be adopted upon a resolution by the Council of Ministers following the proposal put forward by the Home Affairs Minister jointly with the Minister of Justice
Liechtenstein	National Police in cooperation with the Data Protection Office
Lithuania	Regulations of registers and information systems are approved by resolutions of the Government
Luxembourg	Le pouvoir réglementaire était chargé de formuler ces règles.
Malta	NA
Monaco	Le législateur et le pouvoir réglementaire. [The legislator and regulatory power.]
Montenegro	No answer.
The Netherlands	By national law.
Portugal	The Assembly of the Republic
Serbia	"Decisions on such matters shall be issued by the Minister, by regulation, possibly Secretary of State in the Ministry of Internal Affairs."
Slovak Republic	Controller of the information system – the Ministry of the Interior of the Slovak Republic.
Slovenia	"The Police and other public services in accordance with the law."
Sweden	These rules are formulated in law or ordinance, thus the Parliament or the

	Government.
Switzerland	Soit l'organe responsable du système d'information (comme fedpol s'agissant des systèmes d'information de police) établit ces règles en application de principe de proportionnalité. ... Soit ces règles sont fixées par le législateur. Les lois fédérales au sens formel sont soumises à l'adoption du Parlement fédéral et au référendum facultatif (approbation par la population suisse). De plus, lorsqu'une base légale est créée ou modifiée, le PFPDT est consulté préalablement. [The body responsible for the information system (such as fedpol in the case of police information systems) establishes these rules in application of the principle of proportionality. ... Or these rules are set by the legislature. The federal laws in the formal sense are subject to the adoption of the federal Parliament and to an optional referendum (approved by the Swiss population). In addition, when a legal basis is created or modified, the PFPDT is consulted beforehand.]
UK	The Association of Chief Police Officers (ACPO) and the National Policing Improvement Agency (NPIA) formulated the MOPI guidance with input from the Information Commissioner's Office.

Table 91
Where countries have established rules aimed at data quality

	Q.107 Has your country established rules aimed at regular checks on the quality of personal data collected and stored for police purposes? (R87(15) Principle 7.2; Explanatory Memorandum para. 98)
Yes	Albania, Austria, Croatia, Czech Republic, Germany, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Liechtenstein, Lithuania, Luxembourg, Monaco, Sweden, Switzerland.
No	Malta, Cyprus, Slovenia.
Internal regulations	Bosnia and Herzegovina, Estonia, UK.
No specific law reported	Bosnia and Herzegovina.
No answer	Andorra, Finland, France, Slovak Republic, Ukraine.

Table 91b

Germany	Yes. Checks can be carried out by the Federal Commissioner for Data Protection and Freedom of Information and the data protection commissioners of the various public bodies. In individual cases, a review can be carried out by a court.
Ireland	The Garda Information Services Centre (GISC) are tasked with quality assurance of data entered into PULSE by both Garda members and GISC staff on foot of incident reports phoned in by Garda members. The Gardaí also have a data analysis service which utilises data analysts to determine crime trends, etc. but also has the added benefit of identifying erroneously entered or missing data.
Italy	The Joint Police Data Processing Center carries out sample checks on the quality of data.

Table 92
Authority responsible for rules aimed at data quality

	Q.108 Who or which authority was responsible for formulating the rules. Please describe the content and application of the said rules. Kindly provide a reference and attach the relevant text. (R87(15) Principle 7.2; Explanatory Memorandum para. 98)
Albania	Laws formulated by the Ministry of Justice and other regulation formulated by the General Directorate of State Police or by the latter in cooperation with the

	Commissioner for Personal Data Protection
Andorra	No answer.
Austria	Federal law
Bosnia and Herzegovina	Instructions from the Police authorities.
Croatia	By law (which simply declares the principle of implementing data quality)
Cyprus	NA
Czech Republic	Legal obligation & police internal regulations.
Estonia	Supervisory Authority, Police Information Security Department, Ministry of Internal
France	No response.
Germany	The legislator.
Hungary	Police authorities.
Ireland	The Code of Practice on Data Protection in the Garda Síochána (from where the said rules emanate) was developed by the Garda Síochána in co-operation with the Office of the Data Protection Commissioner and has been approved by the Data Protection Commissioner under section 13 of the Data Protection Act 1988.
Italy	By law
Liechtenstein	National Police in cooperation with the Data Protection Office. The National Police Force checks the processed data at the latest every five years for topicality and the need for further processing. Data no longer needed are deleted.
Lithuania	Resolutions of the Government.
Luxembourg	Le pouvoir législatif était chargé de formuler ces règles.
Malta	NA
Monaco	Procédures internes de contrôle par voie hiérarchique et examen par la Commission de Contrôle des Informations Nominatives dans le cadre des formalités préalables et du contrôle a posteriori. [Internal control procedures through official channels and review by the Commission de Contrôle des Informations Nominatives within the framework of preliminary formalities and a posteriori control.]
Montenegro	*No answer.*
The Netherlands	*By national law.*
Portugal	*"The National Authority for Data Protection has powers of investigation, may perform inquiries, access the data, object of the processing and gather all the information required to carry out control and supervision functions pursuant to article 22(3/a) of the Law 67/98, of 26 October."*
Serbia	*Unclear response.*
Slovak Republic	*Controller of the information system – the Ministry of the Interior of the Slovak Republic.*
Slovenia	*The Police – General Police Directorate*
Sweden	*These rules are formulated in law or ordinance, thus the Parliament or the Government.*
Switzerland	Soit l'organe responsable du système d'information (comme fedpol s'agissant des systèmes d'information de police) établit ces règles en application de principe de proportionnalité. ... Soit ces règles sont fixées par le législateur. Les lois fédérales au sens formel sont soumises à l'adoption du Parlement fédéral et au référendum facultatif (approbation par la population suisse). De plus, lorsqu'une base légale est créée ou modifiée, le PFPDT est consulté préalablement. [The body responsible for the information system (such as fedpol in the case of police information systems) establishes these rules in application of the principle of proportionality. ... Or these rules are set by the legislature. The federal laws in the formal sense are subject to the adoption of the federal Parliament and to an optional referendum (approved by the Swiss population). In addition, when a legal basis is created or modified, the PFPDT is consulted beforehand.]
UK	*No answer. ("The ICO cannot answer this question.")*

Table 93
Measures taken to ensure physical and logical security of police data

	Q.109 Has the "responsible body" (i.e. the controller of the police files) taken all the necessary measures to ensure the appropriate physical and logical security of the personal data collected and stored for police purposes, and to prevent unauthorised access, communication or alteration thereto? *(R87(15) Principle 8; Explanatory Memorandum para. 100)*
Yes	Andorra, Austria, Bosnia and Herzegovina, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Hungary, Ireland, Lithuania, Luxembourg, Malta, Monaco, Portugal, Slovak Republic, Slovenia, Sweden, Switzerland, The former Yugoslav Republic of Macedonia.
No answer	Ukraine, UK

Table 93b

Andorra	La sécurité physique des données est pleinement assurée compte tenu que des accès sont limités et contrôlés par de moyens techniques qui permettent d'une part de savoir qui a consulter quelles informations, que cette personne ne puisse pas modifier ou détruire celles-ci, et finalement pour quels motifs elle à fait cette consultation. / La sécurité logique des données est assurée informatiquement par un système de droit d'accès, de droit de modifications, d'historique des accès, création, impression et modification. Postérieurement un centre de traitement des données effectue les vérifications pour garantir cette sécurité et fiabilité des données. [The physical security of data is fully secured given that access is limited and controlled by technical means that allow on the one hand to know who has accessed what information, that such person may not alter or destroy such information, and finally for what reasons such person made such consultation. Logical security of data is ensured by a system of right of access, right to make changes, log of access, creation, modification and printing. Subsequently, a data processing center conducts audits to ensure the security and reliability of the data.] Tous les fonctionnaires de police ne disposent pas des mêmes droits d'accès ni des mêmes compétences pour enregistrer ou modifier des données. Ces droits sont établis par la direction des services de police et dépendent des compétences exercées, des catégories de fonctionnaires et des nécessités du poste de travail. [Not all police officers have the same access rights or the same powers to save or change data; these rights are established by police management depending on the skills performed, the category of staff and the needs of the workplace.]
Czech Republic and Hungary	Checks/inspections carried out by their data protection authorities
Italy	The *Garante* carried out investigations in 2005 to verify appropriateness of the security measures the law requires to be in place regarding the personal data processed by the DPC of the police. Following those investigations – which highlighted several criticalities in terms of data security – the Garante issued a decision (on 17 November 2005) requiring the Public Security Department to take security measures that should enhance the protection of DPC information.
Liechtenstein	Police data and especially the information systems must be protected from misuse by approved technical and organizational measures as specified in Art. 9 of the Data Protection Act. Art. 9 DPA and Art. 34f PA. The National Police is technically connected to the public administration. The IT infrastructure is generally organized by a central public authority. In this respect the Data Protection Office is in permanent contact with those responsible in connection with IT security. In this regard they are aware that technical and organisational measures have been implemented.

Table 94
Where are different characteristics and contents of police data taken into account

	Q.110 For these purposes, have the different characteristics and contents of files containing personal data collected and stored for police purposes been taken into account? *(R87(15) Principle 8; Explanatory Memorandum para. 100)*
Yes	Andorra, Bosnia and Herzegovina, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Hungary, Ireland, Lithuania, Luxembourg, Malta, Monaco, Portugal, Slovak Republic, Slovenia, Sweden, Switzerland, The former Yugoslav Republic of Macedonia.
No answer	Ukraine, UK.
Other	*Andorra:* Not all police officers have the same access rights or the same powers to save or change data; these rights are established by police management depending on the skills performed, the category of staff and the needs of the workplace. *Italy:* "In its decision of 17 November 2005, the Garante considered encrypted storage to be both necessary and appropriate in order to protect – at least – certain data categories. During the investigations that led to the above decision, the Public Security Department informed the Garante that they had relied on encrypted storage with regard to especially confidential information contained in their filing systems." *Liechtenstein:* Art. 21 para. 1 DPO provides that the responsible authorities shall draft processing regulations for automated files which: a) contain sensitive data or personal profiles; b) are used by more than one authority; c) are made accessible to foreign authorities, international organisations, or private individuals; or d) are linked to other files. "[The Data Protection Office is] aware that the National Police has a processing regulation for automated files where needed." Art. 9 DPO describes the general minimum requirements for data security. More detailed rules have been issued by the Government in the DPO in Art. 20 ff."