MINISTERS' DEPUTIES CM Documents **CM(2018)2-addfinal** 18 May 2018

128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018)

Ad hoc Committee on Data Protection (CAHDATA) –

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

Explanatory report

I. Introduction

1. In the 35 years that have elapsed since the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data, also known as Convention 108 (hereafter also referred to as "the Convention") was opened for signature, the Convention has served as the foundation for international data protection law in over 40 European countries. It has also influenced policy and legislation far beyond Europe's shores. With new challenges to human rights and fundamental freedoms, notably to the right to private life, arising every day, it appeared clear that the Convention should be modernised in order to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies (IT), the globalisation of processing operations and the ever greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism.

2. A broad consensus on the following aspects of the modernisation process emerged: the general and technologically neutral nature of the Convention's provisions must be maintained; the Convention's coherence and compatibility with other legal frameworks must be preserved; and the Convention's open character, which gives it a unique potential as a universal standard, must be reaffirmed. The text of the Convention is of a general nature and can be supplemented with more detailed soft-law sectoral texts in the form notably of Committee of Ministers' recommendations elaborated with the participation of interested stakeholders.

3. The modernisation work was carried out in the broader context of various parallel reforms of international data protection instruments and taking due account of the 1980 (revised in 2013) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD), the 1990 United Nations Guidelines for the Regulation of Computerized Personal Data Files, the European Union's (EU) framework[1] since 1995, the Asia-Pacific Economic Cooperation Privacy framework (2004) and the 2009 "International Standards on the Protection of Privacy with regard to the processing of Personal Data".[2] With regard to the EU data protection reform package in particular, the works ran in parallel and utmost care was taken to ensure consistency between both legal frameworks. The EU data protection framework gives substance and amplifies the principles of Convention 108 and takes into account accession to Convention 108, notably with regard to international transfers.[3]

4. The Consultative Committee set up by Article 18 of the Convention prepared draft modernisation proposals which were adopted at its 29th Plenary meeting (27-30 November 2012) and submitted to the Committee of Ministers. The Committee of Ministers subsequently entrusted the *ad hoc* Committee on data protection (CAHDATA) with the task of finalising the modernisation proposals. This was completed on the occasion of the 3rd meeting of the CAHDATA (1-3 December 2014). Further to the finalisation of the EU data protection framework, another CAHDATA was established with a view to examine outstanding issues. The last CAHDATA meeting (15-16 June 2016) finalised its proposals and transmitted them to the Committee of Ministers for consideration and adoption.

5. The text of this explanatory report is intended to guide and assist the application of the provisions of the Convention and provides an indication as to how the drafters envisaged the operation of the Convention.

6. The Committee of Ministers has endorsed the explanatory report. In this respect, the explanatory report forms part of the context in which the meaning of certain terms used in the Convention is to be ascertained (note: ref. Article 31, paragraphs 1 and 2 of the United Nations Vienna Convention on the Law of Treaties).

The Protocol was adopted by the Committee of Ministers on 18 May 2018. The appendix to the Protocol forms an integral part of the Protocol and has the same legal value as the other provisions of the Protocol.

This Protocol was opened for signature in Strasbourg,[on 25 June 2018].

II. Commentaries

7. The purpose of this Protocol is to modernise the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108) and its Additional Protocol regarding supervisory authorities and transborder flows (ETS No. 181), and to strengthen their application. From its entry into force, the Additional Protocol shall be considered an integral part of the Convention as amended.

8. The explanatory reports to Convention 108 and to its additional protocol remain relevant in so far as they provide historical context and describe the evolution of both instruments, and they can be read in conjunction with the present document for those purposes.

Preamble

9. The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms.

10. A major objective of the Convention is to put individuals in a position to know about, to understand and to control the processing of their personal data by others. Accordingly, the preamble expressly refers to the right to personal autonomy and the right to control one's personal data, which stems in particular from the right to privacy, as well as to the dignity of individuals. Human dignity requires that safeguards be put in place when processing personal data, in order for individuals not to be treated as mere objects.

11. Taking into account the role of the right to protection of personal data in society, the preamble underlines the principle that the interests, rights and fundamental freedoms of individuals have, where necessary, to be reconciled with each other. It is in order to maintain a careful balance between the different interests, rights and fundamental freedoms that the Convention lays down certain conditions and restrictions with regard to the processing of information and the protection of personal data. The right to data protection is for instance to be considered alongside the right to 'freedom of expression' as laid down in Article 10 of the European Convention on Human Rights (ETS No. 5), which includes the freedom to hold opinions and to receive and impart information. Furthermore, the Convention confirms that the exercise of the right to data protection, which is not absolute, should notably not be used as a general means to prevent public access to official documents.[4]

12. Convention 108, through the principles it lays down and the values it enshrines, protects the individual while providing a framework for international data flows. This is important as global information flows play an increasingly significant role in modern society, enabling the exercise of fundamental rights and freedoms while triggering innovation and fostering social and economic progress, while also playing a vital role in ensuring public safety. The

flow of personal data in an information and communication society must respect the fundamental rights and freedoms of individuals. Furthermore, the development and use of innovative technologies should also respect those rights. This will help to build trust in innovation and new technologies and further enable their development.

13. As international co-operation between supervisory authorities is a key element for effective protection of individuals, the Convention aims to reinforce such co-operation, notably by requiring Parties to render mutual assistance, and providing the appropriate legal basis for a framework of co-operation and exchange of information for investigations and enforcement.

Chapter I – General provisions

Article 1 – Object and purpose

14. The first article describes the Convention's object and purpose. This article focuses on the subject of protection: individuals are to be protected when their personal data is processed.[5] More recently, data protection has been included as a fundamental right in Article 8 of the Charter of Fundamental Rights of the EU as well as in the constitutions of several Parties to the Convention.

15. The guarantees set out in the Convention are extended to every individual regardless of nationality or residence. No discrimination between citizens and third country nationals in the application of these guarantees is allowed.[6] Clauses restricting data protection to a State's own nationals or legally resident foreign nationals would be incompatible with the Convention.

Article 2 – Definitions

16. The definitions used in this Convention are meant to ensure the uniform application of terms to express certain fundamental concepts in national legislation.

Litt. a. – "personal data"

17. "Identifiable individual" means a person who can be directly or indirectly identified. An individual is not considered "identifiable" if his or her identification would require unreasonable time, effort or resources. Such is the case, for example, when identifying a data subject would require excessively complex, long and costly operations. The issue of what constitutes "unreasonable time, efforts or resources" should be assessed on a case-by-case basis. For example, consideration could be given to the purpose of the processing and taking into account objective criteria such as the cost, the benefits of such an identification, the type of controller, the technology used, etc. Furthermore, technological and other developments may change what constitutes "unreasonable time, effort or other resources".

18. The notion of "identifiable" refers not only to the individual's civil or legal identity as such, but also to what may allow to "individualise" or single out (and thus allow to treat differently) one person from others. This "individualisation" could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, biometric or genetic data, location data, an IP address, or other identifier. The use of a pseudonym or of any digital identifier/digital identity does not lead to anonymisation of the data as the data subject can still be identifiable or individualised. Pseudonymous data is thus to be considered as personal data and is covered by the provisions of the Convention. The quality of the pseudonymisation techniques applied should be duly taken into account when assessing the appropriateness of safeguards implemented to mitigate the risks to data subjects.

19. Data is to be considered as anonymous only as long as it is impossible to re-identify the data subject or if such re-identification would require unreasonable time, effort or resources, taking into consideration the available technology at the time of the processing and technological developments. Data that appears to be anonymous because it is not accompanied by any obvious identifying element may, nevertheless in particular cases (not requiring unreasonable time, effort or resources), permit the identification of an individual. This is the case, for example, where it is possible for the controller or any person to identify the individual through the combination of

different types of data, such as physical, physiological, genetic, economic, or social data (combination of data on the age, sex, occupation, geolocation, family status, etc.). Where this is the case, the data may not be considered anonymous and is covered by the provisions of the Convention.

20. When data is made anonymous, appropriate means should be put in place to avoid re-identification of data subjects, in particular, all technical means should be implemented in order to guarantee that the individual is not, or is no longer, identifiable. They should be regularly re-evaluated in light of the fast pace of technological development.

Litt. b. and c. – "data processing"

21. "Data processing" starts from the collection of personal data and covers all operations performed on personal data, whether partially or totally automated. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria, allowing the controller or any other person to search, combine or correlate the data related to a specific data subject.

Litt. d. –"controller"

22. "Controller" refers to the person or body having decision-making power concerning the purposes and means of the processing, whether this power derives from a legal designation or factual circumstances that are to be assessed on a case-by-case basis. In some cases, there may be multiple controllers or co-controllers (jointly responsible for a processing and possibly responsible for different aspects of that processing). When assessing whether the person or body is a controller, special account should be taken of whether that person or body determines the reasons justifying the processing, in other terms its purposes and the means used for it. Further relevant factors for this assessment include whether the person or body has control over the processing methods, the choice of data to be processed and who is allowed to access it. Those who are not directly subject to the controller and carry out the processing on the controller's behalf, and solely according to the controller's instructions, are to be considered processors. The controller remains responsible for the processing also where a processor is processing the data on his or her behalf.

Litt. e. – "recipient"

23. "Recipient" is an individual or an entity who receives personal data or to whom personal data is made available. Depending on the circumstances, the recipient may be a controller or a processor. For example, an enterprise can send certain data of employees to a government department that will process it as a controller for tax purposes. It may send it to a company offering storage services and acting as a processor. The recipient can be a public authority or an entity that has been granted the right to exercise a public function but where the data received by the authority or entity is processed in the framework of a particular inquiry in accordance with the applicable law, that public authority or entity shall not be regarded as a recipient. Requests for disclosure from public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data protection rules according to the purposes of the processing.

Litt. f. – "processor"

24. "Processor" is any natural or legal person (other than an employee of the data controller) who processes data on behalf of the controller and according to the controller's instructions. The instructions given by the controller establish the limit of what the processor is allowed to do with the personal data.

Article 3 – Scope

25. According to *paragraph 1,* each Party should apply the Convention to all processing, whether within the public or private sector, subject to its jurisdiction.

26. Making the scope of the protection dependent on the notion of "jurisdiction" of the Parties, is justified by the objective of better standing the test of time and accommodating continual technological developments.

27. *Paragraph 2* excludes processing carried out for purely personal or household activities from the scope of the Convention. This exclusion aims at avoiding the imposition of unreasonable obligations on data processing carried out by individuals in their private sphere for activities relating to the exercise of their private life. Personal or household activities are activities which are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others. These activities have no professional or commercial aspects and relate exclusively to personal or household

activities such as storing family or private pictures on a computer, creating a list of the contact details of friends and family members, correspondence, etc. The sharing of data within the private sphere encompasses notably the sharing between a family, a restricted circle of friends or a circle which is limited in its size and based on a personal relationship or a particular relation of trust.

28. Whether activities are “purely personal or household activities” will depend on the circumstances. For example, when personal data is made available to a large number of persons or to persons obviously external to the private sphere, such as a public website on the internet, the exemption will not apply. Likewise, the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual in his or her family home for the purposes of protecting the property, health and life of the home owners, but which covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, cannot be regarded as an activity which is a purely “personal or household” activity.[7]

29. The Convention nonetheless applies to data processing carried out by providers of the means for processing personal data for such personal or household activities.

30. While the Convention concerns data processing relating to individuals, the Parties may extend the protection in their domestic law to data relating to legal persons in order to protect their legitimate interests. The Convention applies to living individuals: it is not meant to apply to personal data relating to deceased persons. However, this does not prevent Parties from extending the protection to deceased persons.

Chapter II – Basic principles of data protection

Article 4 – Duties of the Parties

31. As this article indicates, the Convention obliges Parties to incorporate its provisions into their law and secure their effective application in practice; how this is done depends on the applicable legal system and the approach taken regarding the incorporation of international treaties.

32. The term “law of the Parties” denotes, according to the legal and constitutional system of the particular country, all enforceable rules, whether of statute law or case law. It must meet the qualitative requirements of accessibility and previsibility (or “foreseeability”). This implies that the law should be sufficiently clear to allow individuals and other entities to regulate their own behaviour in light of the expected legal consequences of their actions, and that the persons who are likely to be affected by this law should have access to it. It encompasses rules that place obligations or confer rights on persons (whether natural or legal) or which govern the organisation, powers and responsibilities of public authorities or lay down procedure. In particular, it includes States' constitutions and all written acts of legislative authorities (laws in the formal sense) as well as all regulatory measures (decrees, regulations, orders and administrative directives) based on such laws. It also covers international conventions applicable in domestic law, including EU law. Furthermore, it includes all other statutes of a general nature, whether of public or private law (including the law of contracts), together with court decisions in common law countries, or in all countries, established case law interpreting a written law. In addition, it includes any act of a professional body under powers delegated by the legislator and in accordance with its independent rule-making powers.

33. Such a “law of the Parties” may be usefully reinforced by voluntary regulation measures in the field of data protection, such as codes of good practice or codes for professional conduct. However, such voluntary measures are not by themselves sufficient to ensure full compliance with the Convention.

34. Where international organisations are concerned,[8] in some situations, the law of such international organisations may be applied directly at the national level of the member States of such organisations depending on each national legal system.

35. The effectiveness of the application of the measures giving effect to the provisions of the Convention is of crucial importance. The role of the supervisory authority (or authorities), together with any remedies that are available to data subjects, should be considered in the overall assessment of the effectiveness of a Party's implementation of the Convention's provisions.

36. It is further stipulated in *paragraph 2* that the measures giving effect to the Convention shall be taken by the Parties concerned and shall have come into force by the time of ratification or accession, that is when a Party becomes legally bound by the Convention. This provision aims to enable the Convention Committee to verify whether all "necessary measures" have been taken, to ensure that the Parties to the Convention observe their commitments and provide the expected level of data protection in their national law. The process and criteria used for this verification are to be clearly defined in the Convention Committee's rules of procedure.

37. Parties commit in *paragraph 3* to contribute actively to the evaluation of their compliance with their commitments, with a view to ensuring regular assessment of the implementation of the principles of the Convention (including its effectiveness). Submission of reports by the Parties on the application of their data protection law could be one possible element of this active contribution.

38. In exercising its powers under paragraph 3, the Convention Committee shall not evaluate whether a Party has taken effective measures, to the extent it has made use of exceptions and restrictions in accordance with the provisions of this Convention. It follows that under Article 11 paragraph 3 a Party shall not be required to provide classified information to the Convention Committee.

39. The evaluation of a Party's compliance will be carried out by the Convention Committee on the basis of an objective, fair and transparent procedure established by the Convention Committee and fully described in its rules of procedure.

Article 5 – Legitimacy of data processing and quality of data

40. *Paragraph 1* provides that data processing must be proportionate, that is, appropriate in relation to the legitimate purpose pursued and having regard to the interests, rights and freedoms of the data subject or the public interest. Such data processing should not lead to a disproportionate interference with these interests, rights and freedoms. The principle of proportionality is to be respected at all stages of processing, including at the initial stage, i.e. when deciding whether or not to carry out the processing.

41. *Paragraph 2* prescribes two alternate essential pre-requisites for a lawful processing: the individual's consent or a legitimate basis prescribed by law. Paragraphs 1, 2, 3 and 4 of Article 5 are cumulative and must be respected in order to ensure the legitimacy of the data processing.

42. The data subject's consent must be freely given, specific, informed and unambiguous. Such consent must represent the free expression of an intentional choice, given either by a statement (which can be written, including by electronic means, or oral) or by a clear affirmative action and which clearly indicates in this specific context the acceptance of the proposed processing of personal data. Mere silence, inactivity or pre-validated forms or boxes should not, therefore, constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes (in the case of multiple purposes, consent should be given for each different purpose). There may be cases with different consent decisions (e.g. where the nature of the data is different even if the purpose is the same – such as health data versus location data: in such cases the data subject may consent to the processing of his or her location data but not to the processing of the health data). The data subject must be informed of the implications of his or her decision (what the fact of consenting entails and the extent to which consent is given). No

undue influence or pressure (which can be of an economic or other nature) whether direct or indirect, may be exercised on the data subject and consent should not be regarded as freely given where the data subject has no genuine or free choice or is unable to refuse or withdraw consent without prejudice.

43. In the context of scientific research it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

44. An expression of consent does not waive the need to respect the basic principles for the protection of personal data set out in Chapter II of the Convention and the proportionality of the processing, for instance, still has to be considered.

45. The data subject has the right to withdraw the consent he or she gave at any time (which is to be distinguished from the separate right to object to processing). This will not affect the lawfulness of the data processing that occurred before the data controller has received his or her withdrawal of consent but does not allow continued processing of data, unless justified by some other legitimate basis laid down by law.

46. The notion of “legitimate basis laid down by law”, referred to in *paragraph 2*, encompasses, *inter alia,* data processing necessary for the fulfilment of a contract (or pre-contractual measures at the request of the data subject) to which the data subject is party; data processing necessary for the protection of the vital interests of the data subject or of another person; data processing necessary for compliance with a legal obligation to which the controller is subject; and data processing carried out on the basis of grounds of public interest or for overriding legitimate interests of the controller or of a third party.

47. Data processing carried out on grounds of public interest should be provided for by law, *inter alia*, for monetary, budgetary and taxation matters, public health and social security, the prevention, investigation, detection and prosecution of criminal offences and the execution of criminal penalties, the protection of national security, defence, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, the enforcement of civil law claims and the protection of judicial independence and judicial proceedings. Data processing may serve both a ground of public interest and the vital interests of the data subject as, for instance, in the case of data processed for humanitarian purposes including monitoring a life-threatening epidemic and its spread or in humanitarian emergencies. The latter may occur in situations of natural disasters where processing of personal data of missing persons may be necessary for a limited time for purposes related to the emergency context – which is to be evaluated on a case-by-case basis. It can also occur in situations of armed conflicts or other violence.[9] The processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations can also be considered as being carried out on grounds of public interest.

48. The conditions for legitimate processing are set out in *paragraphs 3 and 4*. Personal data should be processed lawfully, fairly and in a transparent manner. Personal data must also have been collected for explicit, specified and legitimate purposes, and the processing of that particular data must serve those purposes, or at least not be incompatible with them. The reference to specified "purposes" indicates that it is not permitted to process data for undefined, imprecise or vague purposes. What is considered a legitimate purpose depends on the circumstances as the objective is to ensure that a balancing of all rights, freedoms and interests at stake is made in each instance; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society.

49. The concept of compatible use should not hamper the transparency, legal certainty, predictability or fairness of the processing. Personal data should not be further processed in a way that the data subject might consider unexpected, inappropriate or otherwise objectionable. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data is initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, *inter alia*, any link between those purposes and the purposes of the intended further processing; the context in which the personal data has been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to its further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

50. The further processing of personal data, referred to in *paragraph 4,b.* for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is *a priori* considered as compatible provided that other safeguards exist (such as, for instance, anonymisation of data or data pseudonymisation, except if retention of the identifiable form is necessary; rules of professional secrecy; provisions governing restricted access and communication of data for the above-mentioned purposes, notably in relation to statistics and public archives; and other technical and organisational data-security measures) and that the operations, in principle, exclude any use of the information obtained for decisions or measures concerning a particular individual. "Statistical purposes*"* refers to the elaboration of statistical surveys or the production of statistical, aggregated results. Statistics aim at analysing and characterising mass or collective phenomena in a considered population.[10] Statistical purposes can be pursued either by the public or the private sector. Processing of data for "scientific research purposes*"* aims at providing researchers with information contributing to an understanding of phenomena in varied scientific fields (epidemiology, psychology, economics, sociology, linguistics, political science, criminology, etc.) with a view to establishing permanent principles, laws of behaviour or patterns of causality which transcend all the individuals to whom they apply.[11] "Historical research purposes*"* includes genealogical research. "Archiving purposes in the public interest" can also include archives originating from private entities, where a public interest is involved.

51. Personal data undergoing processing should be adequate, relevant and not excessive. Furthermore, the data should be accurate and, where necessary, regularly kept up to date.

52. The requirement of *paragraph 4,c.* that data be "not excessive" first requires that data processing should be limited to what is necessary for the purpose for which it is processed. It should only be processed if, and as long as, the purposes cannot reasonably be fulfilled by processing information that does not involve personal data. Furthermore, this requirement not only refers to the quantity, but also to the quality of personal data. Personal data which is adequate and relevant but would entail a disproportionate interference in the fundamental rights and freedoms at stake should be considered as excessive and not be processed.

53. The requirement of *paragraph 4,e.* concerning the time-limits for the storage of personal data means that data should be deleted once the purpose for which it was processed has been achieved, or that it should only be kept in a form that prevents any direct or indirect identification of the data subject.

54. Limited exceptions to Article 5 paragraph 4 are permitted under the conditions specified in Article 11 paragraph 1.

Article 6 – Special categories of data

55. Processing of certain types of data, or processing of certain data for the sensitive information it reveals, may lead to encroachments on interests, rights and freedoms. This can for instance be the case where there is a potential risk of discrimination or injury to an individual's dignity or physical integrity, where the data subject's most intimate sphere, such as his or her sex life or sexual orientation, is being affected, or where processing of data could affect the presumption of innocence. It should only be permitted where appropriate safeguards, which

complement the other protective provisions of the Convention, are provided for by law. The requirement of appropriate safeguards, complementing the provisions of the Convention, does not exclude the possibility provided under Article 11 to allow exceptions and restrictions to the rights of data subjects granted under Article 9.

56. In order to prevent adverse effects for the data subject, processing of sensitive data for legitimate purposes needs to be accompanied by appropriate safeguards (which are adapted to the risks at stake and the interests, rights and freedoms to be protected), such as for instance, alone or cumulatively; the data subject's explicit consent; a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted; a professional secrecy obligation; measures following a risk analysis; a particular and qualified organisational or technical security measure (data encryption, for example).

57. Specific types of data processing may entail a particular risk for data subjects independently of the context of the processing. This is, for instance, the case with the processing of genetic data, which can be left by individuals and can reveal information on the health or filiation of the person, as well as of third parties. Genetic data are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained. Similar risks occur with the processing of data related to

criminal offences (which includes suspected offences), criminal convictions (based on criminal law and in the framework of criminal proceedings) and related security measures (involving deprivation of liberty for instance) which require the provision of appropriate safeguards for the rights and freedoms of data subjects.

58. Processing of biometric data, that is data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual, is also considered sensitive when it is precisely used to uniquely identify the data subject.

59. The context of the processing of images is relevant to the determination of the sensitive nature of the data. The processing of images will not generally involve processing of sensitive data as the images will only be covered by the definition of biometric data when being processed through a specific technical mean which permits the unique identification or authentication of an individual. Furthermore, where processing of images is intended to reveal racial, ethnic or health information (see the following point), such processing will be considered as processing of sensitive data. On the contrary, images processed by a video surveillance system solely for security reasons in a shopping area will not generally be considered as processing of sensitive data.

60. Processing of sensitive data has the potential to adversely affect data subjects' rights when it is processed for specific information it reveals. While the processing of family names can in many circumstances be void of any risk for individuals (e.g. common payroll purposes), such processing could in some cases involve sensitive data, for example when the purpose is to reveal the ethnic origin or religious beliefs of the individuals based on the linguistic origin of their names. Information concerning health includes information concerning the past, present and future, physical or mental health of an individual, and which may refer to a person who is sick or healthy. Processing images of persons with thick glasses, a broken leg, burnt skin or any other visible characteristics related to a person's health can only be considered as processing sensitive data when the processing is based on the health information that can be extracted from the pictures.

61. Where sensitive data has to be processed for a statistical purpose it should be collected in such a way that the data subject is not identifiable. Collection of sensitive data without identification data is a safeguard within the meaning of Article 6. Where there is a legitimate need to collect sensitive data for statistical purposes in identifiable form (so that a repeat or longitudinal survey can be carried out, for example), appropriate safeguards should be put in place.[12]

Article 7 – Data security

62. The controller and, where applicable the processor, should take specific security measures, both of technical and organisational nature, for each processing, taking into account: the potential adverse consequences for the individual, the nature of the personal data, the volume of personal data processed, the degree of vulnerability of the technical architecture used for the processing, the need to restrict access to the data, requirements concerning long-term storage, and so forth.

63. Security measures should take into account the current state of the art of data-security methods and techniques in the field of data processing. Their cost should be commensurate with the seriousness and probability of the potential risks. Security measures should be kept under review and updated where necessary.

64. While security measures are aimed at preventing a number of risks, *paragraph 2* contains a specific obligation in cases where a data breach has nevertheless occurred that may seriously interfere with the fundamental rights and freedoms of the individual. For instance, the disclosure of data covered by professional confidentiality, or which may result in financial, reputational, or physical harm or humiliation, could be deemed to constitute a “serious” interference.

65. Where such a data breach has occurred, the controller is required to notify the relevant supervisory authorities of the incident, subject to the exception permitted under Article 11 paragraph 1. This is the minimum requirement. The controller should also notify the supervisory authorities of any measures taken and/or proposed to address the breach and its potential consequences.

66. The notification made by the controller to the supervisory authorities does not preclude other complementary notifications. For instance, the controller may also recognise the need to notify the data subjects in particular when the data breach is likely to result in a significant risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, and to provide them with adequate and meaningful information on, notably, the contact points and possible measures that they could take to mitigate the adverse effects of the breach. In cases where the controller does not spontaneously inform the data subject of the data breach, the supervisory authority, having considered the likely adverse effects of the breach, should be allowed to require the controller to do so. Notification to other relevant authorities such as those in charge of computer systems security may also be desirable.

Article 8 – Transparency of processing

67. The controller is required to act transparently when processing data in order to ensure fair processing and to enable data subjects to understand and thus fully exercise their rights in the context of such data processing.

68. Certain essential information has to be compulsorily provided in a proactive manner by the controller to the data subjects when directly or indirectly (not through the data subject but through a third-party) collecting their data, subject to the possibility to provide for exceptions in line with Article 11 paragraph 1. Information on the name and address of the controller (or co-controllers), the legal basis and the purposes of the data processing, the categories of data processed and recipients, as well as the means of exercising the rights can be provided in any appropriate format (either through a website, technological tools on personal devices, etc.) as long as the information is fairly and effectively presented to the data subject. The information presented should be easily accessible, legible, understandable and adapted to the relevant data subjects (for example, in a child friendly language where necessary). Any additional information that is necessary to ensure fair data processing or that is useful for such purposes, such as the preservation period, the knowledge of the reasoning underlying the data processing, or information on data transfers to a recipient in another Party or non-Party (including whether that particular non-Party provides an appropriate level of data protection, or the measures taken by the controller to guarantee such an appropriate level of data protection) is also to be provided.

69. The controller is not required to provide this information where the data subject has already received it, or in the case of an indirect collection of data through third parties where the processing is expressly prescribed by law, or where this proves to be impossible or it involves disproportionate efforts because the data subject is not directly identifiable or the controller has no way to contact the data subject. Such impossibility can be both of a legal nature (in the context of a criminal investigation for instance) or of a practical nature (for instance when a controller is only processing pictures and does not know the names and contact details of the data subjects).

70. The data controller may use any available, reasonable and affordable means to inform data subjects collectively (through a website or public notice) or individually. If it is impossible to do so when commencing the processing, it can be done at a later stage, for instance when the controller is put in contact with the data subject for any new reason.

Article 9 – Rights of the data subject

71. This article lists the rights that every individual should be able to exercise concerning the processing of personal data relating to him or her. Each Party shall ensure, within its legal order, that all those rights are available for every data subject together with the necessary legal and practical, adequate and effective means to exercise them.

72. These rights include the following:

– the right of everyone not to be subject to a purely automated decision significantly affecting them without having their views taken into consideration (*littera* a.) ;

– the right of everyone to request confirmation of a processing of data relating to them and to access the data at reasonable intervals and without excessive delay or expense (*littera* b.);

– the right of everyone to be provided, on request, with knowledge of the reasoning underlying data processing where the results of such processing are applied to them (*littera* c.);

– the right of everyone to object on grounds relating to their situation, to a processing of personal data relating to them, unless the controller demonstrates legitimate grounds for the processing which override their interests or rights and fundamental freedoms (*littera* d.);

– the right of everyone to rectification or erasure of inaccurate, false, or unlawfully processed data (*littera* e.);

– the right of everyone to a remedy if any of the previous rights is not respected (*littera* f.);

– the right of everyone to obtain assistance from a supervisory authority (*littera* g.).

73. These rights may have to be reconciled with other rights and legitimate interests. They can, in accordance with Article 11, be limited only where this is provided for by law and constitutes a necessary and proportionate measure in a democratic society. For instance, the right to erasure of personal data may be restricted to the extent that processing is necessary for compliance with a legal obligation which requires processing by law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

74. While the Convention does not specify from whom a data subject may obtain confirmation, communication, rectification, and so on, or to whom to object or express his or her views, in most cases, this will be the controller, or the processor on his or her behalf. In exceptional cases, the means to exercise the rights to access, rectification and erasure may involve the intermediary of the supervisory authority. Concerning health data, rights may also be exercised in a different manner than through direct access. They may be exercised, for instance, with the assistance of a health professional when it is in the interest of the data subject, notably to help him/her understand the data or ensure that the data subject's psychological state is appropriately considered when imparting information – in line, of course, with deontological principles.

75. *Littera a.* It is essential that an individual who may be subject to a purely automated decision has the right to challenge such a decision by putting forward, in a meaningful manner, his or her point of view and arguments. In particular, the data subject should have the opportunity to substantiate the possible inaccuracy of the personal data

before it is used, the irrelevance of the profile to be applied to his or her particular situation, or other factors that will have an impact on the result of the automated decision. This is notably the case where individuals are stigmatised by application of algorithmic reasoning resulting in limitation of a right or refusal of a social benefit or where they see their credit capacity evaluated by a software only. However, an individual cannot exercise this right if the automated decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

76. *Littera b.* Data subjects should be entitled to know about the processing of their personal data. The right of access should, in principle, be free of charge. However, the wording of *littera b.* is intended to allow the controller in certain specific conditions to charge a reasonable fee where the requests are excessive and to cover various approaches that could be adopted by a Party for appropriate cases. Such a fee should be exceptional and in any case reasonable, and not prevent or dissuade data subjects from exercising their rights. The controller or processor could also refuse to respond to manifestly unfounded or excessive requests, in particular because of their repetitive character. The controller should in all cases justify such a refusal. To ensure a fair exercise of the right of access, the communication “in an intelligible form” applies to the content as well as to the form of a standardised digital communication.

77. *Littera c.* Data subjects should be entitled to know the reasoning underlying the processing of data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated-decision making including profiling. For instance in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a “yes” or “no” decision, and not simply information on the decision itself. Having an understanding of these elements contributes to the effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority.

78. *Littera d.* As regards the right to object, the controller may have a legitimate ground for data processing, which overrides the interests or rights and freedoms of the data subject. For example, the establishment, exercise or defence of legal claims or reasons of public safety could be considered as overriding legitimate grounds justifying the continuation of the processing. This will have to be demonstrated on a case-by-case basis and failure to demonstrate such compelling legitimate grounds while pursuing the

processing could be considered as unlawful. The right to object operates in a distinct and separate manner from the right to obtain rectification or erasure (*littera e.*).

79. Objection to data processing for marketing purposes should lead to unconditional erasing or removing of the personal data covered by the objection.

80. The right to object may be limited by virtue of a law, for example, for the purpose of the investigation or prosecution of criminal offences. In this case, the data subject can, as the case may be, challenge the lawfulness of the processing on which it is based. When data processing is based on valid consent given by the data subject, the right to withdraw consent can be exercised instead of the right to object. A data subject may withdraw his or her consent and subsequently have to assume the consequences possibly deriving from other legal texts such as the obligation to compensate the controller. Likewise where data processing is based on a contract, the data subject can take the necessary steps to revoke the contract.

81. *Littera e.* The rectification or erasure, if justified, must be free of charge. In the case of rectifications and erasures obtained in conformity with the principle set out in *littera e.*, those rectifications and erasures should, where possible, be brought to the attention of the recipients of the original information, unless this proves to be impossible or involves disproportionate efforts.

82. *Littera g.* aims at ensuring effective protection of data subjects by providing them the right to an assistance of a supervisory authority in exercising the rights provided by the Convention. When the data subject resides in the territory of another Party, he or she can submit the request through the intermediary of the authority designated by

that Party. The request for assistance should contain sufficient information to permit identification of the data processing in question. This right can be limited according to Article 11 or adapted in order to safeguard the interests of a pending judicial procedure.

83. Limited exceptions to Article 9 are permitted under the conditions specified in Article 11, paragraph 1.

Article 10 - Additional obligations

84. In order to ensure that the right to the protection of personal data is effective, additional obligations are imposed on the controller as well as, where applicable, the processor(s).

85. According to *paragraph 1*, the obligation on the controller to ensure adequate data protection is linked to the responsibility to verify and be in a position to demonstrate that data processing is in compliance with the applicable law. The data protection principles set out in the Convention, which are to be applied at all stages of processing, including the design phase, aim at protecting data subjects and are also a mechanism for enhancing their trust. Appropriate measures that the controller and processor may have to take to ensure compliance include: training employees; setting up appropriate notification procedures (for instance to indicate when data have to be deleted from the system); establishing specific contractual provisions where the processing is delegated in order to give effect to the Convention; as well as setting up internal procedures to enable the verification and demonstration of compliance.

86. If, in accordance with Article 11, paragraph 3, a Party choses to limit the powers of a supervisory authority within the meaning of Article 15 with reference to processing activities for national security and defence purposes, the controller has no obligation to demonstrate to such a supervisory authority compliance with data protection requirements for activities falling within the scope of the aforementioned exception.

87. A possible measure that could be taken by the controller to facilitate such a verification and demonstration of compliance would be the designation of a “data protection officer” entrusted with the means necessary to fulfil his or her mandate. Such a data protection officer, whose designation should be notified to the supervisory authority, could be internal or external to the controller.

88. *Paragraph 2* clarifies that before carrying out a data processing activity, the controller will have to examine its potential impact on the rights and fundamental freedoms of the data subjects. This examination can be done without excessive formalities. It will also have to consider respect for the proportionality principle on the basis of a comprehensive overview of the intended processing. In some circumstances, where a processor is involved in addition to the controller, the processor will also have to examine the risks.

IT systems developers, including security professionals, or designers, together with users and legal experts could assist in examining the risks.

89. *Paragraph 3* specifies that in order to better guarantee an effective level of protection, controllers, and, where applicable, processors, should ensure that data protection requirements are integrated as early as possible, that is, ideally at the stage of architecture and system design, in data processing operations through technical and organisational measures (data protection by design). This implementation of data protection requirements should be achieved not only as regards the technology used for processing the data, but also the related work and management processes. Easy-to-use functionalities that facilitate compliance with applicable law should be put in place. For example, secure online access to one’s own data should be offered to data subjects where possible and relevant. There should also be easy-to-use tools to enable data subjects to take their data to another provider of their choice or keep the data themselves (data portability tools). When setting up the technical requirements for default settings, controllers and processors should choose privacy-friendly standard configurations so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default), notably to avoid processing more data than necessary to achieve the legitimate purpose. For example, social networks should be configured by default so as to share posts or pictures only with restricted and chosen circles and not with the whole internet.

90. *Paragraph 4* allows Parties to adapt the additional obligations listed in paragraphs 1 to 3 taking into consideration the risks at stake for the interests, rights and fundamental freedoms of the data subjects. Such adaptation should be done considering the nature and volume of data processed, the nature, scope and purposes of the data processing and, in certain cases, the size of the processing entity. The obligations could be adapted, for example, so as not to entail excessive costs for small and medium-sized enterprises (SMEs) processing only non-sensitive personal data received from customers in the framework of commercial activities and not re-using it for other purposes. Certain categories of data processing, such as processing which does not entail any risk for data subjects, may even be exempt from some of the additional obligations prescribed in this article.

Article 11 – Exceptions and restrictions

91. No exceptions to the provisions of Chapter II are allowed except for a limited number of provisions (Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9) on condition that such exceptions are provided for by law, that they respect the essence of the fundamental rights and freedoms, and are necessary in a democratic society for the grounds listed in *litterae a.* and *b*. of the first paragraph of Article 11. A measure which is "necessary in a democratic society" must pursue a legitimate aim and thus meet a pressing social need which cannot be achieved by less intrusive means. Such a measure should, furthermore, be proportionate to the legitimate aim being pursued and the reasons adduced by the national authorities to justify it should be relevant and adequate. Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed.

92. All processing of personal data must be lawful, fair and transparent in relation to the data subjects, and only processed for specific purposes. This does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security and public safety, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the data subjects.

93. The necessity of such exceptions needs to be examined on a case-by-case basis and in light of the essential objectives of general public interest, as is detailed in *litterae* a. and b. of the first paragraph. *Littera* a. lists some objectives of general public interest of the State or of the international organisation which may require exceptions.

94. The notion of "national security" should be interpreted on the basis of the relevant case law of the European Court of Human Rights.[13]

95. The term "important economic and financial interests" covers, in particular, tax collection requirements and exchange control. The term "prevention, investigation and prosecution of criminal offences and the execution of criminal penalties" in this *littera* includes the prosecution of criminal offences and the application of sanctions related thereto. The term "other essential objectives of general public interest" covers *inter alia*, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions and the enforcement of civil law claims.

96. *Littera b*. concerns the rights and fundamental freedoms of private parties, such as those of the data subject himself or herself (for example when a data subject's vital interests are threatened because he or she is missing) or of third parties, such as freedom of expression, including freedom of journalistic, academic, artistic or literary expression, and the right to receive and impart information, confidentiality of correspondence and communications, or business or commercial secrecy and other legally protected secrets. This should apply in particular to processing of personal data in the audio-visual field and in news archives and press libraries. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

97. The *second paragraph* leaves open the possibility of restricting the provisions set out in Articles 8 and 9 with regard to certain data processing carried out for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes which pose no recognisable risk of infringement to the rights and fundamental freedoms of data subjects. For instance, this could be the case with the use of data for statistical work, in the public and private fields alike, in so far as this data is published in aggregate form and provided that appropriate data protection safeguards are in place (see paragraph 50).

98. The additional exceptions allowed to Article 4 paragraph 3, Article 14 paragraphs 5 and 6, and Article 15 paragraph 2, *litterae* a., b., c., and d., in respect of processing activities for national security and defence purposes are without prejudice to applicable requirements in relation to the independence and effectiveness of review and supervision mechanisms.[14]

Article 12 – Sanctions and remedies

99. In order for the Convention to guarantee an effective level of data protection, the duties of the controller and processor and the rights of data subjects should be reflected in the Parties' legislation with corresponding sanctions and remedies.

100. It is left to each Party to determine the nature (civil, administrative, criminal) of these judicial as well as non-judicial sanctions. These sanctions have to be effective, proportionate and dissuasive. The same goes for remedies: data subjects must have the possibility to judicially challenge a decision or practice, the definition of the modalities to do so being left with the Parties. Non-judicial remedies also have to be made available to data subjects. Financial compensation for material and non-material damages where applicable, caused by the processing and collective actions could also be considered.

Article 13 – Extended protection

101. This article is based on a similar provision, Article 60 of the European Convention on Human Rights. The Convention confirms the principles of data protection law which all Parties are ready to adopt. The text emphasises that these principles constitute only a basis on which Parties may build a more advanced system of protection. The expression "wider measure of protection" therefore refers to a standard of protection which is higher, not lower, than that already required by the Convention.

Chapter III – Transborder flows of personal data**[15]**

Article 14 – Transborder flows of personal data

102. The aim of this article is to facilitate the free flow of information regardless of frontiers (recalled in the preamble), while ensuring an appropriate protection of individuals with regard to the processing of personal data. A transborder data transfer occurs when personal data is disclosed or made available to a recipient subject to the jurisdiction of another State or international organisation.

103. The purpose of the transborder flow regime is to ensure that personal data originally processed within the jurisdiction of a Party (data collected or stored there, for instance), which is subsequently under the jurisdiction of a State which is not Party to the Convention, continues to be processed with appropriate safeguards. What is important is that data processed within the jurisdiction of a Party always remains protected by the relevant data protection principles of the Convention. While there may be a wide variety of systems of protection, protection afforded has to be of such quality as to ensure that human rights are not affected by globalisation and transborder data flows.

104. Article 14 applies only to the outflow of data, not to its inflow, since the latter are covered by the data protection regime of the recipient Party.

105. *Paragraph 1* applies to data flows between Parties to the Convention. Data flows cannot be prohibited or subjected to special authorisation "for the sole purpose of the protection of personal data". However, the Convention does not restrict the freedom of a Party to limit the transfer of personal data to another Party for other

purposes, including for instance national security, defence, public safety, or other important public interests (including protection of state secrecy).

106. The rationale of the provision in *paragraph 1* is that all Parties, having subscribed to the common core of data protection provisions set out in the Convention, are expected to offer a level of protection that is considered appropriate and therefore in principle allows data to circulate freely. There might, however, be exceptional cases where there is a real and serious risk that this free circulation of personal data will lead to the circumvention of the provisions of the Convention. As an exception, this provision has to be interpreted restrictively and Parties cannot rely on it in cases where the risk is either hypothetical or minor. Therefore, a Party may only invoke the exception in a specific case when it has clear and reliable evidence that transferring the data to another Party could significantly undermine the protections afforded to that data under the Convention, and that the likelihood of this happening is high. This might be the case, for instance, when certain protections afforded under the Convention are no longer guaranteed by the other Party (for instance because its supervisory authority is no longer able to effectively exercise its functions) or when data transferred to another Party is likely to be further transferred (onward transfer) without an appropriate level of protection being ensured. A further exception recognised in international law exists where Parties are bound by harmonised rules of protection shared by States belonging to regional (economic) organisations that seek a deeper level of integration.

107. Among others, this applies to the member States of the EU. However, as explicitly stated in the General Data Protection Regulation (EU) 2016/679, a third country's accession to Convention 108 and its implementation will be an important factor when applying the EU's international transfer regime, in particular when assessing whether the third country offers an adequate level of protection (which in turn allows the free flow of personal data).

108. *Paragraph 2* provides for an obligation to ensure, in principle, that “an appropriate level of protection based on the provisions of the Convention is secured”. At the same time, according to paragraph 4, Parties may transfer data even in the absence of an appropriate level of protection where this is justified, among others, by “prevailing legitimate interests, in particular important public interests” to the extent these are provided for by law and such transfers constitute a necessary and proportionate measure in a democratic society (*littera* c.). Personal data may thus be transferred on grounds that are similar to those listed in Article 11, paragraphs 1 and 3. In all cases, Parties remain free under the Convention to restrict data transfers to non-Parties, be it for the purpose of data protection or for other reasons.

109. *Paragraph 2* refers to transborder flows of personal data to a recipient that is not subject to the jurisdiction of a Party. As for any personal data flowing outside national frontiers, an appropriate level of protection is to be guaranteed. In cases where the recipient is not a Party to the Convention, the Convention establishes two mechanisms to ensure that the level of data protection is indeed appropriate; either by law, or by *ad hoc* or approved standardised safeguards that are legally binding and enforceable, as well as duly implemented.

110. *Paragraphs 2 and 3* apply to all forms of appropriate protection, whether provided by law or by standardised safeguards. The law must include the relevant elements of data protection as set out in this Convention. The level of protection should be assessed for each transfer or category of transfers. Various elements of the transfer should be examined such as: the type of data; the purposes and duration of processing for which the data are transferred; the respect of the rule of law by the country of final destination; the general and sectoral legal rules applicable in the State or organisation in question; and the professional and security rules which apply there.

111. The content of the *ad hoc* or standardised safeguards must include the relevant elements of data protection. Moreover, the contractual terms could be such, for example, that the data subject is provided with a contact person on the staff of the person responsible for the data transfers, whose responsibility it is to ensure compliance with the substantive standards of protection. The data subject would be free to contact this person at any time and at no cost in relation to the data processing or transfers and, where applicable, obtain assistance in exercising his or her rights.

112. The assessment as to whether the level of protection is appropriate must take into account the principles of the Convention, the extent to which they are met in the recipient State or organisation – in so far as they are relevant for the specific case of transfer – and how the data subject is able to defend his or her interests where there is non-compliance. The enforceability of data subjects' rights and the provision of effective administrative and judicial redress for the data subjects whose personal data are being transferred should be taken into consideration in the assessment. Similarly, the assessment can be made for a whole State or organisation thereby permitting all data transfers to such a destination.

113. *Paragraph 4* enables Parties to derogate from the principle of requiring an appropriate level of protection and to allow a transfer to a recipient which does not ensure such protection. Such derogations are permitted in limited situations only: with the data subject's consent or specific interest and/or where there are prevailing legitimate interests provided by law and/or the transfer constitutes a necessary and proportionate measure in a democratic society for freedom of expression. Such derogations should respect the principles of necessity and proportionality.

114. *Paragraph 5* makes provision for a complementary safeguard: namely that the competent supervisory authority be provided with all relevant information concerning the transfers of data referred to in paragraphs 3.b, and, upon request 4.b and 4.c. The authority should be entitled to request relevant information about the circumstances and justification of these transfers. Under the conditions laid down in Article 11, paragraph 3, exceptions to Article 14, paragraph 5 are permissible.

115. According to *paragraph 6,* the supervisory authority should be entitled to request that the effectiveness of the measures taken or the existence of prevailing legitimate interests be demonstrated, and to prohibit, suspend or impose conditions on the transfer if this proves necessary to protect the rights and fundamental freedoms of the data subjects. Under the conditions laid down in Article 11, paragraph 3 exceptions to Article 14, paragraph 6 are permissible.

116. Ever increasing data flows and the related need to increase the protection of personal data also require an increase in international enforcement co-operation among competent supervisory authorities.

Chapter IV – Supervisory authorities[16]

Article 15 – Supervisory authorities

117. This article aims at ensuring the effective protection of individuals by requiring the Parties to provide for one or more independent and impartial public supervisory authorities that contribute to the protection of the individuals' rights and freedoms with regard to the processing of their personal data. Such authorities may be a single commissioner or a collegiate body. In order for data protection supervisory authorities to be able to provide for an appropriate remedy, they need to have effective powers and functions and enjoy genuine independence in the fulfilment of their duties. They are an essential component of the data protection supervisory system in a democratic society**.** In so far as Article 11, paragraph 3, applies, other appropriate mechanisms for independent and effective review and supervision of processing activities for national security and defence purposes may be provided for by the Parties.

118. *Paragraph 1* clarifies that more than one authority might be needed to meet the particular circumstances of different legal systems (e.g. federal States). Specific supervisory authorities whose activity is limited to a specific sector (electronic communications sector, health sector, public sector, etc.) may also be put in place. This also

applies to the processing of personal data for journalistic purposes if it is necessary to reconcile the right to the protection of personal data with the right to freedom of expression. The supervisory authorities should have the necessary infrastructure and financial, technical and human resources (lawyers, IT specialists) to take prompt and effective action. The adequacy of resources should be kept under review. Article 11, paragraph 3 allows for exceptions to the powers of supervisory authorities with reference to processing activities for national security and defence purposes (where such exceptions apply, other paragraphs of this article may as a consequence not be applicable or relevant). This is however without prejudice to applicable requirements in relation to the independence and effectiveness of review and supervision mechanisms.[17]

119. Parties have a certain amount of discretion as to how to set up the authorities for enabling them to carry out their task. According to *paragraph 2*, however, they must have, subject to the possibility to provide for exceptions in line with Article 11, paragraph 3, at least the powers of investigation and intervention and the powers to issue decisions with respect to violations of the provisions of the Convention. The latter may involve the imposition of administrative sanctions, including fines. Where the legal system of the Party does not provide for administrative sanctions, paragraph 2 may be applied in such a manner that the sanction is proposed by the competent supervisory authority and imposed by the competent national courts. In any event, any sanctions imposed need to be effective, proportionate and dissuasive.

120. The authority shall be endowed with powers of investigation, subject to the possibility to provide for exceptions in line with Article 11, paragraph 3, such as the possibility to ask the controller and processor for information concerning the processing of personal data and to obtain it. By virtue of Article 15, such information should be made available, in particular, when the supervisory authority is approached by a data subject wishing to exercise the rights provided for in Article 9. The latter is subject to exceptions of Article 11, paragraph 1.

121. The supervisory authority's power of intervention, provided for in paragraph 1, may take various forms in the Parties' law. For example, the authority could be empowered to oblige the controller to rectify, delete or destroy inaccurate or illegally processed data on its own account or if the data subject is not able to exercise these rights personally. The power to take action against controllers who are unwilling to communicate the required information within a reasonable time would also be a particularly effective demonstration of the power of intervention. This power could also include the possibility to issue opinions prior to the implementation of data processing operations (where processing presents particular risks to the rights and fundamental freedoms, the supervisory authority should be consulted by controllers from the earliest stage of design of the processes), or to refer cases, where appropriate, to relevant competent authorities.

122. Moreover, according to *paragraph 4* every data subject should have the possibility to request the supervisory authority to investigate a claim concerning his or her rights and liberties in respect of personal data processing. This helps to guarantee the right to an appropriate remedy, in keeping with Articles 9 and 12. The necessary resources to fulfil this duty should be provided. According to their available resources, the supervisory authorities should be given the possibility to define priorities to deal with the requests and complaints lodged by data subjects.

123. The Parties should give the supervisory authority the power either to engage in legal proceedings or to bring any violations of data protection rules to the attention of the judicial authorities, subject to the possibility to provide for exceptions in line with Article 11 paragraph 3. This power derives from the power to carry out investigations, which may lead the authority to discover an infringement of an individual's right to protection. The Parties may fulfil the obligation to grant this power to the authority by enabling it to make decisions.

124. Where an administrative decision produces legal effects, every affected person has the right to have an effective judicial remedy in accordance with the applicable national law.

125. *Paragraph 2,e*. deals with the awareness raising role of the supervisory authorities. In this context, it seems particularly important that the supervisory authority proactively ensures the visibility of its activities, functions and powers. To this end, the supervisory authority must inform the public through periodical reports (see paragraph

131). It may also publish opinions, issue general recommendations concerning the correct implementation of data protection rules or use any other means of communication. Moreover, it must provide information to individuals and to data controllers and processors about their rights and obligations concerning data protection. While raising awareness on data protection issues, the authorities have to be attentive to specifically address children and vulnerable categories of persons through adapted ways and languages.

126. As provided for under *paragraph 3*, supervisory authorities are, in accordance with the applicable national law, entitled to give opinions on any legislative or administrative measures which provide for the processing of personal data. Only general measures are meant to be covered by this consultative power, not individual measures.

127. In addition to this consultation foreseen under paragraph 3, the authority could also be asked to give its opinion when other measures concerning personal data processing are in preparation, such as for instance codes of conduct or technical norms.

128. Article 15 does not prevent the allocation of other powers to the supervisory authorities.

129. *Paragraph 5* clarifies that supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions, including the composition of the authority; the method for appointing its members; the duration of exercise and conditions of cessation of their functions; the possibility for them to participate in relevant meetings without undue restrictions; the option to consult technical or other experts or to hold external consultations; the availability of sufficient resources to the authority; the possibility to hire its own staff; or the adoption of decisions without being subject to external interference, whether direct or indirect.

130. The prohibition on seeking or accepting instructions covers the performance of the duties as a supervisory authority. This does not prevent supervisory authorities from seeking specialised advice where it is deemed necessary as long as the supervisory authorities exercise their own independent judgment.

131. Transparency on the work and activities of the supervisory authorities is required under *paragraph 7* through, for instance, the publication of annual activity reports comprising *inter alia* information related to their enforcement actions.

132. Notwithstanding this independence, it must be possible to appeal against the decisions of the supervisory authorities through the courts in accordance with the principle of the rule of law, as provided for under *paragraph 9*.

133. Moreover, while supervisory authorities should have the legal capacity to act in court and seek enforcement, the intervention (or lack of) of a supervisory authority should not prevent an affected individual from seeking a judicial remedy (see paragraph 124).

134. *Paragraph 10* of Article 15 states that supervisory authorities shall not be competent with respect to processing carried out by independent bodies when acting in their judicial capacity. Such exemption from supervisory powers should be strictly limited to genuine judicial activities, in accordance with national law.

Chapter V – Co-operation and mutual assistance

Article 16 – Designation of supervisory authorities

135. Chapter V (Articles 16 to 21) forms a set of provisions on co-operation and mutual assistance between Parties, through their various authorities, in giving effect to the data protection laws implemented pursuant to the Convention. These provisions are obligatory except in cases referred to in Article 20. Under Article 16, the Parties shall designate one or more authorities and communicate their contact details, as well as their substantive and territorial competences, if applicable, to the Secretary General of the Council of Europe. Subsequent articles provide for a detailed framework for co-operation and mutual assistance.

136. While the co-operation between Parties will generally be carried out by the supervisory authorities established under Article 15, it cannot be excluded that a Party designates another authority to give effect to the provisions of Article 16.

137. The co-operation and general assistance is relevant for controls *a priori* as well as for controls a*posteriori* (for example to verify the activities of a specific data controller). The information exchanged may be of a legal or factual character.

Article 17 – Forms of co-operation

138. According to Article 17, supervisory authorities within the meaning of Article 15 shall co-operate with one another to the extent necessary for the performance of their duties and the exercise of their powers. Given that Article 17 circumscribes the co-operation of supervisory authorities to what is necessary "for the performance of their duties and exercise of their powers" and the fact that the ability of a supervisory authority to co-operate relies on the extent of its powers, the provision does not apply to the extent that a Party makes use of Article 11, paragraph 3, entailing a limitation of the powers of supervisory authorities pursuant to Article 15, paragraph 2, *litterae* a. to d.

139. Co-operation may take various forms, some “hard” forms, such as enforcement of data protection laws through mutual assistance, in which the legality of action of each supervisory authority is indispensable, to some “soft” forms, such as awareness-raising, training, staff exchange.

140. The catalogue of possible co-operation activities is not exhaustive. In the first place, supervisory authorities shall provide each other with mutual assistance, especially by sharing any relevant and useful information. This information could be of a two-fold nature: “information and documentation on their law and administrative practice relating to data protection” (which normally does not raise any issues, such information could be exchanged freely and made publicly available) as well as confidential information, including personal data.

141. As far as personal data is concerned, such data can be exchanged only if it is essential for the co-operation, that is, if without its provision the co-operation would be rendered ineffective, or if the “data subject concerned has given explicit, specific, free and informed consent”. In any case, the transfer of personal data must comply with the provisions of the Convention, and in particular Chapter II (see also Article 20 providing for the grounds for refusal).

142. Further to the provision of relevant and useful information, the goals of co-operation can be achieved by co-ordinated investigations or interventions as well as joint actions. For the applicable procedures, supervisory authorities shall refer to the applicable domestic legislation such as codes of administrative, civil or criminal procedure, or supra or international commitments by which their jurisdictions are bound, for example, mutual legal assistance treaties, having assessed their legal capacity to enter into a co-operation of that type.

143. *Paragraph 3* refers to a network of supervisory authorities, as a means to contribute to the rationalisation of the co-operation process and thus to the efficiency of the protection of personal data. It is important to note that the Convention refers to “a network” in singular form. This does not prohibit supervisory authorities originating from the Parties to take part in other relevant networks.

Article 18 – Assistance to data subjects

144. *Paragraph 1* ensures that data subjects, whether in a Party to the Convention or in a third country will be enabled to exercise their rights recognised in Article 9 regardless of their place of residence or their nationality.

145. According to *paragraph 2*, where the data subject resides in another Party he or she is given the option to pursue his or her rights either directly in the country where information relating to the data subject concerned is processed, or indirectly, through the intermediary of the designated authority.

146. Moreover, data subjects residing abroad may also have the opportunity to pursue their rights with the assistance of the diplomatic or consular agents of their own country.

147. *Paragraph 3* specifies that requests be as specific as possible in order to expedite the procedure.

Article 19 – Safeguards

148. This article ensures that supervisory authorities shall be bound by the same obligation to observe discretion and confidentiality towards data protection authorities of other Parties and data subjects residing abroad.

149. Assistance from a supervisory authority on behalf of a data subject may only be given in response to a request from this data subject. The authority must have received a mandate from the data subject and may not act autonomously in his or her name. This provision is of fundamental importance for mutual trust, on which mutual assistance is based.

Article 20 – Refusal of requests

150. This article states that Parties are bound to comply with requests for co-operation and mutual assistance. The grounds for refusal to comply are enumerated exhaustively.

151. The term "compliance" which is used in *littera* c. should be understood in the broader sense as covering not only the reply to the request, but also the action preceding it. For example, a requested authority might refuse action not only if transmission to the requesting authority of the information asked for might be harmful for the rights and fundamental freedoms of an individual, but also if the very fact of seeking the information might prejudice his or her rights and fundamental freedoms. Furthermore, a requested authority may be required by applicable national law to ensure that other public order interests are protected (e.g. ensuring the confidentiality of a police investigation). To this end a supervisory authority may be obliged to omit certain information or documents in its response to a request.

Article 21 – Costs and procedures

152. The provisions of this article are analogous to those found in other international instruments.

153. With a view to not burdening the Convention with a mass of implementing details, *paragraph 3* of this article provides that procedure, forms and language to be used can be agreed between the Parties concerned. The text of this paragraph does not require any formal procedures, but allows for administrative arrangements, which may even be confined to specific cases. Moreover, it is advisable that Parties leave to the competent supervisory authorities the power to conclude such arrangements. The forms of co-operation and assistance may also vary from case to case. It is obvious that the transmission of a request for access to sensitive medical information will have requirements which differ from routine inquiries about entries in a population record.

Chapter VI – Convention Committee

154. The purpose of Articles 22, 23 and 24 is to facilitate the effective application of the Convention and, where necessary, to perfect it. The Convention Committee constitutes another means of co-operation of the Parties in giving effect to the data protection laws implemented pursuant to the Convention.

155. A Convention Committee is composed of representatives of all Parties, from the national supervisory authorities or from the government.

156. The nature of the Convention Committee and the likely procedure followed could be similar to those set up under the terms of other conventions concluded in the framework of the Council of Europe.

157. Since the Convention addresses a constantly evolving subject, it can be expected that questions will arise both with regard to the practical application of the Convention (Article 23, *littera* a.) and with regard to its meaning (same article, *littera* d.).

158. The Rules of Procedure of the Convention Committee contain provisions regarding the right to vote of the Parties and the modalities of the exercise of this right, and are appended to the amending Protocol.

159. Any amendment to the Rules of Procedure is subject to a two-thirds majority, with the exception of amendments to the provisions on the right to vote and corresponding modalities, to which Article 25 of the Convention applies.

160. Upon accession, the EU shall make a statement clarifying the distribution of competences between the EU and its member States as regards the protection of personal data under the Convention. Subsequently, the EU will inform the Secretary General of any substantial modification in the distribution of competences.

161. According to Article 25, the Convention Committee is entitled to propose amendments to the Convention and examine other proposals for amendment formulated by a Party or the Committee of Ministers (Article 23 *litterae* b. and c).

162. In order to guarantee the implementation of the data protection principles set by the Convention, the Convention Committee will have a key role in assessing compliance with the Convention, either when preparing an assessment of the level of data protection provided by a candidate for accession (Article 23 *littera* e.) or when periodically reviewing the implementation of the Convention by the Parties (Article 23 *littera* h.). The Convention Committee will also have the power to assess the compliance of the data protection system of a State or international organisation with the Convention if the State or organisation requires the Committee to do so (Article 23 *littera* f.).

163. In providing such opinions on the level of compliance with the Convention, the Convention Committee will work on the basis of a fair, transparent and public procedure detailed in its Rules of Procedure.

164. Furthermore, the Convention Committee may approve models of standardised safeguards for data transfers (Article 23 *littera* g.).

165. Finally, the Convention Committee may help to solve difficulties arising between Parties (Article 23 *littera* i.). Where disputes are concerned, the Convention Committee will seek a settlement through negotiation or any other amicable means.

Chapter VII – Amendments

Article 25 – Amendments

166. The Committee of Ministers, which adopted the original text of this Convention, is also competent to approve any amendments.

167. In accordance with *paragraph 1*, the initiative for amendments may be taken by the Committee of Ministers itself, by the Convention Committee or by a Party (whether a member State of the Council of Europe or not).

168. Any proposal for amendment that has not originated with the Convention Committee should be submitted to it, in accordance with *paragraph 3*, for an opinion.

169. In principle, any amendment shall enter into force on the thirtieth day after all the Parties have informed the Secretary General of the Council of Europe of their acceptance thereof. However, the Committee of Ministers may unanimously decide in certain circumstances, after consulting the Convention Committee, that such amendments shall enter into force following the expiry of a three-year time lapse, unless a Party notifies the Secretary General of an objection. This procedure, the purpose of which is to speed up the entry into force of amendments while preserving the principle of the consent of all the Parties, is intended to apply to minor and technical amendments.

Chapter VIII – Final clauses

Article 26 – Entry into force

170. Since for the effectiveness of the Convention a wide geographic scope is considered essential, paragraph 2 sets at five the number of ratifications by member States of the Council of Europe necessary for the entry into force.

171. The Convention is open for signature by the European Union.[18]

Article 27 – Accession by non-member States and international organisations

172. The Convention, which was originally developed in close co-operation with the OECD and several non-European States, is open to any State around the globe complying with its provisions. The Convention Committee is entrusted with the task of assessing such compliance and preparing an opinion for the Committee of Ministers

relating to the level of data protection of the candidate for accession.

173. Considering the frontierless nature of data flows, accession by countries and international organisations from all over the world is sought. International organisations that can accede to the Convention are solely international organisations which are defined as organisations governed by public international law.

Article 28 – Territorial clause

174. The application of the Convention to remote territories under the jurisdiction of Parties or on whose behalf a Party can make undertakings is of practical importance in view of the use that is made of distant countries for data processing operations either for reasons of cost and manpower or in view of the utilisation of alternating night and daytime data processing capability.

Article 29 – Reservations

175. The rules contained in this Convention constitute the most basic and essential elements for effective data protection. For this reason, the Convention allows no reservations to its provisions, which are, moreover, reasonably flexible, having regard to the exceptions and restrictions permitted under certain articles.

Article 30 – Denunciation

176. Any Party is allowed to denounce the Convention at any time.

Article 31 – Notifications

177. These provisions are in conformity with the customary final clauses contained in other conventions of the Council of Europe.

---

[1] General Data Protection Regulation (EU) 2016/679("GDPR") and Data Protection Directive for Police and Criminal Justice Authorities (EU) 2016/680 ("Police Directive").

[2] Welcomed by the 31st International Conference of Data Protection and Privacy Commissioners, held in Madrid 4-6 November 2009.

[3] See in particular Recital 105 of the GDPR.

[4] See the Council of Europe Convention on Access to Official Documents (CETS No. 205).

[5] “the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8” - ECtHR *MS v. Sweden*, (Application No. 20837/92),1997, paragraph 41.

[6] See Council of Europe Commissioner on Human Rights, The rule of law on the Internet and in the wider digital world, Issue Paper, CommDH/IssuePaper(2014)1, 8 December 2014, p. 48, point 3.3 ’Everyone’ without discrimination.

[7] See Court of Justice of the EU, František Ryneš v. Úřad, 11 December 2014, C-212/13k.

[8] International organisations are defined as organisations governed by public international law.

[9] Where the four Geneva Conventions of 1949, the Additional Protocols thereto of 1977, and the Statutes of the International Red Cross and Red Crescent Movement apply.

[10] Recommendation No. R (97) 18 of the Committee of Ministers to member States, concerning the protection of personal data collected and processed for statistical purposes, Appendix, point 1, 30 September 1997.

[11] Explanatory Memorandum to Recommendation No. R (97) 18 of the Committee of Ministers to member States, concerning the protection of personal data collected and processed for statistical purposes, paragraphs 11 and 14.

[12] See Recommendation Rec No. (97)18 of the Committee of Ministers, op cit.

[13] The relevant case law includes in particular the protection of state security and constitutional democracy from, *inter alia,* espionage, terrorism, support for terrorism and separatism. Where national security is at stake, safeguards against unfettered power must be provided. Relevant decisions of the European Court of Human Rights can be found at the Court's website (hudoc.echr.coe.int).

[14] For Parties that are Council of Europe member States, such requirements have been developed by the case law of the European Court of Human Rights under Article 8 of the ECHR (see in particular ECtHR, *Roman Zakharov v. Russia* (Application No. 47143/06), 4 December 2015, paragraph 233; *Szabó and Vissy v. Hungary* (Application No. 37138/14), 12 January 2016, paragraphs 75 et seq.).

[15] From the entry into force of the Amending Protocol, the Additional Protocol regarding supervisory authorities and transborder flows (ETS No. 181) shall be considered an integral part of the Convention as amended.

[16] From the entry into force of the Amending Protocol, the Additional Protocol regarding supervisory authorities and transborder flows (ETS No. 181) shall be considered an integral part of the Convention as amended.

[17] See footnote 14.

[18] The amendments to the Convention approved by the Committee of Ministers on 15 June 1999 lose their purpose from the entry into force of the Protocol.

Related documents

128th Session of the Committee of Ministers (18 May 2018)
www.coe.int/.../128th-session-of-the-committee-of-ministers-18-may-...

CM(2018)2-final
128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018) - Ad hoc Committee on Data Protection (CAHDATA) – Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

DOCX | 18/05/2018 | English | CM-Public

128th Session of the Committee of Ministers (18 May 2018) - ... **11/01/2018**
www.coe.int/.../may-2018?p_p_id=101_INSTANCE_FJJuJash2rEF&p_p_l...

128th Session of the Committee of Ministers (18 May 2018) - ... **11/01/2018**
www.coe.int/.../128th-session-of-the-committee-of-ministers-18-may-...