PERSONAL DATA PROTECTION

DEPARTMENT FOR THE EXECUTION OF JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS

DG1

THEMATIC FACTSHEET

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

September 2022

PERSONAL DATA PROTECTION

These summaries are made under the sole responsibility of the Department for the Execution of Judgments of the European Court and in no way bind the Committee of Ministers.

1. PERSONAL DATA PROTECTION 3

1.1. Collection and use of personal data 3

1.2. Search and seizure of personal data including correspondence 7

1.3. Monitoring of correspondence in prison 9

1.4. Health-related personal data 13

1.5. Access to and erasure or destruction of personal data 15

2. SECRET SURVEILLANCE 18

2.1. Interception of communications and personal data 18

2.2. Surveillance in the workplace 22

2.3. Mass surveillance 23

Index of cases 26

The protection of personal data is of fundamental importance to a person's enjoyment of their right to respect for private and family life, home and correspondence, as guaranteed notably by Article 8 of the Convention. In its case-law, the European Court has referred to the concept of "personal data" used in the Council of Europe Convention ETS No. 108 for the protection of individuals with regard to automatic processing of personal data and has adopted a broad definition of personal data as "any information relating to an identified or identifiable individual".

The European Court also noted that technological developments with regard to the "automatic processing" of data had led, over the last decades, to enormous challenges for personal data protection, in particular with regard to modern operational possibilities of surveillance, interception of communications and/or data retention.

The present factsheet provides examples of general and individual measures reported by States in the context of the execution of the European Court's judgments concerning various aspects of the protection of personal data: collection and use of personal data, search and seizure of personal data, including correspondence, monitoring of correspondence in prison, health-related personal data, access to, erasure and destruction of personal data, interception of communications and personal data, surveillance in the workplace and mass surveillance.

1. PERSONAL DATA PROTECTION

1.1. Collection and use of personal data

The case concerned the retention and failure to return to the applicant items seized in the context of a criminal investigation due to their negligent loss by the Prosecutor's Office (personal and business correspondence, accounting documents, video cassettes containing business meeting recordings and international passport). In 2000, the Code of Criminal Procedure was amended to ensure that any refusal by the investigating or prosecuting authorities to return seized items is subject to judicial review. Compensation can be requested under Article 49 of the Law on Obligations and Contracts.

BGR / Krasimir Yordanov (50899/99)

Judgment final on 15/05/2007

Final Resolution CM/ResDH(2016)306

The case concerned an infringement of the applicant's right to respect for reputation and honour (as an integral part of his right to private life) by a domestic judgement which identified him by his name as having harassed a work colleague, although the defendant in the case was not him but his local authority employer. The domestic ruling had thus stigmatised him and was likely to have had a major impact on his professional standing, honour and reputation.
In 2019, the Court's judgment was analysed by the General Judiciary Council in a report underlining that domestic courts have the obligation to adequately balance the constitutional rights and interests of the parties concerned (on the one hand, the right to judicial protection and defence, procedural safeguards linked to the principle of transparency and the need to reason decisions and resolutions and, on the other hand, the right to privacy and the protection of personal data (requiring that the inclusion of identifying data (or their anonymization) be reasoned with regard to its legal purpose and proportionality.) Specific training sessions in this respect were organised at the Academy of Judicial Training.

ESP / Vincent Del Campo (25527/13)

Judgment final on 06/11/2018

Action Report DH-DD(2019)1004

The case concerned the authorities' disproportionate interference with the applicant's private life due the publication in the State Gazette, based on provisions of the Disclosure Act 1995, of information about the applicant's service in the KGB as a driver during 1980-1991. The last of such publications in the State Gazette on the same grounds took place in 2009. In light of the present judgment, from now on, the Internal Security Service (KAPO) will carry out the proportionality test before disclosing a person's name and other data.

EST / Soro (22588/08)

Judgment final on 03/12/2015

Final Resolution CM/ResDH(2017)152

This case concerned an applicant, sentenced in the context of a demonstration, whose refusal to undergo DNA testing and be included in the national computerised DNA database (FNAEG) resulted in a criminal conviction. The European Court underlined that no action had been taken upon the Constitutional Council's decision from 2010 requiring - with regard to the DNA database - a determination "of the duration of storage of such personal data depending on the purpose of the file stored and the nature and/or seriousness of the offences in question" and ruled that the regulations on the storage of DNA profiles in the FNAEG did not provide the data subjects with sufficient protection.
Following the Court's judgment, some domestic courts adapted their case-law to avoid the criminal conviction of persons refusing to undergo DNA testing for inclusion in the FNAEG. Subsequently, in October 2021, the Code of Criminal Procedure and the provisions concerning the FNAEG were amended by decree in order to implement the 2010 Constitutional Council's decision and the ECHR's judgment. Thus, the DNA profile of a person convicted of one of the

FRA / Aycaguer (8806/12)

Judgment final on 22/09/2017

Final Resolution CM/ResDH(2022)84

offences referred to in section 706-55 of the Code of Criminal Procedure is kept for 25 years and only exceptionally for 40 years, for acts considered to be of particular gravity. These periods are set at 15 and 25 years for minors. In addition, a law of March 2019 now also allows convicted persons to seek early removal of their DNA profiles from the FNAEG.

The case concerned the collection and retention of the applicant's fingerprints in the National Fingerprint database ("the FAED") in the context of an investigation against him concerning a book theft, which ended with a decision not to prosecute. Following the Court's judgment finding a disproportionate interference with the applicant's private life, his fingerprints were deleted from the database.
In December 2015, a decree modifying the FAED Decree of 1987 was adopted, limiting its application to serious crimes and major offences. It also introduced a distinction between the systems for retaining the fingerprints of persons against whom the judicial authority considered that there were insufficient charges and the others. Regarding persons who receive a final court decision declaring their innocence (discharge or acquittal), the data will be immediately and automatically deleted. In case of dismissal or discontinuation for insufficient charges, the data can be deleted upon the request of the person concerned but may be retained for three to ten years, depending on the nature of the offence. After expiry of these deadlines, data deletion is automatic.

FRA / M.K. (19522/09)

Judgment final on 18/07/2013

Final Resolutionμ CM/ResDH(2016)310

The case concerned the unauthorised disclosure of the applicant's telephone records, provided by the national landline telephone operator to the adversary party in the context of civil inheritance proceedings, and their use by the domestic court to dismiss, in part, the applicant's claim for exoneration from court fees.
To prevent similar violations, the 2011 Law on the protection of personal data created an authority to control personal data processing, the National Centre for the Protection of Personal Data, with the duty to monitor the respect for the legislation on protection of information, and in particular, the right to information, data access and interference. A National Data Protection Strategy and an Action Plan for its implementation were adopted for 2013-2018. Relevant training activities for judges and other legal professionals were organised by the National Institute of Justice.

MDA / Savotchko (33074/04)

Judgment final on 28/06/2017

Final Resolution CM/ResDH(2018)130

The case concerned the failure of the domestic courts to protect the applicant's private life by dismissing her action against a newspaper, which had disclosed her residential address in an article concerning a burglary at her home, relying on the fact that the applicant was a public figure and subject of public interest.
The violation stemmed from the domestic courts' erroneous assessment of conflicting interests and of the notion of "public-interest". Following the judgment, the Court of Cassation changed its case-law accordingly. The judgment was published and disseminated and used in training activities for national judges.

TUR / Alkaya (42811/06)

Judgment final on 09/01/2013

Final Resolution CM/ResDH(2016)209

The case concerned the disclosure of the applicant's name and photograph in newspaper articles, presenting her as a suicide bomber despite discontinued investigations and the authorities' subsequent failure to protect her reputation and dismissal of her claims for damages against the editor-in-chief and journalists. As the violation was due to the domestic courts' erroneous practice, the European Court's judgment resulted in a change of case-law, in particular of the Court of Cassation and the Constitutional Court.

TUR / Tarman (63903/10)

Judgment final on 21/02/2018

Final Resolution CM/ResDH(2019)215

The case concerned the disproportionate interference with the applicant's private life due to the obligation to disclose one's religious affiliation on one's identity card.
To prevent similar violations, a reformed legal framework governing identity cards was introduced in 2016. The new identity cards contain an electronic chip, which may contain information on one's religious affiliation only if the person expressly consents to it in the application form. Information stored on the electronic chips is classified and the right of authorities to access must be granted by law only as far as strictly necessary for the exercise of their duties. As regards civil registers, all citizens have the right to request, in writing, to register, change or leave blank their religious affiliation. Such information shall only be transferred to the electronic chips if the person applying for a new identity card provides explicit consent.

TUR / Sinan Isik (21924/05)

Judgment final on 02/05/2010

Final Resolution CM/ResDH(2018)221

The case concerns the retention of a lifelong peace activist's personal data (*inter alia* name, address, date of birth and presence at demonstrations organised by a violent protest group) in a police database, despite the fact that the applicant had never been convicted of any offence and his risk of violent criminality was remote. The European Court found that the continued retention of that data was disproportionate on account of the inadequate safeguards to enable review and deletion.
All references and entries concerning the applicant were erased by 2019. Following the judgment, the National Common Intelligence Application (NCIA) database has been created to replace police forces' individual counter-terrorism databases, to ensure a consistent approach to the review, retention and disposal of this information. A team of assessors determines whether a record is relevant and necessary and whether it is proportionate for the record to be added to the database. The NCIA database schedules a review of all records after 6, 7 or 10 years depending on the category of the data.
A Records Management Working Group is reviewing and updating the guidance concerning management of information by the police. Following a public consultation, a new Code of Practice for Police Information and Records Management and the associated Authorised Professional Practice have been produced. The Code sets out procedures to be applied in respect of the collection and retention of information which the police must follow when obtaining, managing and using information to carry out their duties. Subject to their ratification by police governance bodies, it is anticipated that these documents will be submitted to the Home Secretary for final approval in 2022. A National Retention Schedule, providing a definitive list of the retention periods for all police information has also been released.

UK. / Catt (43514/15)

Judgment final on 24/10/2019

Action Plan DH-DD(2019)1248

Rule 8.2a Communication from the authorities (20/12/2021)

The case concerned the indefinite retention of the applicant's personal data (DNA profile, fingerprints and photograph) taken in connection with a spent conviction in Northern Ireland for an offence of driving under the excessive influence of alcohol. The European Court found that the indiscriminate nature of the powers of retention, coupled with the absence of sufficient safeguards, exceeded the State's acceptable margin of appreciation in this regard.
In 2018, the Data Protection Act (DPA) introduced periodic reviews of the retention of personal data, including biometrics, for law enforcement purposes. It also provides for oversight by the Information Commissioner. The DPA applies to all parts of the United Kingdom. The specialised legislation in the devolved jurisdictions remains the same as it was at the time when the European Court examined the applicant's complaint, with the exception of Scotland where the Biometrics Commissioner Act 2020 enables the Commissioner to set out retention periods in their Code of Practice.

UK. / Gaughran (45245/15)

Judgment final on 13/06/2020

Action Plan DH-DD(2021)202

The case concerned the unlawful interference with the applicant's private life due to the indefinite retention and disclosure of data regarding a police caution for child abduction received by the applicant following a family dispute. Furthermore, the European Court found insufficient

UK. / M.M. (24029/07)

safeguards in the system to ensure that such private data not be disclosed, in particular, to potential employers.
In Northern Ireland, England and Wales, statutory amendments have been introduced to implement the judgment. Details relating to the applicant were removed from the Northern Ireland Criminal History database. In England and Wales, statutory amendments of 2013 introduced a filtering mechanism so that old and minor cautions and convictions are no longer automatically disclosed on a criminal record certificate. Disclosure is only made after taking into account the seriousness and age of the offence, the age of the offender and the number of offences committed. Further statutory amendments came into force allowing individuals to apply to an independent monitoring body.

Similar statutory amendments came into effect in Northern Ireland in April 2014. The Justice Act (Northern Ireland) 2015 amended the Police and Criminal Evidence (Northern Ireland) Order 1989 to create a statutory power for the recording of cautions and other diversionary disposals on the Northern Ireland criminal history database.
The regime in Scotland does not allow for the automatic disclosure of "alternatives to prosecution" (equivalent to cautions in England and Wales), which are removed from the system after a period of either two or three years. For certain serious sexual and violent offences, information can be retained for up to an additional two years after an application to a court by the chief police officer.

Judgment final on 29/04/2013

Final Resolution CM/ResDH(2015)221

The case concerned the disclosure in the media by a local council of an individual's photographs taken by a CCTV camera installed in a public street, without consent or sufficient safeguards and lack of an effective remedy in this respect. To prevent similar violations, specific provisions are contained in the Data Protection Act 1998 (DPA) and the Information Commissioner's CCTV Code of Practice 2008. The DPA provides the statutory basis for systemic legal control of CCTV surveillance over public areas, setting legally enforceable standards for the collection and processing of images relating to individuals. The Information Commissioner has the power to enforce compliance with the DPA, including imposing monetary penalties for serious breaches. The 2008 CCTV Code of Practice was revised to take into account changes in law, technology, use of CCTV and the shortcomings identified by the European Court, requiring the systematic justification for the use of CCTV, improved quality of images and imposing restrictions on the monitoring and recording of conversations in public spaces.

UK. / Peck (44647/98)

Judgment final on 28/04/2003

Final Resolution CM/ResDH(2011)177

The case concerned the unjustified interference with the minor applicants' right to respect for their private life due to the indefinite retention of blood samples, fingerprints and DNA profiles taken in connection with their arrest for offences for which they were ultimately not convicted.
Following the judgment, the applicants' fingerprints, DNA samples and profiles were destroyed.
In 2012, the Protection of Freedoms Act created a new regime for the retention of biometric samples (DNA and fingerprint) and data. In particular, it introduced a time limit of three years for the retention of fingerprints and DNA profiles for individuals arrested but not convicted of a serious offence, with a possible, single extension of two years upon application by the police to the national courts. In addition, a Biometrics Commissioner has been appointed, whose role is, *inter alia*, to keep the retention and use of biometric material under review.
The 2013 Criminal Justice (Northern Ireland) Act contained provisions similar to those in the Protection of Freedoms Act. As a result of an initial drafting error, an amendment was made by the Northern Ireland Assembly to the Justice (Northern Ireland) Act 2015. However, the new regime for the retention of biometric (DNA and fingerprint) samples and data in Northern Ireland has still not commenced, because of concerns that future investigations into deaths related to the troubles in Northern Ireland could be undermined, should biometric material related to these cases be destroyed. In March 2020, the Police Service of Northern Ireland decided to suspend deletion of biometric data on a non-statutory basis and to await the full commencement of this law.

UK. / S. and Marper (30562/04)

Judgment final on 04/12/2008

Action Report DH-DD(2015)836

Rule 8.2a Communication from the authorities (09/04/2021)

1.2. Search and seizure of personal data including correspondence

The case concerned an inspection on the applicant company's premises in the context of administrative proceedings without prior authorisation by a judge and without effective *ex post facto* review of the decision. The applicant company was subsequently fined for refusing to allow an in-depth examination of its data despite granting access to certain letters from the company's representatives.
To prevent similar violations, the Code of Administrative Justice was amended in 2012 to introduce the possibility of an action before administrative courts against already terminated interferences. In addition, in February 2016, the Supreme Administrative Court modified its case-law explicitly confirming that such actions may also be used to challenge on-site inspections. Finally, the 2001 Act on Protection of Competition was also amended in 2016 and brought in line with that position.

CZE / Delta Pekárny a.s. (97/11)

Judgment final on 02/01/2015

Final Resolution CM/ResDH(2017)299

The case concerned the seizure by the police and the latter's access to the applicant's computer on the grounds that it contained child pornography material, bypassing the normal requirement of prior judicial authorisation, when in fact the computer in question was already in the hands of the police and prior authorisation could have been obtained rapidly without impeding the police inquiries. In 2008, the applicant was sentenced to four years' imprisonment for possession and circulation of pornographic images of minors 2015, the Criminal Procedure Act was amended to strengthen procedural guarantees, introducing the appeal for review of final criminal judgements, which had been impugned in ECHR judgments. The judgment was disseminated to the authorities concerned.

ESP / Trabajo Rueda (32600/12)

Judgment final on 30/08/2017

Final Resolution CM/ResDH(2019)50

The case concerned the applicants' inability to challenge the lawfulness of house searches and seizures undertaken in the framework of fiscal proceedings under the Code of Tax Procedure. In the end, none of the applicants were prosecuted by the tax administration following the proceedings at issue. In 2008, the Code of Tax Procedure was amended, opening the possibility to appeal against a search order before the court of appeal's first president, competent to examine the facts and the law. The amendment also provides for the latter's competence to examine appeals lodged in respect of the conduct of the search and seizure operations.

FRA / Ravon and Others (18497/03)

Judgment final on 21/05/2008

Final Resolution CM/ResDH(2012)28

The case concerned the search of residential and business premises and the seizure of documents in connection with a traffic contravention committed by a third party without an adequately reasoned warrant. In a 1997 landmark judgment, the Federal Constitutional Court acknowledged the applicant's right to have the lawfulness of the search and seizure order examined retrospectively.
The Court's judgment was disseminated to all courts and judicial authorities concerned.

GER / Buck (41604/98)

Judgment final on 28/07/2005

Final Resolution CM/ResDH(2007)80

The case concerned the seizure of the applicant's two computers and hundreds of documents in his absence, on the basis of a warrant worded in too general terms due to the erroneous interpretation of the law on search and seizure operations, in the framework of preliminary criminal investigations. The EU-Directive 2016/680 on personal data processing for the purposes of prevention, investigation, detection or prosecution of criminal offences (transposed into Greek law) seeks to ensure a high level of protection, while ensuring that investigation and prosecution

GRC / Modestou group (51693/13)

Judgment final on 18/09/2017

Action Report DH-DD(2019)1096

of crime be not inhibited. The Directive applies to both cross-border and domestic processing of personal data. It also establishes a supervisory authority to which all individuals who consider their personal data to have been violated can address their complaints.

The case concerned the unlawful search of a lawyer's office by the police in her absence and the indiscriminate seizure of all documents found concerning one of her clients suspected of involvement in illegal financial activities. Following the Court's judgment, the documents related to the criminal proceedings were excluded from evidence by the domestic court and the seized documents were returned to the applicant. As the violation had resulted from the erroneous application of existing law, the judgment was disseminated to the domestic authorities concerned.

HUN / Turan (33068/05)

Judgment finial on 06/10/2010

Final Resolution CM/ResDH(2018)381

The case concerned the lack of adequate and effective safeguards in the supervision of legality and scope of the search of the applicant's apartment and the seizure of his personal belongings, including a computer and hard drive, in an undercover police investigation into the allegation of the unlicensed sale of medicine for treating HIV, hepatitis and cancer via the Internet. Subsequently, the Prosecutor's Office and the administrative courts failed to conduct an adequate and effective *ex post* review of the impugned actions.
To improve the prosecutorial supervision of searches and seizures, the Prosecutor General issued a decree in 2010 with a view to intensifying prosecutorial supervision in proceedings concerning alleged offences by State officials which are now examined as a priority. As from 2012, the quality of prosecutorial supervision has been under continuous assessment. Examples of administrative courts' case-law with regard to actions of State police officials were submitted, in which the courts acknowledged human rights violations by the police and awarded monetary compensation.

LVA / Boze (40927/05)

Judgment final on 13/11/2017

Final Resolution CM/ResDH(2019)299

The case concerned a search conducted by the police at the applicant's home in the framework of contravention proceedings against a third person, without a judicial warrant or permission, contrary to domestic law. To prevent similar violations, the 2009 Code of Minor Offences provided additional guarantees for conducting searches in minor offence cases, requiring a State agent's reasoned statement on the minor offence and a court's prior authorisation. In case of a flagrant minor offence, a search may exceptionally be conducted without a court's prior authorisation, under specific conditions. The Code of Criminal Procedure provides that, in criminal proceedings, on-site investigations of a domicile shall be carried out only with the prior permission of the owner, titleholder or an adult family member.

MDA / Bostan (52507/09)

Judgment final on 08/03/2021

Final Resolution CM/ResDH(2021)291

The case concerned an unlawful interference due to the use of an urgent procedure for confiscating the applicant's postal correspondence in the context of criminal proceedings without judicial authorisation.
The impugned procedure was modified in the 2014 Code of Criminal Procedure. Seizures and searches of postal deliveries now require judicial authorisation.

ROM / Dragos Ioan Rusu (22767/08)

Judgment final on 31/01/2018

Final Resolution CM/ResDH(2019)225

The case concerned a police search of the applicant's flat and the taking of a DNA sample during a murder investigation. The Court found that the taking of the DNA saliva sample had not been "in accordance with the law" within the meaning of Article 8. In particular, the order authorising the police to take a sample of the applicant's saliva did not refer to any specific legal provisions, as the Code of Criminal Procedure did not contain any reference to the taking of DNA samples. Moreover, the authorities had failed to prepare an official record of the procedure.

SER / Dragan Petrovic (75229/10)

Judgment final on 14/08/2020

Action Plan DH-DD(2021)328

The Code of Criminal Procedure was revised in 2011, containing additional safeguards related to DNA mouth swabs and the requirement that only an expert may carry out the procedure.

The case concerned irregularities in the conduct of search and seizure in the applicant's home and notary office and the disclosure of confidential psychiatric information in defamation proceedings due to the misapplication of relevant legal provisions by domestic courts. Hence, training activities and seminars on ECHR requirements when conducting inspections, searches or covert investigations were organised for law enforcement authorities and for the regional prosecutor's offices. As concerns the possibility to challenge the lawfulness of a search order, under the 2012 Code of Criminal Procedure, evidence obtained as a result of an unlawful search becomes inadmissible. Moreover, by a decision of 2019, the Supreme Court introduced the possibility to challenge the lawfulness of a search/investigative operation before administrative jurisdictions.

UKR / Panteleyenko (11901/02)

Judgment final on 12/02/2007

Final Resolution CM/ResDH(2021)137

These cases concerned various irregularities related to the interception of correspondence and to searches in lawyers' premises. In response, the authorities introduced extended judicial control mechanisms and time-limits for the interception of correspondence/communications were introduced. The 2012 Criminal Procedure Code provided safeguards with regard to the searches of premises and seizure of documents and other property, ranging from an extended definition of home (covering also non-residential premises) to the requirement of prior judicial authorisations for searches as well as the obligation to reject ill-founded requests of prosecutors or investigators. Searches without prior judicial authorisation are only allowed in cases of emergency and/or pursuit of a fleeing criminal. A breach of these rules leads to the inadmissibility of the evidence collected. Additional safeguards, introduced in 2017, include audio and video recording of searches, as well as the presence of lawyers and lay witnesses. Searches on lawyers' premises require prior notification of the Regional Bar Council and the presence of its representative. Criminal responsibility is set forth for unlawful entries and searches. The decision of an investigative judge ordering seizure of property is subject to appeal. Furthermore, a request seeking to quash the seizure may be lodged with an investigative judge or a court.

UKR / Voskoboynikov (33015/06)

Judgement final on 05/10/2017

UKR / Golovan (41716/06)

Judgment final on 05/10/2012

UKR / Volokhy (23543/02)

Judgment final on 02/02/2007

UKR / Cases of Koval and Others group (22429/05)

Final Resolution CM/ResDH(2021)48

1.3. Monitoring of correspondence in prison

The case concerned the unjustified supervision by the prison authorities of the applicant's application form sent to the European Commission on Human Rights. In 1998, the Law on the execution of punishments provided that correspondence addressed to institutions of human rights of the UN and the Council of Europe are not subject to control by the administration.

BGR / Mironov (30381/96)

Judgment final on 12/04/1999

Final Resolution CM/ResDH(2004)15

The violation found in this case concerned the unjustified routine monitoring of correspondence in prison, including correspondence with lawyers. In 2009, the Execution of Punishments and Pre-Trial Detention Act entered into force, regulating the right to correspondence and telephone use of prisoners. The control of prisoners' correspondence concerns only the material content and not the written content of the letter. In a judgment of 2013, the Supreme Court of Cassation held

BGR / Petrov group (15197/02)

Judgment final on 22/08/2008

that claims for compensation brought by prisoners alleging a breach of their right to correspondence should be examined by the administrative courts under the 1988 State and Municipalities Liability for Damage Act.	**Final Resolution CM/ResDH(2014)258**
The case concerned the unlawful interference with a prisoner's private life due to the monitoring of his correspondence addressed to the Ombudsman and to the Attorney General as well as to the Court, during his solitary confinement. In July 2018, Parliament amended the Prison Regulations with regard to the prisoners' correspondence and telephone communications as well solitary confinement as a disciplinary punishment or for purposes other than formal disciplinary punishment.	***CYP / Onoufriou (24407/04)*** ***Judgment final on 07/04/2010*** **Final Resolution CM/ResDH(2019)86**
The case concerned a disproportionate interference due to the opening of the applicant's correspondence by the prison authorities. In 2000, the Imprisonment Act established that a prison officer may open letters sent by or to a prisoner in the presence of the addressee, except letters addressed to his legal defence counsel, a prosecutor, or a court (including the European Court, the Legal Chancellor and the Ministry of Justice).	***EST / Slavgorodski (37043/97)*** ***Judgment final on 12/12/2000*** **Final Resolution CM/ResDH(2001)101**
The case concerned poor conditions of detention in Korydallos men's prison and interference with correspondence. In 2000, the Code of Criminal Procedure relating to the application of sentences was amended to remove the distinction between correspondence between the accused and lawyers who had assisted in the proceedings for which they had been detained, which was not subject to monitoring, and correspondence between the accused and lawyers who had not assisted them in the proceedings, which was subject to monitoring. Furthermore, a memorandum was sent to prison directors specifying that detainees' correspondence with the HR Commission or European Court should remain unopened.	***FRA / Slimane-Kaid (27019/95)*** ***Judgment final on 12/04/1999*** **Final Resolution CM/ResDH(2007)50**
The case concerned poor conditions of detention in Korydallos men's prison and interference with the prisoners' correspondence. The 1999 Penitentiary Code introduced sufficient safeguards for the protection of prisoners' correspondence, explicitly prohibiting any control of prisoners' correspondence and form of communication, unless required for national security reasons or related to particularly serious offences. When a restriction is imposed on correspondence or communications, the prisoner may appeal to the competent judge pursuant to the 1994 Act on freedom of correspondence and communication.	***GRC / Peers (28524/95)*** ***Judgment final on 19/04/2001*** **Final Resolution CM/ResDH(2009)127**
The cases concerned the lack of clarity of domestic law on monitoring of prisoners' correspondence allowing the authorities too much discretion, particularly in respect of the duration of the monitoring measures and the reasons justifying such measures, authorising the monitoring of correspondence with the organs of the European Convention on Human Rights and providing for no effective remedy against decisions ordering the monitoring of correspondence. To prevent arbitrary or unlawful interference in prisoners' correspondence based on the Administration of Prisons Law of 1975, a legislative reform of prison administration was adopted in 2004, defining clear grounds for restricting the prisoners' correspondence and criteria for the duration of the measure. Judicial review of the respective decision became available in principle. However, the effectiveness of this judicial review has been challenged, particularly as regards the length of such proceedings (see Interim Resolution (2005)56 in *Messina No.2* group). Prior to this reform, in 1999, circulars of the Ministry of Justice had banned the censorship of correspondence sent by prisoners to the Convention organs in practice.	***ITA / Calogero Diana (15211/89)*** ***Judgment final on 15/11/1996*** **Final Resolution CM/ResDH(2005)55** ***ITA / Labita (26772/95)*** ***Judgment final on 06/04/2000*** **Final Resolution CM/ResDH(2009)83**

The case concerned inhuman treatment with regard to a body search and the conditions of detention in Pravieniskes Prison, including overcrowding; unlawful interference due to the monitoring and censoring of the applicant's letters in prison, including letters addressed to the ECHR organs. According to the provision of the 2003 Code on the Execution of Criminal sentences, the monitoring and censoring of detainees' correspondence requires the authorisation of the prosecutor or the prison governor or a judicial decision. The Code also determines cases in which the control of detainees' correspondence cannot be authorized, which include correspondence with the bodies of the European Convention of Human Rights.	***LIT / Valasinas (44558/98)*** ***Judgment final on 24/10/2001*** **Final Resolution CM/ResDH(2004)41**
The case concerned the right to correspondence of prisoners on remand. According to the 2005 amendment of the Law on Criminal Procedure, their correspondence may be supervised only while investigating grave or extremely serious crimes and only for a maximum period of 30 days.	***LVA / Lavents (58442/00)*** ***Judgment final on 28/02/2003*** **Final Resolution CM/ResDH(2009)131**
The case concerned unjustified interference due to the control of a detainee's correspondence with the European Commission of Human Rights by prison authorities of the Netherlands Antilles and interference with his correspondence with his lawyer and a former inmate and lack of an effective remedy. To prevent unjustified interference with the prisoners' right to correspondence with the European Commission of Human Rights, the regulations governing the prison system of the Netherlands Antilles were changed and the general Prison Rules adopted in 1999 provided that correspondence with addressees entitled to hear prisoners' complaints or cases following a complaint shall not be monitored and not be opened without the inmate's written consent. The blanket provision banning all correspondence with former inmates was also lifted.	***NLD / A.B. (37328/97)*** ***Judgment final on 29/04/2002*** **Final Resolution CM/ResDH(2010)103**
These cases concerned the monitoring of correspondence in detention on remand and refusal of family visits and, in some cases, lack of procedural guarantees and excessive length in detention on remand. As concerns the monitoring and censoring of correspondence of detainees on remand, the 1998 Code of Execution of Criminal Sentences was amended in 2003 and 2012, providing that correspondence with the Ombudsman and international bodies of human rights protection must be sent directly to the recipients without censorship. This rule also applies to correspondence with investigating authorities, judicial authorities, other state organs and organs of municipalities. Correspondence between individuals detained on remand and their lawyers is, as a rule, not subject to censorship. Exceptionally, only during the investigation and for a period no longer than 14 days from the day of arrest, a prosecutor, in certain situations, may reserve the right to monitor the correspondence between the suspect and his lawyer. In addition, persons alleging infringement of their right to respect for their correspondence may claim compensation under the Civil Code.	***POL / Klamecki No.2 group (31583/96)*** ***Judgment final on 03/07/2003*** **Final Resolution CM/ResDH(2013)228**
The case concerned monitoring of both private and privileged correspondence, notably with the lawyer, by the prison authorities in 2008-2009. The authorities undertook legislative measures, in particular, in 2012, Article 91 § 3 of the Code on Execution of Sentences was amended, providing that the correspondence between a prisoner and his counsel may not be censored unless there is reliable information about planning or committing a crime. Article 15 § 4 further provides that correspondence with interstate bodes for the protection of human rights may not be censored.	***RUS / Boris Popov (23284/04)*** ***Judgment final on 28/01/2011*** **Action Report DH-DD(2017)924**

In 2011, the Federal Penitentiary Service introduced "Guidance to their staff", which contains a requirement that censorship be forbidden not only in respect of detainees' correspondence with their legal counsel, but also with their representative before the European Court, as well as other requirements.
The judgment has been translated and disseminated to the relevant authorities.

TUR / Tamer group (6289/02)

Judgment final on 05/03/2007

Action Report DH-DD(2021)940

This group of cases concerned unjustified interference by prison authorities with detainees' right to correspondence. The interception and censorship measures concerned were decided upon by the prison disciplinary commission and supervised by the public prosecutor, not by an independent court, on the basis of an unspecified regulatory framework.
The 2005 Law on the Execution of Sentences and Preventive Measures and the 2020 Directive on Management of the Prisons and Enforcement of Sentences and Preventive Measures set out to provide sufficient clarity on the right to monitor the detainees' correspondence. Correspondence between inmates and their lawyer and official authorities are not subject to inspection, except for inmates convicted of terrorism-related or organised crimes or in exceptional cases, if the authorities have reason to believe an abuse of privilege has occurred and that the content of the letter threatens the safety of the establishment or of others or is otherwise unlawful.
The remaining general correspondence is inspected by the reading commission of the prison administration and is referred to the disciplinary commission, which may decide to retain it, if it poses a threat to order and security in the prison, singles out serving officials as targets, allows communication with a terrorist or criminal organisations, contains false or misleading information likely to cause panic in individuals or institutions or contains threats or insults. The detainee may lodge an appeal against such decision to the enforcement court, which has to decide within seven days. A further appeal may be lodged with the Assize Court.

UK. / Szuluk (36936/05)

Judgment final on 02/09/2009

Final Resolution CM/ResDH(2013)88

The case concerned the unjustified monitoring by prison authorities of medical correspondence between a convicted prisoner detained in a high-security prison and his external medical specialist. The Prison Service Instruction on prisoner communications was amended in 2011 to provide that: "Correspondence between a prisoner and a registered medical practitioner must be handled in confidence but only to the extent that the registered medical practitioner is acting in a professional capacity and the correspondence directly relates to the treatment of the prisoner". In respect of England and Wales, a Statutory Instrument of 2010 amended relevant regulations to provide that a prisoner may correspond confidentially with a registered medical practitioner who has treated the prisoner for a life-threatening condition, and such correspondence may not be opened, read or stopped unless the Prison Governor has "reasonable cause" to believe that the contents do not relate to the treatment of that condition. The Scottish Prison Service made a similar provision in Rule 58 of the Prisons and Young Offenders Institutions (Scotland) Rules 2011, which is designed to be consistent with the decision in this case. The Northern Ireland Prison Service issued an Instruction to Governors in 2012, amending the Standing Orders of the Northern Ireland Prison Service. If a prisoner were to develop a life-threatening illness whilst in prison, he/she would have no need to correspond with a consultant as he/she would receive care on-site from the healthcare professionals. There would be a duty of care on behalf of the prison healthcare team to make contact with the prisoner's external healthcare provider and any such contacts would be covered by the medical in-confidence procedures already in place.

UKR / Mikhaylyuk and Petrov (11932/02)

Judgment final on 10/03/2010

The case concerned the unforeseeable interception and opening of correspondence of two residents of a prison colony (who worked there but did not serve sentences) by the respective prison administration. The violation stemmed from an administrative malpractice of the penitentiary institution concerned and the national courts' misinterpretation of the law in the specific circumstances of this case. The 2013 Ministry of Justice Instruction "On the organisation of correspondence of persons held in penitentiary institutions and in pre-trial detention centres"

was published and is hence accessible to the public. Training sessions for judges and candidates to judicial positions were held on the ECHR jurisprudence including the present judgment, which was translated, published and disseminated to all authorities concerned.

Final Resolution CM/ResDH(2018)40

1.4. Health-related personal data

The case concerned the disclosure of information about the applicant's health status in criminal proceedings against her husband, in particular, the disclosure of her identity and medical data in the Court of Appeal's judgment and the decisions to limit the confidentiality of the trial record to a period of ten years. Following the present judgment, the Chancellor of Justice requested the impugned decision's revision pursuant to the Code of Judicial Procedure in order to remedy the individual situation. In 1998, the Supreme Court found that the Court of Appeal - under the Act on the Publicity of the Court Proceedings - had misapplied the law and extended the period during which the trial records are to be kept confidential from ten to forty years.

FIN / Z. (22009/93)

Judgment final on 25/02/1997

Final Resolution CM/ResDH(99)24

The case concerned the unjustified interference with private life due to the collection of personal medical data by a State agency (MAKKEDI) in the process of an administrative inquiry concerning the applicant's health care on the basis of legal provisions lacking sufficient precision and adequate legal protection against arbitrariness.
In 2007, the MADEKKI was integrated into the Health Inspectorate. Concerning the protection of patient data, the 2009 Law on the Rights of Patients provides that such data may be used only with the written consent of the patient or in cases provided by this law. The law lists public healthcare institutions, including the Health Inspectorate, that may receive, collect and use patient data. The Health Inspectorate is authorised to collect patient data for ensuring the supervision of the healthcare sector. The range of supervisory functions is defined in its Statute, approved by the Cabinet of Ministers in 2008. The procedure for the collection of patient data is established in the Health Inspectorate Internal Rules of 2013. These rules require that, in case an investigation is initiated by the Health Inspectorate, an expert should evaluate the scope of information necessary and determine the time-period of the data to be processed.

LVA / L.H. (52019/07)

Judgment final on 29/07/2014

Final Resolution CM/ResDH(2017)64

The case concerned the disclosure of the applicant's HIV positive status in a certificate exempting him from military service issued in 2011. To prevent similar violations, in 2012, upon request of the Ombudsman, the Constitutional Court declared unconstitutional the 2005 Government decision requiring the specific illness reference code of the Medical Standards to be indicated in the exemption certificate. In 2013, the Government replaced its decision accordingly. During the period 2016-2019, more than 240 judges and prosecutors attended training activities of the National Institute of Justice on Article 8 issues, including on data protection.

MDA / P.T. (1122/12)

Judgment final on 26/08/2020

Final Resolution CM/ResDH(2021)120

The case concerned the disclosure of information of a medical nature by a medical institution to a person's employer, including sensitive details about her pregnancy, her state of health and treatment received despite an explicit prohibition in domestic legislation to disclose such information.
In 2012, the Law on the protection of personal data set up rules and proceedings for protection and management of personal data under the supervision of the Centre for the Protection of Personal Data. This law was adopted in the context of the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 and its Additional protocol of 2001, as well as Directive 95/46/EC of the European Parliament and of the Council on

MDA / Radu (50073/07)

Judgment final on 15/07/2014

Final Resolution CM/ResDH(2017)347

the protection of individuals with regard to the processing of personal data and on the free movement of such data. Relevant instructions were issued by the Ministry of Health to all medical institutions.
The medical documents at issue were destroyed by the employer.

The case concerned the disclosure, by a public hospital to the police, of the applicants' medical data relating to their treatment for drug addiction. In 2013, a new Code of Criminal Procedure entered into force providing for the public prosecutors' supervision of police access to personal data. In 2019, the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.223) was signed. In 2020, a Personal Data Protection Act was adopted implementing the relevant EU regulations in the field of personal data protection. The Personal Data Protection Agency adopted Rules on the processing of data and on data protection impact assessments. In 2021, a Law on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties was under preparation.

MKD / J.M. and A.T. (79783/13)

Judgment final on 22/10/2020

Final Resolution CM/ResDH(2021)123

The case concerned violation of the right to private life of the applicants, neither suspect nor accused in any investigation, on account of the disclosure of their medical record to prosecutors. The Court concluded that the collection by the prosecutor's office of confidential medical information concerning these applicants was not accompanied by sufficient safeguards to prevent disclosure inconsistent with the respect for their private life.
The authorities referred to a number of legislative and regulatory acts concerning healthcare and protection of personal data which were adopted or amended following the Court's judgment. In particular, they referred to a special instruction from 2013 addressed by the Prosecutor General to the prosecutors on the collection and processing of personal medical data. They also cited domestic courts' case-law which is aligned with the European Court's case-law. The judgment has been published and disseminated.

RUS / Avilkina and Others (1585/09)

Judgment final on 07/10/2013

Action report DH-DD(2014)1329

The case concerned the authorities' denial of the applicant's access to her medical report after examination in prison on grounds of security and public order on the basis of a circular of the General Directorate of Prisons and Detention Places of 1990. As from 2005, the Code on the Execution of Sentences and Security Measures as well as the Regulation on the Administration of the Facilities and Executions of Sentences and Security Measures and the 2007 Circular of Ministry of Justice grant detainees the right to obtain access to their medical files and to take copies of the enclosed documents.

TUR / Usla No. 2 (23815/04)

Judgment final on 20/04/2009

Final Resolution CM/ResDH(2014)129

The case concerned the unlawful collection, retention and use of sensitive, obsolete and irrelevant data concerning the applicant's mental health (in particular the military enlistment office's certificate confirming the applicant being unfit for military service), in considering his application for promotion in a State-owned company as well as the domestic courts' failure to respond to the applicant's principal arguments adduced in the civil data protection proceedings against his employer.
The Constitution of 1996, as amended in 2004 and 2014, provides that collection, retention, use, and dissemination of confidential information about a person without his/her consent is not permitted, unless provided for by law in the interests of the national security, economic welfare and human rights. The 2010 Law on Personal Data Protection provided that personal information shall be processed only for specific and legitimate purposes with the consent of the person and that processing of personal information, particularly information on the state of health, shall be prohibited.

UKR / Surikov (42788/06)

Judgment final on 26/04/2017

Action Report DH-DD(2021)1012

In 2017, the Unified State Register of Recruits, Conscripts and Reservists was set up as an automated IT system to collect, store, process and use data on military personnel. The unlawful disclosure of personal data entails administrative and civil responsibility. The Parliament Commissioner for Human Rights also monitors compliance with the data protection legislation.

1.5. Access to and erasure or destruction of personal data

BGR / Dimitrov-Kazakov (11379/03)

Judgment final on 10/05/2011

Final Resolution CM/ResDH(2013)119

The case concerned the registration of the applicant's name in a police record of "offenders" after his questioning by the police without any official indictment and the lack of an effective remedy in this respect.
Finally, the applicant's name was struck off the police records in 2002. The impugned confidential instruction of the Minister of Internal Affairs of 1993 as the legal basis for the registration was revoked in 2002. The Ministry of the Interior Act as the new legal framework was adopted in 2006. Under a decree for police registration of 2011, personal data may only be registered when charges are brought in relation to a serious intentional crime. Police authorities *ex officio* or upon request from the person concerned are obliged to end police registration when criminal proceedings at stake are discontinued or the person is acquitted. Refusals can be appealed against before the administrative courts. The Commission for Personal Data Protection, established under the 2006 Protection of Personal Data Act prohibiting the processing of data for purposes other than those for which the information was originally collected, monitors police registration decisions made by the Ministry of the Interior.

FRA / Brunet (21010/10)

Judgment final on 18/12/2014

Final Resolution CM/ResDH(2018)156

The case concerned the inability to seek deletion of information recorded in the police database STIC (system for processing recorded offences) despite the discontinuation of criminal proceedings against the applicant, for 20 years. To execute the European Court's judgment, the retention period of recorded data has not been legally modified, however, decisions of discontinuation have been systematically mentioned in the record since 2011. Moreover, the law of 2016 on the fight against organised crime, terrorism and their financing, allows the prosecutor to grant an application for early deletion if the case concerned was dismissed for a reason other than insufficiency of charges. The public prosecutor's decision on the erasure or rectification of personal data may be appealed before the courts.

ITA / Godelli (33783/09)

Judgment final on 18/03/2013

Final Resolution CM/ResDH(2015)176

The case concerned the legal inability of a child abandoned at birth to gain access to information on his/her origins or to make a request for her biological mother to waive the confidentiality of information. The Court criticised a lack of proportionality between the child's interests and those of the biological mother, who wished that her identity remains confidential and that the child not have access to her will.
In 2015, following the Court's judgment, the Trieste juvenile court communicated to the applicant her mother's identity. In 2013, the Constitutional Court declared unconstitutional the legal provision, introduced in 2003, that prevented a child abandoned at birth from gaining access to information on his/her birth mother without granting the judge the possibility to verify the birth mother's will. In 2015, a draft law on the procedure for requesting information concerning one's origins was approved by the Chamber of Deputies.

POL / Joanna Szulc (43932/08)

The case concerned the authorities' refusal, for over ten years, to grant the applicant – who denied any collaboration with the security services during the communist era – access to all

documents about her, collected by those services. The Court noted, in particular, the failure to put in place an effective procedure whereby interested parties could obtain access to security service documents concerning themselves and confirmed the approach taken in previous cases concerning applicants seeking access to their files created by the secret services under a totalitarian regime.
Following the Court's judgment, the applicant was granted access to copies of all documents concerning her which had been created by the communist security services.
In 2010, the Law on the Institute of National Remembrance of 1998 was amended to provide for a right of access to documents deposited with the Institute. Hence, everyone has the right to apply for access to documents that have been deposited with the Institute that concern them. Those documents are made available by administrative decision with a right to appeal to the President of the Institute of National Remembrance. The decision of the President of the Institute of National Remembrance may be appealed against before administrative courts.

Judgment final on 13/02/2013
Final Resolution CM/ResDH(2014)60

The case concerned excessively lengthy administrative proceedings to deal with an access request to personal information collected by the communist secret services. In order to allow effective access to records, the National Council for the Study of the Securitate Archives continued the inventory process of documents transferred from the Securitate archives. An inventory of cases pertaining to criminal issues was published on its website. A new technical system was set up for document management and digitalisation. Average length of access proceedings was reduced to between two and six months. All Securitate files were transferred to the National Council except those containing classified information with regard to national security. Information requests of interested parties must be treated within 30 days.

ROM / Haralambie (21737/03)
Judgment final on 27/01/2010
Final Resolution CM/ResDH(2017)237

The case concerned the insufficient safeguards against arbitrary interference with the applicant's right to private life owing to the storage and public disclosure of private information by the Romanian Intelligence Service, in its capacity as custodian of the archives of the former communist secret service (the *Securitate*).Following the judgment, the entries in the registers resulting in the misleading designation of the applicant as a member of an extreme-right pre-war organisation were modified so as to avoid further confusion on account of name similarities. In 2008, Parliament reformed the legal framework for the processing of information contained in the archives of the Securitate. Under the 2008 Regulation, the processing of such information was transferred to a civilian administrative body (the National Council for the Study of the Securitate Archives – "NCSAS"), responsible for enabling and regulating the access to surveillance files. Interested persons can file a written application for access or rectification of information with the NCSAS, which is bound to respond within 30 days and whose decisions are subject to judicial review.

ROM / Rotaru (28341/95)
Judgment final on 04/05/2000
Final Resolution CM/ResDH(2014)253

The case concerned the unjustified storage by the Security Service of information on the applicants' former political activities and the refusal to grant access to the full extent of personal information contained in such records as well as the lack of any effective remedy.
Following the Court's judgment, the information on the applicants was deleted from the records of the Security Service and is therefore neither searchable nor accessible to Security Service personnel. In January 2008, the newly created Commission on Security and Integrity Protection began its control function also aimed at improving individual access to domestic legal remedies. It supervises personal data processing by the Security Service and, after 2012, also by the Police. As from January 2007, an appeal to a general administrative court against a decision by the Security Service not to correct or delete personal data allegedly processed in contravention of legislation, became possible.
Finally, in 2012, the Police Data Act entered into force. Its general purpose is to protect privacy when personal data is processed in the context of law enforcement activities. Its substance

SWE / Segerstedt-Wiberg and Others (62332/00)
Judgment final on 06/09/2006
Final Resolution CM/ResDH(2012)222

largely coincides with previous legislation, but provides clearer and more detailed regulations in certain areas, including data deletion.

UK. / Roche (32555/96)

Judgment final on 19/10/2005

Final Resolution CM/ResDH(2009)20

The case concerned the failure to fulfil the positive obligation to provide an effective and accessible procedure enabling the applicant, a former Royal Engineer in the British Army, to have access to all relevant and appropriate information which would allow him to assess any risk to which he had been exposed during his participation in mustard and nerve gas tests at the Chemical and Biological Defence Establishment at Porton Down.

To prevent similar violations, the Data Protection Act 1998 (entry into force 2000) introduced a right to receive one's personal data held by a public authority. An appeal to the Information Commissioner, an independent supervisory authority reporting directly to Parliament, is possible. Decisions of the Information Commissioner may be appealed against before the Information Tribunal. A separate National Security Appeals Panel of the Tribunal may hear appeals against exemptions from disclosure for reasons of national security.

The Freedom of Information Act 2000 (entry into force 2005) created a general right of access to any information held by a public authority. The appeals procedure is similar to that under the DPA 1998. Under the Human Rights Act 1998 (entry into force 2000) judicial review of the authorities' actions can also be sought in the Administrative Court.

Furthermore, the Porton Down Volunteers' Helpline was set up in February 1998, with the objective of helping former volunteers or their representatives to gain easy access to information relating to their participation in tests at Porton Down. Finally, procedures regarding information requests about one's actual or possible exposure to hazard were simplified.

2. SECRET SURVEILLANCE

2.1. Interception of communications and personal data

The case concerned the applicant's complaint that the police had not had a valid court warrant to place her under secret surveillance during criminal investigations into allegations of bribery. The measures included the use of recording-equipment during a meeting with the applicant, the interception of telephone conversations and the videorecording of the handover of the bribe money, given in marked banknotes. The Court criticised, in particular, that the warrant was too vague, lacking details regarding the object of the surveillance measure, as well as the insufficient judicial supervision. To prevent similar violations, as from 2010, the practical conduct of operative and intelligence activities was improved with regard to the procedure, authorisation of operations, documentation of results as well as supervision by the General Department of the Criminal Police. In March 2020, the Board of the Prosecutor General's Office ensured prosecutorial oversight over the lawfulness of operative and intelligence activities. The Code of Criminal Procedure of 2021 comprises general regulations and detailed guarantees regarding operative and intelligence measures (undercover investigative actions) which, within the framework of criminal proceedings, can only be carried out on the instruction of the investigator and on the basis of a court decision.

ARM / Hambardzumyan (43478/11)

Judgment final on 05/03/2020

Final Resolution CM/ResDH(2021)302

The case concerned unlawful acts carried out by the authorities in the context of criminal investigations, *i.e.* the obtention and use of the applicant's telephone calling list and the recording of a conversation by means of a body-planted listening device, without a valid legal basis for either.
Under the 2002 Code of Criminal Procedure, a judge can grant access to telecommunications data by a reasoned written order. The conditions for the use of monitoring devices (called "operative investigative means") by the police in the course of proceedings concerning intentional criminal offences are also set out therein. Authorisation by a prosecutor is needed for audio and video surveillance of persons and objects; authorisation by a judge is needed for home or correspondence to be affected. The Supreme Prosecutor's Office published interpretation guidance in 2004. The judgment was translated, published and disseminated to all authorities concerned.

CZE / Heglas (5935/02)

Judgment final on 09/07/2007

Final Resolution CM/ResDH(2011)98

The case concerned the lack of sufficient reasoning in the preliminary investigation judges' and the prosecutors' authorisations of different secret surveillance measures in criminal proceedings. The European Court found an unlawful interference with the right to private life despite the acceptance – by domestic courts – of the retroactive justifications of these measures.
An amendment to the Code of Criminal Procedure of 2013 clearly foresees that the use of information obtained by surveillance activities as evidence requires prior authorisation. The Supreme Court changed its case-law in 2017, when it underlined that judicial *ex post* control cannot eliminate the inadmissibility of evidence obtained without prior, sufficiently reasoned authorisations. Moreover, under the terms of the 2015 Compensation of Damage Caused in Offence Proceedings Act, compensation may also be requested for damages caused by unlawful surveillance activities. Relevant training and awareness-raising activities were organised for judges, prosecutors and advocates.

EST / Libik and Others (173/15)

Judgment final on 07/10/2019

Final Resolution CM/ResDH(2021)58

The case concerned the real-time geolocation of the applicant's vehicle as a surveillance measure taken in the context of a criminal investigation into his involvement in international drug-trafficking offences on the basis of a law which, at the relevant time prior to 2014, did not indicate with sufficient clarity to what extent and how the authorities were entitled to use their discretionary power. The judgement was published and disseminated to all authorities concerned, including the Attorney General. In 2014, a law on geolocalisation entered into force which put such a measure, requiring a sufficiently reasoned authorisation by a magistrate, under judicial control.

FRA / Ben Faiza (31446/12)

Judgment final on 08/05/2018

Final Resolution CM/ResDH(2021)369

The case concerned the unlawful tapping and recording of the applicant's telephone conversation by the police during criminal proceedings instituted against him, as the domestic law did not indicate with reasonable clarity the scope and manner of exercise of the margin of discretion conferred on the public authorities.
To prevent similar violations, the 1991 Act concerning the secrecy of telecommunications amended the Code of Criminal Procedure relating to interceptions ordered by the judiciary. Hence, the investigating judge may, if the penalty concerned is equal or superior to two years imprisonment, order the interception, recording and transcription of telecommunications. The decision to intercept, which must be taken in writing, is not of a judicial nature and cannot be appealed. The decision must contain all elements permitting the identification of the telephone line to be intercepted and state the offence which justifies this measure. It must also specify its duration (a maximum period of four months, renewable once). Each of the interception and recording operations must be mentioned on a record which states the day and time when it began and when it finished. The recordings will be destroyed on the initiative of the prosecution after expiry of the time limit for bringing a prosecution. No telephone line to a lawyer's office or his home may be intercepted without the President of the Bar having been previously informed by the investigating judge.

FRA / Kruslin (11801/85)

Judgment final on 24/04/1990

Final Resolution CM/ResDH(92)41

The case concerned an unlawful use of listening devices in criminal proceedings, in the apartment of a third party regularly visited by a murder suspect, based on unclear regulations concerning the authorities' discretion concerning audio surveillance.
Measures relating to the use of listening devices in proceedings relating to organised crime were introduced in the Code of Criminal Procedure in 2004, specifying the categories of persons who might be subjected to such measures and the nature of the offences which might warrant them. This law also applies to visiting rooms in detention centres (public places). It provides a time frame for the operations and determines the conditions for erasure or destruction of the recordings. The Cassation Court and the Constitutional Council changed their respective case-law accordingly.

FRA / Vetter (59842/00)

Judgment final on 31/08/2005

Final Resolution CM/ResDH(2010)5

The case concerned the leak to the media of the applicant's (a politician and founding member of the Liberal Democrats political party) telephone conversations, which had been intercepted by the State Security Department and the lack of an effective remedy allowing for an examination of the legality of the surveillance measures. In 2013, the Law on Criminal Intelligence provided for effective domestic remedies, enabling judicial examination of the legality and the implementation of surveillance measures. In June 2015, the Supreme Court published on its website a survey of the domestic case-law with regard to the Code of Criminal Procedure and the Law on Criminal Intelligence as concerns the monitoring, recording and storage of information transmitted through the electronic communications networks, and provided information regarding the criteria required for the secret surveillance measures to comply with Article 8.

LIT / Draksas (36662/04)

Judgment final on 31/10/2012

Final Resolution CM/ResDH(2016)124

The case concerned an arbitrary interference, due the impossibility for the applicants to verify if covert interception of telephone conversations in the framework of the criminal proceedings had

LVA / Santare and Labaznikovs (34148/07)

Judgment final on 30/06/2016

Final Resolution CM/ResDH(2017)213

been carried out on the basis of a prior judicial authorisation and the failure of the domestic courts to effectively review the lawfulness of the contested measure contrary to existing legal provisions.
The Criminal Procedure Code of 2005 provided that, whenever information obtained through surveillance measures is used as evidence in the criminal proceedings, the case file should include a reference letter with the respective authorisation mentioning the authorising institution, and the date and period of time for which the measure had been authorised. Such reference letters, issued by the Supreme Court, allow the persons concerned to verify whether the evidence was obtained in compliance with the prescribed procedure. The 2014 amendments to the Criminal Procedure Code widened the judiciary's competence regarding the admissibility of evidence obtained as a result of special operative measures: upon an arguable claim by the prosecutor, victim, defendant or defence counsel, the trial court must consider material resulting from classified special investigation related to the pieces of evidence used in criminal proceedings.

LVA / Meimanis (70597/11)

Judgment finalon 21/10/2015

Final Resolution CM/ResDH(2017)211

The case concerned the unlawful interception of the applicant's cell telephone conversations without *ex post facto* judicial approval, in an operational investigation by the Bureau for the Prevention and Combating of Corruption for attempting to take a bribe. The violation had resulted from an inconsistency between the terms of the Law on Operational Activities in force at the material time and the practice of domestic law-enforcement authorities, according to which an *ex post facto* approval by the judicial authorities was not sought in all cases, especially when the operational activities were completed within 72 hours and no extension was necessary. In June 2011, the Constitutional Court ruled that *an ex post facto* judicial approval of the operational measures must always be obtained by the Supreme Court President (or a specially authorised judge) notwithstanding that the measure in question had been terminated in less than 72 hours. The domestic authorities are bound by this interpretation. The judgment was published and widely disseminated to all relevant courts and judicial authorities.

NLD / R.V. and Others (14084/88)

Decision final on 15/05/1992

Final Resolution CM/ResDH(2007)88

The violation found in this case related to the surveillance - under a 1972 Decree on intelligence and security services - of the applicants' activities by the intelligence and security services as well as the denial of access to the compilation and the retention of personal information concerning them.
The 1988 Intelligence and Security Services Act contained substantive modifications with regard to the conditions under which information procured may be registered and passed on to other bodies or persons. However, the Act did not introduce any change in regard of the circumstances in which covert modes of surveillance may be deployed.
In 2002, the Intelligence and Security Services Act defined the circumstances and conditions empowering authorities to carry out measures of secret surveillance and established the procedure concerning requests for access to security service files, including appeal. The Act also provided a definition of persons liable to be subject to measures of secret surveillance and a description of the means to be employed to that end. According to the Act, security services have to publish an annual report which is submitted to Parliament, in which areas of specific attention concerning the services for the past and coming year are outlined.

SUI / Vukota-Bojic (61838/10)

Judgment final on 18/01/2017

Final Resolution CM/ResDH(2019)233

The case concerned an arbitrary interference with the applicant's private life due to the secret surveillance of a social-insurance claimant by private investigators without sufficient legal clarity of the scope and manner of exercise of the discretion conferred on insurance companies acting as public authorities in insurance disputes.
In October 2016, the National Accident Insurance Fund announced it would cease to use private detectives in the fight against insurance fraud. In 2017, the Federal Court delivered two leading judgments according to which the relevance of the present judgment applies to all areas of law. In September 2019 an amendment to the Federal Law on Social Insurance entered into force establishing the legal basis for the surveillance of insured persons. In particular, it allows the recording of images and videos for investigative purposes. It also contains a list of possible

measures subject to judicial authorisation or requiring only an insurance manager's decision. Furthermore, the amendment lists the circumstances which justify the surveillance, providing for the obligation to inform the person concerned and establishing general rules for the storage/destruction of the data collected.

SUI / Kopp (23224/94)

Judgment final on 25/03/1998

Final Resolution CM/ResDH(2005)96

The case concerned the lack of predictability of the domestic legislation regarding the surveillance of a lawyer's telephone lines, in the context of criminal proceedings to which he was a "third party", not a suspect, on orders of the Federal Public Prosecutor.
The Court found that the violation was due to a discrepancy between the clear text of the legislation protecting legal professional privilege and the practice followed, as the law did not state clearly under what conditions and by whom the distinction between matters connected with a lawyer's work and those relating to his other activities is to be drawn. In 2002, the Federal Law on the monitoring of postal correspondence and telecommunications set out in detail the conditions under which telephone calls may be intercepted. It includes exceptions for which authorisation may be given to monitor persons bound by professional confidentiality, when they are not themselves suspects or charged. If the monitoring of a lawyer reveals information falling under the professional privilege, the relevant documents must be removed from the file and cannot be used in criminal proceedings.

SVN / Benedik (62357/14)

Judgment final on 24/07/2018

Final Resolution CM/ResDH(2021)294

The case concerned the police's failure to obtain a court order to access subscriber information associated with a dynamic IP address, recorded by the Swiss law-enforcement authorities during their monitoring of users of a certain file-sharing network. This led to the identification of the applicant after he had shared files over the network, including child pornography. The Court found in particular that the legal provision used by the police to obtain the subscriber information had lacked clarity, offered virtually no protection from arbitrary interference, had no safeguards against abuse and no independent supervision of the police powers involved.
The violation at hand resulted partly from the deficient legislative provisions and partly from inadequate case-law of domestic courts. Pursuant to the 2019 amendments of the Code of Criminal Procedure, access to and transfer of communication traffic data require a court order and are supervised by courts. All data gathered by the police is to be submitted to the state prosecutor. Internal supervision within the police and administrative supervision by the Ministry of Internal affairs is also to be regulated. Moreover, a circular letter by the State Prosecutor's Office was addressed to the prosecutors and the police on the Court's findings. In July 2018, a binding instruction was issued to the police to obtain a prior court order when requesting subscriber data related to a specific IP address. In October 2018, domestic case-law changed, highlighting that a court order was necessary for obtaining subscriber information associated with the dynamic IP address referring to the Court's judgment.

UK. / Malone (8691/79)

Judgment final on 26/04/1985

Final Resolution CM/ResDH(86)1

The case concerned the admitted existence in England and Wales of laws and practices permitting the interception of postal and telephone communications and the "metering" of telephones by or on behalf of the police within the context of criminal investigations.
The 1985 Interception of Communications Act brought domestic law in compliance with the ECHR. It did so by establishing a comprehensive statutory framework governing the interception of communications on the public postal and telecommunications systems, in which the grounds for authorised interception are expressly set out, and in which any interception carried out other than in accordance with the Act's provisions is made a criminal offence.

UK. / Liberty and Others (58243/00)

Judgment final on 01/10/2008

The case concerned the unlawful interference with the applicants, two non-governmental organisations working in the field of human rights and established in Ireland and the United Kingdom, right to private life due to the insufficient clarity of the Interception of Communications Act 1985 which conferred on the authorities very wide discretion to monitor certain forms of their electronic communications.

The Interception of Communications Act 1985 was replaced by the Regulation of Investigatory Powers Act 2000 which provided clear procedures for the authorisation and processing of interception warrants as well as the processing, communication and destruction of intercepted material.	**Final Resolution CM/ResDH(2011)83**
The case concerned the covert surveillance of a detainee's consultations with his lawyer and the person appointed to assist him, as a vulnerable person, following his arrest. The legal regime failed to provide sufficient safeguards for the protection of material obtained by covert surveillance of lawyer-client consultations. In 2010, the Implementing Code for the secure handling, storage and destruction of material obtained through covert surveillance was brought into operation to rectify the legal lacuna. The judgment was published and disseminated to all authorities concerned.	***UK. / R.E. (62498/11)*** ***Judgment final on 27/01/2016*** **Final Resolution CM/ResDH(2016)143**

2.2. Surveillance in the workplace

The case concerned the decision of a private company to dismiss an employee after monitoring his electronic communications and accessing their contents, and the domestic courts' failure to protect his right to respect for his private life and correspondence. In particular, the national courts had failed to determine whether the applicant had received prior notice from his employer of the fact of the monitoring or had been informed of the nature or extent of the monitoring and the degree of intrusion. The violation was due to an erroneous application of domestic law in the specific case. The judgment was published, translated and disseminated to all domestic courts. It is used in training activities of the National Institute for Judges and Magistrates.	***ROM / Barbulescu (61496/08)*** ***Judgment final on 05/09/2017*** **Final Resolution CM/ResDH(2019)124**
The case concerned the arbitrary interference with the applicant's right to private life and correspondence due to the monitoring of her telephone, e-mail and internet usage during the course of her employment by a public body without her knowledge and with no domestic law in place to regulate such monitoring. The Regulation of Investigatory Powers Act 2000 provides for the regulation of the interception of communications. The Telecommunications Regulations 2000 sets out the circumstances in which employers may record or monitor employee's communications (such as e-mail or telephone) without the consent of the employee or the other party to the communication. Guidance on monitoring staff usage of technology was put in place and included the requirement to inform staff of interceptions made under the Regulations without consent. For interceptions outside the scope of the Regulations, the consent of the sender and recipient is required and may be obtained by inserting a clause in staff contracts and by call operators stating that calls might be monitored or recorded unless third parties object.	***UK. / Copland (62617/00)*** ***Judgment final on 03/07/2007*** **Final Resolution CM/ResDH(2010)79**
The case concerned an unlawful interference with the applicants' right to private life due to the use of covert listening devices in their workplace or residence by the police, on the grounds that the legal basis was neither binding nor publicly accessible and that the applicants lacked an effective remedy since the complaint procedure did not protect against abuse of authority. To prevent similar violations, the relevant part of the Police Act was introduced in 1999 along with the Code of Practice on Intrusive Surveillance Work, both legally binding and accessible. Furthermore, the Regulation of Investigatory Powers Act 2000 provided independent oversight by a Chief Surveillance Commissioner and established an independent tribunal to consider complaints.	***UK. / Govell group (27237/95)*** ***Judgment final on 18/05/1998*** **Final Resolution CM/ResDH(2005)68**

UK. / Halford (20605/92)

Judgment final on 25/06/1997

Final Resolution CM/ResDH(2007)15

The case concerned a violation of the applicant's right to respect for her privacy on account of the interception, between 1990 and 1992, of telephone calls she had made on her office telephones, which were linked to internal telecommunications systems operated by public authorities. The Court found that such interference was illegal because, at that time, the domestic law did not regulate the interception of telephone calls made on this kind of telecommunications system. Furthermore, due to the lack of any regulation in this matter, no effective remedy had been available to the applicant to complain about the interception of her telephone calls.
Following the judgment, the intercepted material was destroyed.
New legislation was adopted, The Regulation of Investigatory Powers Act 2000, which provided for the regulation of the interception of communications. Its purpose was to prohibit the interception of communications on public and private networks and carve out from that overall prohibition certain limited circumstances whereby interception may lawfully be carried out on such networks. The intentional and unauthorised interception of a communication by means of a private telecommunications system constitutes a criminal offence. The Act also created a new civil liability: the sender, the recipient, or the intended recipient of an intercepted communication may sue the person who has the right to control the operation or the use of the telecommunication system in question. The latter will be liable unless he can show that he acted with lawful authority. Interception on a private network carried out in accordance with a warrant from the Secretary of State is lawful. Since the entry into force of the Human Rights Act in 2000, any person may bring proceedings against the authority concerned The Investigatory Powers Tribunal is competent for proceedings against the intelligence services concerning, *inter alia*, an interception of communications.

2.3. Mass surveillance

BGR / Association for European Integration and Human Rights and Ekimdzhiev group (62540/00)

Judgment final on 30/01/2008

Action Plan DH-DD(2019)401

The case concerned secret surveillance and the system of retention and subsequent accessing of communications data. The main shortcomings in the legal framework governing targeted secret surveillance found by the Court concerned: the lack of an independent control over the implementation of secret surveillance measures; the discretionary use of intelligence falling outside the scope of the original application for surveillance; the lack of sufficient safeguards in relation to surveillance carried out on national security grounds; the lack of precise regulations on screening, preserving the confidentiality and integrity and destruction of the intelligence gathered; the lack of notification of the persons subjected to secret surveillance outside criminal proceedings and the lack of an effective remedy.
So far, the measures adopted show considerable progress, such as the improvement of judicial authorisation procedures (also in the context of protection of national security), the setting up of the "National Bureau" as a monitoring body, the introduction of a compensatory remedy and a decrease in the use of secret surveillance.
Following legislative amendments in 2013 and 2015, surveillance requests must be thoroughly reasoned and substantiated and may be submitted only for the purpose of preventing or investigating an exhaustive list of serious criminal offences. As noted by the National Bureau monitoring the secret surveillance system, the safeguards with regard to the judicial authorisation of surveillance for the protection of national security are similar to those concerning criminal matters. The normal time-limits range from 20 days to six months. Under the Code of Criminal Procedure, intelligence falling outside the scope of the original application can be used only insofar as it concerns other serious criminal offences for which secret surveillance is permissible. A specific 15-year time-limit for preservation of intelligence related to certain offences concerning national security was introduced in 2015. The National Bureau notifies, of its own motion, citizens who have been subject to unlawful secret surveillance, failing certain

countervailing interests. Since 2009, it has been possible to request compensation for unlawful secret surveillance. The Supreme Court of Cassation has recently clarified the definition of "unlawfulness" in this context in its case-law.

HUN / Szabo and Vissy (37138/14)

Judgment final on 12/06/2016

Action Plan DH-DD(2021)89

The case concerned legislation on secret surveillance measures for national security purposes introduced in 2011, which did not provide for sufficiently precise, effective and comprehensive safeguards on the ordering, execution and potential redressing of such measures. The Court underlined that the scope of the measures could include virtually anyone, with new technologies enabling the Government to intercept masses of data easily concerning even persons outside the original range of operation. Furthermore, the ordering of such measures was taking place entirely within the realm of the executive and without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place.
The authorities acknowledged the need to amend the current legislation on secret surveillance measures and informed the CM about the ongoing preparatory work to this aim. In July 2018, the impugned provision on intelligence gathering for national security in the Police Act was moved to a different chapter of the same Act, the content remaining unchanged.

SER / Youth Initiative for Human Rights (48135/06)

Judgment final on 25/09/2013

Final Resolution CM/ResDH(2018)71

The case concerned the arbitrary refusal of access to information obtained via electronic surveillance by the Intelligence Agency despite a final and binding order by the Information Commissioner, a domestic body set up to ensure observance of the Freedom of Information Act 2004. The Court indicated under Article 46 that the most natural way to implement its judgment in this case would be to ensure that the agency provided the applicant NGO with the information it had requested on how many people had been subjected to electronic surveillance in 2005.
In execution of the judgment, the Intelligence Agency provided the applicant NGO with the information requested in a letter dated 19 June 2014. Moreover, the Government Agent sent clear guidelines to the Director of the Intelligence Agency as to his obligation to strictly comply with domestic law and ECHR standards with regard to the access to information gathered via electronic surveillance.

SWE / Centrum for Rättvisa (35252/08)

Judgment final on 25/05/2021

Action PlanDH-DD(2021)1287

The case concerned the alleged risk that the applicant foundation's communications would be intercepted and examined by way of intelligence signals, as it communicated on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax, often on sensitive matters.
The Court found, in particular, that the bulk interception regime suffered from three deficiencies: the absence of a clear rule on destroying intercepted material which did not contain personal data; the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration be given to the privacy interests of individuals; and the absence of an effective *ex post facto* review. As a result, the system did not meet the requirement of "end-to-end" safeguards, it overstepped the margin of appreciation left to the respondent State in that regard and, overall, did not guard against the risk of arbitrariness and abuse.
In January 2022, the Act on Personal Data Processing at the National Defence Radio Establishment entered into force. It contains detailed provisions imposing a requirement for the National Defence Radio Establishment, before deciding to transmit intelligence material to foreign partners, to analyse and assess whether a foreign data recipient provides sufficient protection for that data, thus addressing in part the shortcomings identified by the Court concerning the legislation of the transmission of intelligence of material to foreign partners. A concrete response still has to be provided with regard to the other shortcomings found by the European Court in this case.

This case concerns the disclosure by the first applicant – a military official in the Romanian Intelligence Service ("SRI") – of information on wide-scale illegal telephone tapping on the part of the SRI and of the content of some of the communications thus intercepted, including telephone conversations between the other two applicants. These disclosures during a press conference in 1996 resulted in the first applicant's conviction, in last instance by the Supreme Court of Justice in May 2002, to a suspended prison term. When it comes to the interception of communications, the European Court found violations of Articles 8 and 13 of the Convention because of the lack of safeguards in the legislation on secret surveillance measures based on national security considerations, in particular, as regards the collecting and storing of personal data by the SRI, and the absence of domestic remedies allowing to challenge the retention of such data by the same.

Law No. 255/2013, in force as of 1 February 2014, amended the relevant legal framework, namely the National Security Act and the Act governing the organisation and operation of the SRI, and addressed some of the deficiencies identified by the Court in this and other previous cases raising the same issues. This legislative reform notably introduced the requirement for judicial authorisation for secret surveillance measures on national security grounds, except in emergency situations, when such authorisation can be granted by the prosecutor for a duration of 48 hours; in this latter case, the prosecutor's authorisation is submitted to an *ex officio* judicial review and the judge can order the intelligence services to cease their activities and destroy the data collected when the authorisation was unduly granted. The judgment was widely disseminated to the courts and other competent authorities and was published in the Official Gazette.

ROM / Bucur and Toma (40238/02)

Judgment final on 08/04/2013

Action Plan DH-DD(2014)636

Communication from the authorities on the general measures (legislative amendments) DH-DD(2014)592

The case concerned certain shortcomings in the secret surveillance regime including bulk interception and obtaining communications data from communication service providers in the UK prior to 2018 (violations of Articles 8 and 10). Whilst finding that the Convention does not prohibit the use of bulk interception per se to protect national security interests and other essential national interests against serious external threats, the Court underlined the need for "end-to-end safeguards" and set out the approach to be followed in such cases. The Court found that, despite its safeguards, including some robust ones, the previous legal framework in the UK (the Regulation of Investigatory Powers Act (RIPA) 2000) which had been in place until 2018 had not contained sufficient "end-to-end safeguards" to provide adequate and effective guarantees against arbitrariness and the risk of abuse.

The Investigatory Powers Act (IPA) replaced the previous legal framework RIPA. It introduced a 'double lock' which requires warrants for the use of investigatory powers to be authorised by a Secretary of State and approved by a judge in the Office of the Investigatory Powers Commissioner. Moreover, the Investigatory Powers Commissioner ensures robust independent oversight of how these powers are used. Further measures will be prepared in order to remedy all the shortcomings identified by the European Court.

UK. / Big Brother Watch and Others (58170/13)

Judgment final on 25/05/2021

Action Plan DH-DD(2021)1326

Index of cases

ARM / Hambardzumyan 17
BGR / Association for European Integration and Human Rights and Ekimdzhiev group 22
BGR / Dimitrov-Kazakov 14
BGR / Krasimir Yordanov 4
BGR / Mironov 9
BGR / Petrov group 10
CYP / Onoufriou 10
CZE / Delta Pekárny a.s. 7
CZE / Heglas 17
ESP / Trabajo Rueda 7
ESP / Vincent Del Campo 4
EST / Libik and Others 17
EST / Slavgorodski 10
EST / Soro 4
FIN / Z. 13
FRA / Aycaguer 4
FRA / Ben Faiza 17
FRA / Brunet 15
FRA / Kruslin 17
FRA / M.K. 4
FRA / Ravon and Others 7
FRA / Slimane-Kaid 10
FRA / Vetter 18
GER / Buck 8
GRC / Modestou group 8
GRC / Peers 10
HUN / Szabo and Vissy 22
HUN / Turan 8
ITA / Calogero Diana 10
ITA / Godelli 15
ITA / Labita 10
LIT / Draksas 18
LIT / Valasinas 11
LVA / Boze 8
LVA / L.H. 13
LVA / Lavents 11
LVA / Meimanis 18
LVA / Santare and Labaznikovs 18
MDA / Bostan 8
MDA / P.T. 13
MDA / Radu 13
MDA / Savotchko 5
MKD / J.M. and A.T. 13
NLD / A.B. 11
NLD / R.V. and Others 19
POL / Joanna Szulc 15
POL / Klamecki No.2 group 11
ROM / Barbulescu 20
ROM / Bucur and Toma 23
ROM / Dragos Ioan Rusu 8
ROM / Haralambie 15
ROM / Rotaru 15
RUS / Avilkina and Others 14
RUS / Boris Popov 11
SER / Dragan Petrovic 9
SER / Youth Initiative for Human Rights 22
SUI / Kopp 19
SUI / Vukota-Bojic 19
SVN / Benedik 19
SWE / Centrum for Rättvisa 22
SWE / Segerstedt-Wiberg and Others 16
TUR / Alkaya 5
TUR / Sinan Isik 5
TUR / Tamer group 11
TUR / Tarman 5
TUR / Usla No. 2 14
UK. / Big Brother Watch and Others 23
UK. / Catt 5
UK. / Copland 21
UK. / Gaughran 6
UK. / Govell group 21
UK. / Halford 21
UK. / Liberty and Others 20
UK. / M.M. 6
UK. / Malone 20
UK. / Peck 6
UK. / R.E. 20
UK. / Roche 16
UK. / S. and Marper 7
UK. / Szuluk 12
UKR / Cases of Koval and Others group 9
UKR / Golovan 9
UKR / Mikhaylyuk and Petrov 12
UKR / Panteleyenko 9
UKR / Surikov 14
UKR / Volokhy 9
UKR / Voskoboynikov 9