COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 10 March 2016

T-PD(2016)01

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(T-PD)

DRAFT EVALUATION AND FOLLOW-UP QUESTIONNAIRE

The draft questionnaire was prepared by Claire Gayrel, Researcher at CRIDS (Research Center on Information, Law and Society).

Directorate General Human Rights and Rule of Law

Evaluation and follow-up questionnaire

Introduction

1. Objectives of the questionnaire

As stated by the Consultative Committee of the Convention (T-PD), the objective of the evaluation and follow-up process is "*to ensure the credibility of Convention 108 and to establish genuine dynamic of harmonized protection, guaranteeing that data flows between parties occur among States offering an appropriate level of protection*".[1]

The evaluation **criteria** shall be based on: "*data protection national law in force, as well as other relevant laws, in particular those providing for restrictions to the right of privacy and data protection; supervisory authority; remedies available to data subjects; and the case-law*".[2]

Besides, the questionnaire should enable to gather information on: "- *Case-law; - The constitutional, institutional, legislative and regulatory framework; - the specific institutional framework or data protection relating to supervisory authority; - the existence of awareness raising and training programs; - the main features of the development of ICTs*".[3]

The questionnaire actually pursues two types of objectives. On the one hand, the questionnaire aims at assessing compliance with the convention 108 in a given party, both *in law* and *in practice*, following convention's duty enshrined in article 4. On the other hand, the evaluations could subsequently serve to facilitate the work of the Committee, notably by enabling the identification of good practices among the parties and possibly inspire the work of the Committee to draft new legal standards. We also believe that since the Committee has opted for a transparent procedure, with the publications of the evaluation documents, the questionnaire and evaluation process could be a very useful material for academics or NGOs following data protection developments.

2. Methodology

In order to enable a "*transparent, effective and impartial*" evaluation, the elaboration of the questionnaire relies on three components.

The identification and selection of the evaluation criteria

As has been required by the Consultative Committee, the evaluation of the legislation in force and its effectiveness requires to give particular attention to Articles 2, 4, 5, 6, 7bis, 8, 8bis, 9, 10, 11, 12 and 12bis.[4] The proposed questionnaire has taken a divergent approach in some respects.

Indeed, assessing compliance with convention 108 is not an easy task, if we consider the wide range of exemptions, sectoral legislations, codes of conduct and case-law that may enter into account. In order to reach the general objectives explained above, the questionnaire shall address a wide scope of issues, both from a theoretical (how does the legislation address a principle/right/obligation), and practical (how is such principle/right/obligation enforced?) points of view. Besides, the evaluation of both the *scope*

[1] T-PD-BUR(2013)02 rev5 – *Information elements on the evaluation and follow-up mechanism*, 14 April 2014, p.3
[2] *Idem*, p. 5
[3] *Idem*, p. 6
[4] *Idem*

of exceptions on the one hand, and the *legality* and *necessity* of such exceptions on the other hand, may require the examination of many pieces of legislations. We have tried to achieve a proper balance between excessive detailed questions assessing each paragraph of the convention and essential questions that relate to the core objectives of the convention 108 as far as enhancing harmonization of protection is concerned. This is why certain criteria have been specifically tackled, while some others have been left aside.

Indeed, we believe that Articles 1 and 3, in particular with respect to the *comprehensive scope* of application of the convention (application to both the public and private sector) and the requirement to afford protection to *every individual*, whatever his or her nationality and residence, should be taken into account specifically in the course of the evaluation.

In contrast, Articles 8bis, as far as it refers to "additional obligations" and Article 11 "extended protection" have not been retained as evaluation criteria since they refer, according to us to additional protection mechanisms. We believe that these criteria could be included in a subsequent version of the questionnaire, when a complete cycle of evaluation of State Parties would be achieved. In that way, this first questionnaire focuses on the essential provisions in order to check whether harmonization is sufficiently achieved with respect to the basic principles, rights and obligations.

A double questionnaire

Two questionnaires have been elaborated for the purposes of evaluation procedure.

The first questionnaire is intended to Parties, candidates and relevant stakeholders that would be willing to participate and provide their opinion regarding the level of compliance with convention 108. As much as possible, the questions address both the level of protection afforded *in the law* and *in the practice* in order to get an accurate vision of both the formal protection of personal data in a given jurisdiction and the practical implementation and interpretation of the law by supervisory authority(ies) and courts.

The second questionnaire is addressed to the working group and mandated experts. This specific questionnaire for experts was elaborated in parallel in view to harmonize the structure of the evaluation reports of the Working group. Since only evaluation reports shall be made publicly available, we believe it is important for the working group to have a harmonized approach in the preparation of the reports.

3. Structure

The proposed questionnaire consists in 7 sections. We explain hereunder briefly, for each section, the specific objective pursued and, where relevant, the issues that receive specific emphasis in the questionnaire.

Section 1. General context (questions to States)

- *International commitments and constitutional protection*

On the one hand, the questionnaire intends to collect information regarding the international commitments (whether binding or non-binding) of the States in the field of privacy and data protection. In this respect, different questions are proposed for States that are Parties to Convention 108 and States that are not Party to the Convention. On the other hand, the questionnaire addresses the question of the constitutional protection of privacy and personal data.

- *Main features of ICTs developments (evaluators)*

As required by the Committee (see *supra* "objectives of the questionnaire"), the questionnaire should enable to collect information regarding the main features of ICTs developments in the State assessed. We suggest relying on the ICT development index

published by the United Nations International Telecommunication Union.[5] It is based on internationally agreed ICT indicators in order to measure the information society, the digital divide and compare ICT performance across countries. It is based on 11 indicators grouped in three clusters: access, use and skills as follows:

- The ***access*** sub-index captures ICT readiness, and includes five infrastructure and access indicators:
    - Fixed telephone subscriptions/100 inhabitants
    - Mobile-cellular telephone subscriptions/100 inhabitants
    - International Internet bandwidth (bits/s) per user
    - Percentage of households with a computer
    - Percentage of households with Internet access
- The ***use*** sub-index captures ICT intensity, and includes three ICT intensity and usage indicators:
    - Percentage of individuals using the Internet
    - Fixed (wired)-broadband subscriptions/100 inhabitants
    - Wireless broadband subscriptions/100 inhabitants
- The ***skills*** sub-index captures ICT capability or skills as indispensable input indicators.
    - Adult literacy rate (percentage population 15 and older who can read and write simple statements with understanding and do simple arithmetic calculations)
    - Gross enrolment ratio secondary level (total enrolment in a specific level of education as a percentage of all eligible)
    - Gross enrolment ratio tertiary level (total enrolment in a specific level of education as a percentage of all eligible).

The ICT development index allows retrieving harmonized data across countries regarding the main features of ICT development. Each year, a rank is published, and all performance data are available for each country in the form of a "*country card"*.

The evaluators should use this country card in their evaluation report as relevant context information.

Section 1 bis. General context (questions to IOs)

The case of international organisations requires addressing specific questions. Indeed, there are a number of the convention's provisions that may not be applicable to most international organisations (see *Infra* "specific issues regarding international organisations"), which are usually not subject to national legislations and benefit from a wide immunity of jurisdiction.

This implies that the regime of immunity of the international organisation must first be analysed carefully in order to assess its compatibility with an accession to convention 108. Indeed, although exceptional, a possible incompatibility might arise in case an IO is not exclusively subject to its binding data protection rules, but remain subject to certain jurisdictions' rules (as far as data processing activities are carried out in this jurisdiction). If one of these jurisdictions is neither party to convention 108 nor recognised as affording an *appropriate* level of protection according to article 12 of the convention, accession of the organisation to the convention may consequently lead to liberalise the flows of data towards such jurisdiction, creating (possibly) a loophole of protection. In practice, such a "loophole scenario" is however exceptional, It may arise when the IO is operating in a State that has

[5] All ICT development index data and rank for 2015 can be found here: http://www.itu.int/net4/ITU-D/idi/2015/

not formally recognized its privileges and immunities under a status agreement and where domestic courts do not apply customary international law relating to immunity of IOs, and finally where national legislations would actively prevent an IO from applying its own rules. In addition, such loopholes may still be considered as compatible with convention 108 if the flows of data towards that jurisdiction may be considered as entering within one of the exception provided for in article 12§4 of the convention. The regime of immunity of an IO therefore requires an evaluation on a case-by-case basis of the mandate and data processing activities of the organisation. This preliminary assessment is necessary to state whether the accession of the organisation is *compatible* or not with the goals of convention 108 to establish genuine dynamic of harmonised protection while liberalising data flows between parties.

Section 2. General data protection law(s)

This section of the questionnaire is dedicated to the general data protection legislation (in case of States) or general regulatory binding instrument (in case of international organisation). It aims at identifying the relevant provisions of the law and identifying the applicable exemptions/restrictions to certain principles. However, the specific safeguards and provisions applicable to activities that are exempted or partially exempted from the scope of the general data protection law(s) are discussed in sections 3 and 4 of the questionnaire.

This section is divided in 11 sub-topics described below that address the most important data protection principles. The questionnaire tries to deal with both the implementation *in the law* of the said principles/rights/obligations and their implementation *in practice* (in the case law, or by the supervisory authority(ies) and/or through means of recommendations).

1. Scope of application
2. Principle of legitimacy
3. Purpose limitation principle
4. Data quality principle
5. Principle of limited retention
6. Proportionality principle
7. Transparency principle
8. Principle of security
9. Individual's rights
10. Special categories of data
11. International transfers

Section 3. Legality and Necessity of exemptions for major legitimate interests of the State

This section seeks to collect the elementary information in order as to analyse the *justifications* for the exemptions to general data protection principles for data processing necessary for the protection of national security, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences as provided for in article 9§1 a) of the convention. As suggested by the Committee, the questionnaire should focus on laws that have an impact on the level of protection of personal data, in particular those providing for derogations for law enforcement or national security considerations.[6] The questionnaire addresses both issues in order to assess the compatibility of the national provisions concerned with the *legality* and *necessity* requirements of article 9.

1. Exemptions for national security considerations (secret surveillance)

[6] *Idem,* p. 6

Under this sub-section, the focus is on national provisions organising secret surveillance activities by intelligence and/or law enforcement agencies (as far as the distinction is relevant under national law) *for national security considerations*, and provisions that enable strategic, large-scale surveillance.

2. Exemptions for criminal law enforcement purposes

Under this sub-section, the focus is on other data processing activities carries out in the framework of criminal law enforcement activities (including secret surveillance by these agencies as far as it has not been dealt with in the former sub-section and other data processing). Assessing compliance with the conditions of *legality* and necessity of article 9 regarding exemptions to basic principles for the protection of personal data for criminal law enforcement data processing is a rather complex task as the differences of approach between Parties and candidates can be important. We suggest focusing on three main areas of data processing by law enforcement agencies:

- Interception of communications in the course of a *criminal investigation* (as far as interception of communications by law enforcement agencies can be distinguished from other secret surveillance activities dealt with in the former sub-section)
- Major law enforcement files
- Criminal records database

Section 4. Legality and necessity of exemptions for major legitimate interests of private parties

In the document “Information elements on the evaluation and follow-up mechanism”, the Committee has not emphasised the need to assess implementation of article 9§1 b) of the convention. We propose to consider here three main areas where basic principles for the protection of personal data as enshrined in chapter II of the convention may be derogated when necessary for the protection of rights and fundamental freedoms of others: the right to freedom of expression, intellectual property rights (copyright law), and freedom of access to information. However, considering the length and burden of the evaluation process in practice, the evaluation of this section may be postponed after a first complete cycle of evaluations will be achieved.

1. Exemptions for the protection of the data subject
2. Exemptions for the protection of the rights and fundamental freedoms of others

Section 5. Sectoral data protection instrument(s)

There may be numerous secondary legislation providing for specific data protection rules. We suggest focusing on two categories of legislations that may have a substantial impact on the individual’s rights: the legislation relating to the national identification database, and the law on census (if any).

1. National identification database
2. Census law
3. Other relevant sectoral instrument (in the private sector)
4. Codes of conduct

Section 6. Supervision and enforcement

A supervision and enforcement mechanism of the data protection rules is an essential aspect of the convention 108. Supervision and enforcement of the principles and obligations enshrined in convention 108 requires ensuring effective and independent oversight,

promoting compliance with data protection law, providing supervisory authority(ies) with the necessary enforcement powers, assisting data subjects in the exercise of their rights and providing appropriate sanctions and remedies mechanisms.

1. Ensuring effective and independent oversight
2. Promoting compliance with data protection law
3. Enforcement powers of supervisory authority(ies)
4. Assisting data subjects in the exercise of their rights
5. Sanctions and remedies mechanisms

Section 7. Contribution to the evaluation process

Finally, this section deals with the quality of the contribution(s) from stakeholders, and in particular the State or organisation concerned. This section is primarily relevant for the working group and the experts drafting the evaluation report. It is essential that the evaluation process reports whether the State or organisation participated effectively to the evaluation. It is also necessary to mention whether contributions from other stakeholders (especially contributions from the civil society) were received and the relevance of these contributions in the evaluation process.

4. Specific issues regarding of international organisations

As explained earlier, there are a number of the convention's provisions that may not be applicable to most international organisations, which are not subject to national legislations and benefit from a wide immunity of jurisdiction.

The provisions that may not be relevant to most IOs are, in particular, those referring to ***judicial redress*** in the convention 108:

- Article 10 and article 8 f.: the establishment of appropriate ***judicial sanctions*** and the right for every individual to have a ***remedy*** where his or her rights under this convention have been violated.
- Article 12bis d.: the power of competent supervisory authority(ies) to ***engage in legal proceedings or to bring to the attention of the competent judicial authorities*** violations of the provisions of this convention.
- Article 12bis §6: The possibility to ***appeal against decisions of the supervisory authority(ies***) through the courts.

The regime of immunity has a direct incidence on the responsibility of IOs and possibility for individual data subjects to exercise their right to redress. The issues of "*judicial* redress" and "remedies" in the context of IOs are a particularly complex legal matter and it is not the purpose of the present contribution to analyse in detail the European and international standards in this field.[7] However, the principle established by the European Court of Human Rights, in the context of Article 6 of the convention, is the "counterbalance" principle.[8] Indeed, if the Court generally asserts that "*the attribution of privileges and immunities to international organisations is an essential means of ensuring the proper functioning of such organisations free from unilateral interference by individual governments*", the Court examine whether the immunity from jurisdiction of an IO under the Convention is acceptable, in particular if

[7] A brief overview of the issue of responsibility of International organisations in the context of data protection is provided in a study relating to INTERPOL. See C. Gayrel and F. de Villenfagne, *Data Protection at ICPO-INTERPOL, assessment, issues and outlook,* 2011, in particular "Requirement to offer a right of access to courts and tribunals: what obligations for INTERPOL under international law?", pp. 43-52, available here : http://www.interpol.int/fr/About-INTERPOL/Structure-and-governance/CCF/External-study

[8] ECtHR, *Waite and Kennedy v. Germany*, 18 February 1999

"*applicants had available to them reasonable alternative means to protect effectively their rights*". The availability of "*reasonable alternative means*" is therefore the fundamental requirement to counterbalance the immunity from jurisdiction enjoyed by international organisations. In particular, the access to an independent agency to settle disputes appears to be an essential criterion.

Besides, provisions relating to the processing of personal data for "*the protection of national security, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences*" and for "*the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression*" (article 9) may not be fully relevant for international organisations. As a consequence, sections 3 and 4 may not be applicable to them, or only partially, depending on the mandate of the organisation concerned.

The current version of the questionnaire is primarily addressed to States and specific questions should be further elaborated to tackle the issue of judicial redress and remedies according to a slightly different standard that the one provided in the convention in order to allow accession by international organisations. Additional comments in this respect in the explanatory report could be useful.

5. Burden and length

The questionnaire is rather long and will require a substantial allocation of time and resources on the part of the State party, Candidate State or international organisation. In the same time, the questions are not "tricky" and require descriptive and informative answers regarding the state of the law, case-law and practice. The participation of supervisory authorities is essential and should facilitate the fulfillment of the questionnaire, as they are generally well aware of the legal framework and practices in place. We believe that it is the duty of the States or organisations to demonstrate in their answers effective compliance with convention 108. As a consequence, it is their responsibility to provide the necessary information following the structured questionnaire, although such a structure and organisation of topics may not be fully consistent with the way their domestic law is drafted. It is very important to highlight the responsibility of parties in this respect in the light of their duties following article 4§3 of the convention. Parties 'contribution and efforts to compile and summarise the relevant information under each section and subsection of the questionnaire in English language is also essential for the evaluation process by foreign experts.

The work of the working group involved in the evaluation should be almost exclusively analytical. As a principle, they should not be required to carry out research tasks, such as the identification and collection of relevant information and sources of law. Indeed, such tasks may be extremely time-consuming, especially for experts who are not familiar with the mandate of an organisation, or who are not country native (which should be the case). Besides, the work of experts participating to the analysis of the answers and overall evaluation is framed by a separate questionnaire requiring them to provide their opinion, with regard to the answers provided, on each specific criterion previously identified. The criteria are obviously based on the content of the principles and obligations of convention 108 and where relevant on the guidance of the European Court of Human Rights case-law.

As a consequence, much of the burden involved by the questionnaire actually relies on the States or organisations being evaluated. If States and organisations duly contribute to the evaluation with detailed answers, the work of experts is essentially limited to analysing the answers and identifying loopholes of protection or areas of divergences of opinion between the different stakeholders who contributed (e.g.: area where NGO and governmental authorities may differ).

Section 1. General context (questions to State parties and candidates)

1. International commitments and constitutional protection of privacy and personal data

Questions to State Parties or State candidates (whether member states of the Council of Europe or not):

Is the **right to private life**, or specific elements of the right to private life (e.g. the right to secrecy of communications, right to family life etc.) protected under the constitution or any other type of norm endorsing a constitutional value? What is/are the scope of such relevant rights following the main relevant case law? (Mention essential constitutional or Supreme Court's case-law in this respect)

Is the **right to data protection** or elements of such right, protected under the constitution or any other type of norm endorsing a constitutional value? What is/are the scope of the relevant rights following the main relevant case law? (Mention essential constitutional or Supreme Court's case-law in this respect)

Questions to State Parties or State candidates (not Party to Council of Europe):

What international or regional instruments, whether binding or non-binding, laying down the right to privacy or governing the collection and handling of personal information (i.e. data protection) is the Candidate State a signatory to? (mention all relevant instruments, whether it has binding effect or not, and the status of ratification)

What are the legal effects of such international commitments in the internal legal order of the Candidate State? Explain the conditions under which international norms find to apply in the Candidate State? (mention relevant constitutional provisions, if any, and the relevant case-law regarding the effect of international law in the internal legal order)

2. Main features of ICT development

Questions to evaluators

What is the rank of the State concerned in the most recent ICT development index?

See the rank established following the ICT development index here: http://www.itu.int/net4/ITU-D/idi/2015/index.html#idi2015rank-tab

What are the most interesting features of ICT development that can de extracted from the ICT Development sub-index "Access", "Use" and "Skills" of the State concerned?

See all country cards here: http://www.itu.int/net4/ITU-D/idi/2015/index.html

Section 1 bis. General context (questions to international organisations)

Mandate

What is the mandate of the organisation and what are the main purposes of data processing of the organisation?

International commitments

What international instruments, whether binding or non-binding, laying down the right to privacy or governing the collection and handling of personal information (i.e. data protection)

is the international organisation a signatory to? (mention all relevant instruments, whether it has binding effect or not, and the status of ratification)

Immunity regime

The processing of personal data by International organisations benefiting from the immunity of jurisdictions at the national level of its State Parties shall be subject to a comprehensive set of rules having a binding character (see §34 to 36 of the explanatory report)

The processing of personal data by International organisations that would benefit from a partial immunity of jurisdiction should not be subject to a jurisdiction that is not Party to convention 108 or that is not recognised as affording an appropriate level of protection.

Question to IOs

What is the mandate of the organisation and what are the main purposes of data processing of the organisation?

Does the international organisation benefit from the immunity of jurisdiction? Explain in general the extent to which the IO remains subject to national laws of one or more of its State Parties (e.g.: whether customary international law is not applied in domestic courts, and whether any instances have been identified in which domestic laws prevent the IO from applying/enforcing its rules).

In particular, are some processing of personal data carried out by the international organisation subject to the jurisdiction of States that are not parties to convention 108 or that are not recognised as affording an appropriate level of protection?

Do the rules governing the processing of personal data in the organisation have a binding character?

Question to evaluators

Is the international organisation regime of immunity, in particular regarding the processing of personal data, compatible with accession to convention 108?

Section 2. Data Protection Law(s)

3. Scope of application

Criterion

The material scope of application of the convention follows from the articles 1, 2a., 2 b. and 3 of the convention. The evaluation of the national general data protection legislation must rely on the following five criteria:

- The horizontal application of convention 108 to data processing, whether carried out in the public or private sector (art. 3§1)
- The application of the convention to the processing of "personal data", understood as "any information relating to an identified or identifiable individual" (art. 2.a.)
- The protection conferred to "every individual", "whatever his or her nationality or residence" (art. 1)
- The application to automated processing and non-automated processing of personal data within a structured set, where those data are accessible and retrievable according to specific criteria (art. 2 b.)
- Data processing carried out by an individual in the course of (purely) personal or household activities are the only ones that can be totally excluded from the scope of application. (art. 3 §1 bis).

Questions to parties and candidates

What is/are the general data protection instrument(s) regulating the processing of personal data and implementing the obligations of convention 108? (Mention here the main relevant binding instruments useful for the evaluation of the implementation of convention and having a comprehensive scope of application. Sectoral or specific legislation regulating certain processing activities should be discussed in section 3, 4 and 5 of the present questionnaire.)

- *Notion of personal data*

How is the notion of "personal data" implemented and defined in the(se) law(s)?

Which categories of person (natural and/or legal persons) benefit from the protection of personal data in the(se) law(s)?

Has the notion of personal data been interpreted in complex cases by the supervisory authority or in the case-law? If yes, how?

- *Activities covered by the general legislation(s)*

How is the notion of "data processing" implemented and defined in the(se) law(s)?

Has the notion of "data processing" been interpreted in complex cases by the supervisory authority or in the case-law? If yes, how?

To which data processing activities (automated and/or non automated) does the law apply?

To which data processing sectors does the law apply (scope of application)?

Are there activities *totally excluded* from the scope of application of the relevant general legislations? (mention only exclusions)

Questions to evaluators

Is the scope of application of the general data protection instrument(s) compatible with the whole criteria of the scope of application of convention 108? (specify possible loopholes of protection).

4. Legitimacy

Criterion

Data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law (art. 5§2)

Questions to parties and candidates

What are the legitimate bases provided by the general data protection legislation(s) for the processing of personal data?

How is the notion of “consent” defined?

Has the notion of consent been interpreted in complex cases by the supervisory authority or in the case-law following a complaint or a consultation? Or has the supervisory authority issued specific recommendations regarding consent?

Are data processing carried out on important grounds of public interests be provided by law? If yes, mention the main relevant legislations providing the legitimate basis for the following processing of personal data:

- For important economic or financial interest of the State, including monetary, budgetary and taxation matters
- Public health and social security
- Prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties
- The protection of national security
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions
- The enforcement of civil law claims
- The protection of judicial independence and judicial proceedings

Questions to evaluators

Is the definition and/or interpretation of the notion of consent compatible with the convention?

Are the other legitimate bases provided by law comparable to those listed in the explanatory report to the convention?

Are data processing carried out on important grounds of public interests (notably those foreseen in §47 of the explanatory report) provided for by law?

5. Purpose limitation principle

Criterion

Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for historical, statistical and scientific purposes is, subject to appropriate safeguards, compatible with those purposes (art. 5§4 b.)
Exceptions to the purpose limitation principle are allowed when such an exception is provided for by law and constitutes a necessary and proportionate measure in a democratic

society for the protection of national security, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences (art. 9 §1 a.); or the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.(art 9§1 b.)

Questions to parties and candidates

How does the law provide for the purpose limitation principle and principle of further compatible use?

Has this principle been interpreted in complex cases by the supervisory authority or in case-law following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the purpose limitation principle in practice?

What are the safeguards applicable to the processing of personal data for historical, statistical and scientific purposes?

What are, if any, the data processing activities exempted from this principle?

Questions to evaluators

Is the implementation of the purpose limitation principle *in the law* compatible with the convention?

Does the application of the purpose limitation principle seem compatible with the convention *in practice*?

Are the exceptions to the purpose limitation principle strictly limited to data processing activities foreseen in article 9§1 of the convention?

6. Data quality principle

Criterion

Personal data undergoing processing shall be adequate, relevant and not excessive in relation to the purposes for which they are processed (art. 5§4 c.); accurate and, where necessary, kept up to date (art. 5§4 d.)

Exceptions to the data limitation principle are allowed when such an exception is provided for by law and constitutes a necessary and proportionate measure in a democratic society for the protection of national security, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences (art. 9 §1 a.); or the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.(art 9§1 b.)

Questions to parties and candidates

How does the law provide for the data quality principle?

Has this principle been interpreted in complex cases by the supervisory authority or in case law following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the data quality principle in practice?

What are, if any, the data processing activities, exempted from this principle?

Questions to evaluators

Is the implementation of the data quality principle *in the law* compatible with the convention?

Does the application of this principle seem compatible with the convention *in practice*?

Are the exceptions to the data quality principle strictly limited to data processing activities foreseen in article 9§1 of the convention?

7. Principle of limited retention

Criterion

Personal data undergoing processing shall be preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

Exceptions to the data limitation principle are allowed when such an exception is provided for by law and constitutes a necessary and proportionate measure in a democratic society for the protection of national security, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences (art. 9 §1 a.); or the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.(art 9§1 b.)

Questions to parties and candidates

How does the law provide for the principle of limited retention?

Has this principle been interpreted in complex cases by the supervisory authority or in case law following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the principle of limited retention in practice?

What are, if any, the data processing activities, exempted from this principle?

Questions to evaluators

Is the implementation of the principle of limited retention *in the law* compatible with the convention?

Does the application of the principle of limited retention seem compatible with the convention *in practice*?

Are the exceptions to the principle of limited retention strictly limited to data processing activities foreseen in article 9§1 of the convention?

8. Principle of proportionality

Criterion

Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

Questions to parties and candidates

How does the law provide for the principle of proportionality applied at all stages of a data processing?

Has this principle been interpreted in complex cases by the supervisory authority or in caselaw following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the principle of proportionality at all stages of data processing?

What are, if any, the data processing activities, exempted from this principle?

Questions to evaluators

Is the implementation of the principle of proportionality *in the law* compatible with the convention?

Does the application of the principle of proportionality seem compatible with the convention *in practice*?

Are there exceptions to the principle of proportionality?

9. Transparency principle

Criterion - principle

The principle of transparency follows from several provisions of the convention. First the convention demands that personal data undergoing processing shall be processed fairly and in a transparent manner (art. 5§4 a.). Second, each Party shall provide that the controller informs the data subjects of: a) the controller's identity and habitual residence or establishment; b) the legal basis and the purposes of the intended processing; c) the categories of personal data processed; d) the recipients or categories of recipients of the personal data, if any; and e) the means of exercising the rights set out in Article 8; as well as any necessary additional information in order to ensure fair and transparent processing of the personal data (art. 7bis§1). Third, every individual shall have a right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her (art. 8 c.).

Questions to parties and candidates

How does the law provide for the principle of transparency of a data processing? (*mention all relevant provisions, except those relating to individual's access rights*)

Has this principle been interpreted in complex cases by the supervisory authority or in case-law following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the principle of transparency?

Exceptions

Exceptions to the principle of transparency are allowed in the following cases:

- where the data subject already has the relevant information (art. 7bis §1bis)

- Where the personal data are not collected from the data subjects and the processing is expressly prescribed by law (art. 7bis §2)

- Where the personal data are not collected from the data subjects and compliance with the information duty proves to be impossible or involves disproportionate efforts (art.7bis §2)

- when such an exception is provided for by law and constitutes a necessary and proportionate measure in a democratic society for the protection of national security, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences (art. 9 §1 a.);

- when such an exception is provided for by law and constitutes a necessary and proportionate measure in a democratic society for the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression. (art 9§1 b.)

Restrictions to the principle of transparency may be provided for by law with respect to data processing for historical, statistical and scientific purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects (art. 9§2)

Questions to parties and candidates

What are the data processing activities and/or data processing sectors exempted from the transparency principle **when personal data are directly collected from the data subjects**?

What are the data processing activities and/or data processing sectors exempted from the transparency principle **when personal data are not directly collected from the data subjects**?

Are there **restrictions** (partial application of the transparency principle to certain data processing activities) to the principle of transparency?

Has this principle been interpreted in complex cases by the supervisory authority or in caselaw following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the principle of transparency in practice?

Questions to evaluators

Is the transparency principle adequately implemented in the law?

Are the exceptions to the transparency principle strictly limited to those allowed under art. 7bis and 9§1 of the convention? (whether in cases of direct or indirect collection)

Are the restrictions to the transparency principle strictly limited to those allowed under article 9§2 of the convention?

Does the application of the principle of transparency seem compatible with the convention *in practice*?

10. Principle of security

Criterion

Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

Each Party shall provide that the controller shall notify, without delay, at least the competent supervisory authority within the meaning of Article 12bis of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects. (art. 7)

Exceptions to the obligation of notification is allowed when such an exception is provided for by law and constitutes a necessary and proportionate measure in a democratic society for the protection of national security, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences (art. 9 §1 a.); or the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.(art 9§1 b.)

Questions to parties and candidates

How does the law provide for the principle of data security?

Has this principle been interpreted in complex cases by the supervisory authority or in caselaw following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the principle of data security?

How is the principle of data breach notification provided in the law?

What are the data processing activities and/or data processing sectors exempted from the principle of data breach notification?

Questions to evaluators

Is the principle of data security adequately implemented *in the law*?

Does the application of the security principle seem compatible with the convention in practice?

Are the exceptions to the principle of data breach notification strictly limited to those foreseen in article 9§1 of the convention?

11. Individual's rights

Criterion – right of access

Right of access: every individual shall have a *right to obtain*, on request, *at reasonable intervals* and *without excessive delay or expense, confirmation* of the processing of personal data relating to him or her; the communication *in an intelligible form of the data processed*; all available information on *their origin*, on the *preservation period* as well as any other information that the controller is required to provide in order to ensure the transparency of processing (art. 8 b.)

Questions to parties and candidates

How is the individual's right of access provided by the law?

Has this principle been interpreted in complex cases by the supervisory authority or in case-law following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the individual's right of access?

Criterion – right of rectification

Right of rectification and erasure: every individual shall have a right to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being or have been processed contrary to the provisions of this Convention (art. 8 e.)

Questions to parties and candidates

How is the individual's right of rectification provided by the law?

Has this principle been interpreted in complex cases by the supervisory authority or in case-law following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the individual's right of rectification?

Criterion – right of opposition

Right of opposition: every individual shall have a right to object at any time to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms (art. 8 d.)

Questions to parties and candidates

How is the individual's right of access provided by the law?

Has this principle been interpreted in complex cases by the supervisory authority or in caselaw following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the individual's right of opposition?

Criterion – safeguards in case of automated individual decisions

Safeguards in case of **individual automated decisions**: Every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration (art. 8 a.)

Questions to parties and candidates

How is the individual's right not to be subject to an automated individual decision without having his/her view taken into account provided by the law?

Has this principle been interpreted in complex cases by the supervisory authority or in caselaw following a complaint or a consultation? If yes, how?

Has the supervisory authority issued, on its own initiative, specific recommendations to promote compliance with the individual's right not to be subject to an automated individual decision?

Exceptions

Exceptions to the above-mentioned rights are allowed when such an exception is provided for by law and constitutes a necessary and proportionate measure in a democratic society for the protection of national security, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences (art. 9 §1 a.); or for the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.(art 9§1 b.)

Restrictions to the principle of transparency may be provided for by law with respect to data processing for historical, statistical and scientific purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects (art. 9§2)

Questions to parties and candidates

What are the data processing activities and/or data processing sectors exempted from the rights of access, rectification, opposition and right not to be subject to an automated individual decision without having his/her view taken into account?

Are there restrictions to the rights of access, rectification, opposition and right not to be subject to an automated individual decision without having his/her view taken into account?

Questions to evaluators

Is the right of access adequately implemented in the law?

Does the right of access appear to be adequately applied in practice?

Is the right of rectification adequately implemented in the law?

Does the right of rectification appear to be adequately applied in practice?

Is the right of opposition adequately implemented in the law?

Does the right of opposition appear to be adequately applied in practice?

Is the right not to be subject to an automated individual decision without having his/her view taken into account adequately implemented in the law?

Does the right not to be subject to automated individual decision appear to be adequately applied in practice?

Are the exceptions to the individual's rights limited to those allowed under 9§1 of the convention?

Are the restrictions to the individual's rights strictly limited to those allowed under article 9§2 of the convention?

12. Special categories of personal data

Criterion

The processing of genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life; shall only be allowed where specific and additional appropriate safeguards are enshrined in law, complementing those of this Convention.

Questions to parties and candidates

Does the law identify special categories of data subject to a specific regime? If yes, mention all categories of personal data

What are, if any, the specific and additional safeguards enshrined in law for the processing if such categories of personal data? (Mention most important safeguards)

Questions to evaluators

Are special categories of personal data foreseen in the law in compliance with those identified under article 6 of the convention?

Is the processing of such categories of personal data subject to specific and additional safeguards? If yes, can such safeguards be considered as guarding against the risks that the processing of such sensitive data may present to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination?

13. International transfers

Criterion

Principle of free flows of personal data between parties to convention 108: A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may however do so if bound by harmonised rules of protection shared by States belonging to a regional international organisation.

Restrictions to transfers towards non-parties to convention 108: When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this

Convention, the transfer of personal data may only take place where an ***appropriate level of protection*** based on the provisions of this Convention is secured. An appropriate level of protection can be secured by: a) the law of that State or international organisation, including the applicable international treaties or agreements; or b) ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.

Exceptions: each Party may provide that the transfer of personal data may take place if: a) the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or b) the specific interests of the data subject require it in the particular case; or c) prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society.

Questions to parties and candidates

Does the law provide for restrictions regarding transfers of personal data? How are they established? Towards which categories of destinations?

Questions to evaluators

Are transfers of personal data between parties to convention 108 subject to any restriction?

Are transfers of personal data towards non parties to convention 108 subject to a condition of appropriate level of protection defined in compliance with article 12§3 of the convention?

Are exceptions to such restrictions compliant with those listed in article 12§4 of the convention?

Section 4. *Legality* and *necessity* of exemptions for major legitimate interests of the State (article 9§1)

14. Exemptions for national security considerations (secret surveillance)

The exemptions to basic principles for the protection of personal data (chapter II of the convention) for data processing carried out for national security purposes shall satisfy the criteria of *legality* and *necessity* derived from article 8 of the ECHR.

The legality criterion requires that the measures be prescribed by an accessible and foreseeable law, which must be sufficiently detailed (§89 of the explanatory report). Foreseeability in the special context of secret measures of surveillance requires the domestic law to be **sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which** public authorities are empowered to resort to any such measures (*Roman Zakharov v. Russia*). Besides, the notion of national security should be understood strictly in the sense of protecting the national sovereignty of the State against internal or external threats, including the protection of the international relations of the State, and interpreted on the basis of the relevant case-law of the ECtHR, which includes in particular the protection of State security and constitutional democracy from espionage, terrorism, support for terrorism and separatism (explanatory report §90).

In particular, the ECtHR held that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are **strictly necessary** for safeguarding democratic institutions (*Kennedy v. the United Kingdom*). In practice, there have to be **adequate and effective guarantees against abuse.** The assessment of this matter depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (*Klass and Others v. Germany*). Interferences by the executive authorities with an individual's rights should be subject to an **effective control** which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

Questions to State parties and candidates

Are data processing for the protection of national security *provided for by law*? Which is/are the main legal bases for such processing?

In general, how the notion of national security is understood in the candidate State or State Party? (According to the constitution, relevant legislative acts, case-law or practice)?

How do(es) such law(s) organise secret surveillance measures? For which purposes secret surveillance measures for national security considerations may be adopted? Mention the relevant provisions providing for the basis of secret surveillance measures for national security considerations.

To which safeguards are such measures of secret surveillance subject? Explain the safeguards provided in particular with respect to the nature, scope and duration of the possible measures, grounds required for ordering them, authorities competent to authorize, carry out and supervise them and the kind of remedy provided for by law.

Questions to evaluators

Are data processing necessary for national security considerations provided for by law?

Do such law(s) or any other law organize and/or enable the conduct of strategic, large scale, or indiscriminate secret surveillance?

Do the conditions applicable to secret surveillance measures for considerations of national security appear to afford adequate and effective guarantees against abuse? The assessment requires taking into account the nature, scope and duration of the possible measures, grounds required for ordering them, authorities competent to authorise, carry out and supervise them (see *infra*) and the kind of remedy provided for by law.

More specifically, is the supervision and review *a posteriori* of secret surveillance measures for national security considerations subject to an effective independent control (preferably judicial)?

In conclusion, can it be considered that secret surveillance measures for national security considerations satisfy the conditions of *legality* (accessible and foreseeable law) and *necessity* of the convention 108, as expressed and interpreted under ECtHR case law?

15. Exemptions for criminal law enforcement purposes

Questions to candidates and parties

Which is/are the main legal basis for data processing for criminal law enforcement purposes?

1) Interception of communications

To which extent interception of communications by law enforcement authorities for purposes of criminal law enforcement derogate to the following basic principles for the protection of personal data? Justify the reasons for such limitations for each convention principle that does not apply to the interception of communications.

- *Purpose limitation principle*

For which purposes (types of offences) can a measure of interception of communications be ordered?

- *Data quality principle*

Are there any data quality safeguards applicable?

- *Principle of limited retention*

What is the retention duration of the communications?

- *Data security principle*

To which security measures are such law enforcement file(s) subject according to the law?

- *Transparency principle*

To which extent interception of communications derogate to the principle of transparency? (explain the time and conditions under which the person concerned becomes aware that his/her communications have been intercepted)

- *Individual's rights*

What are the conditions for individual's access, rectification and/or deletion of communication records held by law enforcement authority(ies)?

2) Major law enforcement files (except criminal records see *Infra*)

To which extent law enforcement files derogate to the following basic principles for the protection of personal data? Justify the reasons for such limitations for each convention principle that does not apply to law enforcement file(s).

- *Purpose limitation principle*

What are the primary purposes of the law enforcement file(s) established by law?

Under which conditions (for which secondary purposes) can they be used and accessed to by public and/or private authorities?

- *Data quality principle*

Are there any data quality safeguards applicable to law enforcement file(s)?

- *Principle of limited retention*

What are the retention durations established for the(se) law enforcement file(s)

- *Data security principle*

To which security measures are such law enforcement file(s) subject according to the law?

- *Transparency principle*

To which extent do such law enforcement file(s) derogate to the principle of transparency?

- *Individual's rights*

What are the conditions for individual's access, rectification and/or deletion of records held in law enforcement file(s)?

3) Criminal records

To which extent criminal records database derogate to the following basic principles for the protection of personal data? Justify the reasons for such limitations for each convention principle that does not apply to law enforcement file(s).

- *Purpose limitation principle*

How is organized the criminal records database? Under which conditions can it be used and access to by public and/or private authorities?

- *Data quality principle*

How is data quality of criminal records ensured?

- *Principle of limited retention*

What are the retention duration of criminal records?

- *Data security principle*

Is the criminal records database subject to protection against unauthorized access/consultation?

- *Transparency principle*

How is transparency about the functioning of the criminal records database ensured?

- *Individual's rights*

What are the conditions for individual's access, rectification and/or deletion of criminal records?

Questions to evaluators

Are main data processing for criminal law enforcement purposes duly provided for by law?

Do the limitations to the basic principles for the protection of personal data for criminal law enforcement purposes appear adequately justified?

Can it be considered that data processing for criminal law enforcement purposes satisfy the conditions of *legality* (accessible and foreseeable law) and *necessity* of the convention 108?

Section 5. *Legality* and *necessity* of exemptions for major interests of private parties (article 9§2)

16. Exemptions for the protection of the data subject

Question to Party and candidate

Are there any limitations to the basic principles for the protection of personal data (principle of legitimacy, data quality principle, principle of limited retention, data security principle, transparency principle or individual's rights), which are justified on the ground of the protection of the data subject? Justify the reasons for such limitations.

Question to evaluator

Are the exemptions to basic data protection principles for reasons of protecting the data subjects appear sufficiently justified?

17. Exemptions for the protection of the rights and fundamental freedoms of others

Question to parties and candidates

How is foreseen the articulation between the right to data protection and the right to freedom of expression? Mention main relevant provisions and case-law.

Are there any limitations to the basic principles for the protection of personal data that are justified on the ground of protection of rights related to copyright?

Is there any legislation organising access to public information in your jurisdiction? If yes, how is the right of access to documents held by public institutions articulated with personal data protection law?

Are there any other domains where a fundamental right and freedom justify limitations to the basic principles for the protection of personal data? If yes, how are such rights articulated?

Questions to evaluators

Do the limitations to the basic principles for the protection of personal data for the protection of freedom of expression appear adequately justified and articulated in the law?

Do the limitations to the basic principles for the protection of personal data for the protection of intellectual property rights appear adequately justified and articulated in the law?

Do the limitations to the basic principles for the protection of personal data for the protection of freedom of access to information appear adequately justified and articulated in the law?

Do other limitations to the basic principles for the protection of personal data for the protection of freedom of access to information appear adequately justified and articulated in the law?

Section 6. Other Sectoral Data Protection Law and codes of conduct

With respect to data processing carried out in the public sector, is there any law providing for the establishment of a national identification database? If yes, what are the specific data protection safeguards applicable to the management of such database?

Is there any law organizing a periodic census? If yes, explain how the census works and the specific data protection safeguards applicable to the census operation?

Are there any other data processing activities in the public or private sector subject to specific sectoral legislations (e.g.: in the field of credit reporting)? Mention the most relevant specific legislations and explain briefly their scope of application.

What are the main relevant codes of conduct applicable to specific data processing?

Section 7. Supervision & Enforcement

18. Ensuring effective and independent oversight

Establishment of supervisory authority(ies)

Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this convention. (art. 12bis §1)

Criterion of independence

The supervisory authority(ies) shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions (art. 12bis §4)

Criterion of capacity

Each Party shall ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions and exercise of their powers.

Criterion of accountability

Each supervisory authority shall prepare and publish a periodical report outlining its activities. (art. 12bis §5bis) Members and staff of the supervisory authorities shall be bound by obligations of confidentiality with regard to confidential information they have access to or have had access to in the performance of their duties and exercise of their powers. (art. 12bis §5 ter) Decisions of the supervisory authority(ies) may be appealed against through the courts (art. 12 bis §6).[9]

Questions to parties and candidates

What are the supervisory authority(ies) responsible for ensuring compliance with data protection principles and obligations?

Is/Are such supervisory authority(ies) independent according to statutory provisions?

How does the law ensure that supervisory authorities act with complete independence?

What is the composition of the supervisory authorities? How are its members appointed? How is revocation or cessation of functions organized?

How much is the annual budget of the said authorities?

Can supervisory authority(ies) employ their staff freely? How much people are presently employed by the said authorities?

[9] This requirement may not be applicable to IOs

Are members of the supervisory authority(ies) subject to an obligation of confidentiality with regard to confidential information they have access to or have had access to in the performance of their duties and exercise of their powers?

Shall the supervisory authority(ies) prepare and publish a periodical report outlining its activities?

Can decisions of the supervisory authority(ies) be appealed against through the court?

Questions to evaluators

Can it be considered that supervisory authority(ies) enjoy complete independence in the exercise of its/their functions? In particular, is the criterion of independence of supervisory authority(ies) adequately tackled in the law?

Can it be considered that the said authorities are in capacity to work effectively to accomplish their functions? (in particular with respect to their staff support and financial capacity)

Can it be considered that the supervisory authority(ies) are accountable for their decisions and actions?

19. Promoting compliance with data protection law

Supervisory authority(ies) shall promote public awareness of their functions and powers as well as their activities; public awareness of the rights of data subjects and the exercise of such rights; awareness of controllers and processors of their responsibilities under this convention (art.12bis §2 e.)

Questions to parties and candidates

Is there an obligation of registration/notification of activities of processing in force with respect to the public and/or private sector? If yes, how many processing have been registered in the last years?

Is there a system of complaints available to individuals? If yes, how many complaints have been launched by individuals in the last years?

Are there any available survey results (conducted by supervisory authorities or other bodies) concerning the level of public awareness (whether among data controllers and/or data subjects) regarding data protection? If yes, indicate which organism organized the survey, the date when it was conducted and the main relevant results.

Are there any available statistics regarding website visits of the supervisory authority or other relevant figures/statistics that may be enlightening as to the work of promotion of compliance with data protection? Provide main relevant figures.

Questions to evaluators

Taking into account previous answers to the questionnaire regarding the actions taken by supervisory authorities to raise public awareness with respect to data protection rights and obligations, can it be considered that the supervisory authority(ies) do(es) actively promote compliance with data protection law?

Do available figures and statistics demonstrate a low/medium/high degree of awareness and/or increasing degree of public awareness regarding data protection?

20. Enforcement powers of supervisory authority(ies)

Investigation and intervention powers

Each party shall provide that supervisory authority(ies) shall have powers of investigation and intervention (Art. 12bis §2 a.).

Consultation powers

The competent supervisory authority(ies) shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data (art.12bis §2 2bis)

Supervision of international transfers

The competent supervisory authority shall perform the functions relating to transfers of data provided for under Article 12, notably the approval of standardised safeguards;

Each party shall provide that the competent supervisory authority is provided with all relevant information concerning the transfers of data under *ad hoc* or approved standardized safeguards and upon request regarding transfers carried out outside appropriate safeguards, in particular those carried out for the specific interests of the data subject in a particular case or when prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society (art. 12§5).

Each party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend, or subject to condition such transfers. (art. 12§6). Exceptions to the provisions of this article are allowed insofar as they constitute a necessary and proportionate measure in a democratic society for the freedom of expression (art. 12§7).

Questions to parties and candidates

What are the investigation powers of the supervisory authority(ies)? Can it act on complaint and/or on its own initiative?

What are the powers of intervention of the supervisory authority(ies)? (e.g.: power to impose rectification, deletion, or destruction of inaccurate information; power to seek mandatory injunctions against controllers who would not cooperate in the course of an investigation, data processing prior check mechanisms, power to refer cases to national parliaments or other institutions et cet...)

What are the consultation powers of the supervisory authority(ies)?

How many consultations have been carried out in the last years?

What are the powers of the supervisory authority(ies) regarding international transfers?

Questions to evaluators

Do(es) the supervisory authorities enjoy appropriate investigation, intervention and consultation powers so as to ensure compliance with the provisions of the convention?

Do(es) the supervisory authority(ies) duly monitor authorizations of international transfers of data?

21. Providing assistance to data subjects in the exercise of their rights

Criterion: dealing with complaints

Every individual shall have a right to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 12bis, in exercising his or her rights under this Convention (art. 8 g.) In particular, each competent supervisory authority(ies) shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress (art. 12 bis §3).

Criterion: request for assistance on behalf of a data subject

Besides, each party shall assist any data subject, whatever his or her nationality or residence, to exercise his or her rights under Article 8 of the convention. Where a data subject resides in the territory of another party, he or she shall be given the option of submitting the request through the intermediary of the supervisory authority designated by that party (art. 14).

Questions to parties and candidates

Can all data subjects, whatever his or her nationality and residence, lodge complaints or requests for assistance to the supervisory authority(ies)?

Is there any mechanism of cooperation with other supervisory authority(ies) established in other jurisdictions to deal with complaints of a data subject having a transnational character?

What are the specific actions taken by the supervisory authority(ies) to assist data subjects in the exercise of their rights?

Questions to evaluators

Does the system ensure appropriate assistance to all data subjects, whatever his or her nationality or residence, in the exercise of their rights?

22. Sanctions and remedies mechanisms

Every individual shall have a right to have a remedy where his or her rights under this convention have been violated (art. 8 f.) and each party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this convention (art. 10).[10]

In particular, supervisory authority(ies) shall have powers to issue decisions with respect to violations of the provisions of this convention and may, in particular, impose administrative sanctions (art. 12bis §2 c.)

Besides, they shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of the convention (art. 12bis §2 d.)[11]

Questions to parties and candidates

Do(es) supervisory authority(ies) have a power of sanctions with respect to violations of the data protection law? What is the nature of such sanctions?

[10] This requirement may only be partially applicable to IOs

[11] This requirement may not be applicable to IOs

Can they engage in legal proceedings or bring to the attention of the competent judicial authorities violations of the convention? Under which conditions?

What are the available remedies mechanisms to data subjects in case of violations of the law?

Questions to evaluators

Does the system provide for appropriate judicial and non judicial sanctions and remedies in case of violations of the data protection law?

Section 8: General context of the evaluation process

1. Duty to contribute to the evaluation process

Criterion

Each Party undertakes: a. to allow the Convention Committee provided for in Chapter V to evaluate the effectiveness of the measures it has taken in its law to give effect to the provisions of this Convention; and b. to contribute actively to this evaluation process. (art 4§3)

Questions to Parties and candidates stakeholders

Please indicate you role for the purpose of this evaluation?

Questions to evaluators

Has the State Party, Candidate State or international organisation duly completed the questionnaire and provided satisfactory contributions so as to allow a proper evaluation of the compliance with the convention?

Have other relevant stakeholders contributed? Indicate which organisation, academic or NGO sent contributions and mention their overall relevance in relation to the evaluation process.