

## **The modernised Convention 108: novelties in a nutshell**

With the modernisation of the 1981 Convention 108, its original principles have been reaffirmed, some have been strengthened and some new safeguards have been laid down: They had to be applied to the new realities of the on-line world while new practices had led to the recognition of new principles in the field. The principles of transparency, proportionality, accountability, data minimisation, privacy by design, etc. are now acknowledged as key elements of the protection mechanism and have been integrated in the modernised instrument.

The main novelties<sup>1</sup> of the modernised Convention can be presented as follows:

### **Object and purpose of the Convention (Article 1)**

Under article 1 the objective of the Convention is clearly underlined, namely to guarantee to every individuals within the jurisdiction of one of the Parties (regardless of their nationality or place of residence) the protection of their personal data when undergoing processing, thus contributing to respect for their rights and fundamental freedoms, and in particular their right to privacy.

Using this wording, the Convention highlights the fact that the processing of personal data may positively enable the exercise of other fundamental rights and freedoms, which can thus be facilitated by guaranteeing the right to data protection.

### **Definitions and scope of application (Articles 2 and 3)**

While essential notions such as the definition of personal data and the one of data subjects are not at all modified, other changes are proposed in the definitions: the concept of 'file' is abandoned. 'Controller of a data file' is replaced by 'data controller', in addition to which the terms 'processor' and 'recipient' are used.

The scope of application includes both automated and non-automated processing of personal data (manual processing where the data form part of a structure which makes it possible to search by data subject according to pre-determined criteria) which falls under the jurisdiction of a party to the Convention. The omnibus nature of the

---

<sup>1</sup> This document presents the novelties and does not repeat the provisions which already exist since the 1981 Convention and its 2001 additional Protocol. For a complete view of the modernised Convention, please read the consolidated version published on our website.

Convention is preserved and the scope naturally continues to cover the processing in the private and public sectors indistinctly, as this is one of the great strengths of the Convention.

On the other hand, the Convention no longer applies to data processing carried out by a natural person for the exercise of purely personal or household activities.

Furthermore, Parties are no longer provided with the possibility to make declarations aimed at exempting from the application of the Convention certain types of data processing (e.g. national security and defense purposes).

#### Duties of the parties (Article 4)

Each Party has to adopt in its domestic law the measures necessary to give effect to the provisions of the Convention.

Furthermore, each Party should demonstrate that such measures have actually been taken and are effective and accept that the Convention Committee may check that these requirements have been complied with. This evaluation process of the Parties ("follow-up mechanism") is necessary to guarantee that the level of protection established by the Convention is actually afforded by the Parties.

It is important to note that international organisations now have the possibility to accede to the Convention (Article 27), as does the European Union (Article 26).

#### Legitimacy of data processing and quality of data (Article 5)

Article 5 clarifies the application of the principle of proportionality to underline that it should apply throughout the entire processing, and in particular in respect of the means and methods used in the processing. It is furthermore reinforced by the principle of data minimisation.

A new provision is introduced to clearly lay down the legal basis of the processing: the consent (which to be valid has to satisfy several criteria) of the data subject or some other legitimate basis laid down by law (contract, vital interest of the data subject, legal obligation of the controller, etc.).

#### Sensitive data (Article 6)

The catalogue of sensitive data has been extended to include genetic and biometric data, as well as data processed for the information they reveal relating to trade-union membership or ethnic origin (those two latter categories are being added to the existing ban on the processing of personal data revealing racial origin, political opinions or religious or other beliefs, health or sexual life and personal data relating to offences, criminal proceedings and convictions).

### Data security (Article 7)

In terms of data security, the requirement to notify, without delay, any security breaches is introduced. This requirement is limited to cases which may seriously interfere with the rights and fundamental freedoms of data subjects, which should be notified, at least, to the supervisory authorities.

### Transparency of processing (Article 8)

Controllers will have the obligation to guarantee transparency of the data processing and will to that end have to provide a required set of information, in particular relating to their identity and usual place of residence or establishment, on the legal basis and the purposes of the processing, the data recipients and on the categories of personal data processed. They should furthermore provide any additional information necessary to ensure a fair and transparently processing. The Controller is exempted from providing such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

### Rights of the data subject (Article 9)

Data subjects are granted new rights so that they have greater control over their data in the digital age.

The modernised Convention extends the catalogue of information to be transmitted to data subjects when they exercise their right of access. Furthermore, data subjects are entitled to obtain knowledge of the reasoning underlying the data processing, the results of which are applied to her/him. This new right is particularly important in terms of profiling of individuals<sup>2</sup>.

It is to be associated with another novelty, namely the right not to be subject to a decision which affects the data subject which is based solely on an automated processing, without the data subject having her/his views taken into consideration.

Data subjects have a right to object at any time to their personal data being processed, unless the controller demonstrates compelling legitimate grounds for the processing which override their interests or rights and fundamental freedoms.

### Additional obligations (Article 10)

The modernised Convention imposes broader obligations on those processing data or having data processed on their behalf.

---

<sup>2</sup> On this subject see Recommendation (2010) 13 on the Protection of Individuals with regard to Automatic Processing of Personal Data in the context of profiling and its Explanatory memorandum.

Accountability becomes an integral part of the protective scheme, with an obligation for the controllers to be able to demonstrate compliance with the data protection rules.

Controllers should take all appropriate measures – including when the processing is outsourced – to ensure that the right to data protection is ensured (privacy by design, examination of the likely impact of the intended data processing on the rights and fundamental freedoms of data subjects (“privacy impact assessment”) and privacy by default).

#### Exceptions and Restrictions (Article 11)

The rights laid down in the Convention are not absolute and may be limited when this is prescribed by law and constitutes a necessary measure in a democratic society on the basis of specified and limited grounds. Among those limited grounds are now included “essential objectives of public interest” as well as a reference to the right to freedom of expression.

The list of provisions of the Convention that can be restricted has been slightly extended (see references to Articles 7.1 on security and 8.1 on transparency in Article 11.1) and a new paragraph of this Article specifically deals with processing activities for national security and defense purposes, for which the “monitoring” powers of the Committee as well as some missions of the supervisory authorities can be limited. The requirement that processing activities for national security and defense purposes be subject to an independent and effective review and supervision is clearly laid down.

It is important to recall once again that contrary to the previous provisions of Convention 108, Parties to the modernised Convention will no longer be able to exclude from the scope of application of the Convention certain types of processing.

#### Transborder flows of personal data (Article 14)

The aim of this provision is to facilitate, where applicable, the free flow of information regardless of frontiers, while ensuring an appropriate protection of individuals with regard to the processing of personal data.

The purpose of the transborder flow regime is to ensure that information originally processed within the jurisdiction of a Party always remains protected by appropriate data protection principles.

Data flows between Parties cannot be prohibited or subject to special authorisation as all of them, having subscribed to the common core of data protection provisions set out in the Convention, offer a level of protection considered appropriate. One exception exists: when there is a real and serious risk that such transfer would lead to circumventing the provisions of the Convention.

In the absence of harmonised rules of protection shared by States belonging to a regional international organisation and governing data flows (see for instance the data protection framework of the European Union), data flows between Parties should thus operate freely.

Regarding transborder flows of data to a recipient that is not subject to the jurisdiction of a Party, an appropriate level of protection in the recipient State or organisation is to be guaranteed. As this cannot be presumed since the recipient is not a Party, the Convention establishes two main means 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 (notably contractual clauses or binding corporate rules) , as well as duly implemented.

#### Supervisory authorities (Article 15)

Building on Article 1 of the additional protocol, the modernised Convention complements the catalogue of the authorities' powers with a provision that, in addition to their powers to intervene, investigate, engage in legal proceedings or bring to the attention of the judicial authorities violations of data protection provisions, the authorities also have a duty to raise awareness, provide information and educate all players involved (data subjects, controllers, processors etc.). It also allows the authorities to take decisions and impose sanctions. Furthermore, it is recalled that the supervisory authorities should be independent in exercising these tasks and powers.

#### Forms of co-operation (Article 17)

The modernised Convention also addresses the issue of co-operation (and mutual assistance) between the supervisory authorities.

The supervisory authorities have to co-ordinate their investigations, to conduct joint actions and to provide to each other information and documentation on their law and administrative practices relating to data protection.

The information exchanged between the supervisory authorities will include personal data only where such data are essential for co-operation or where the data subject has given the specific, free and informed consent.

Finally the Convention provides a forum for increased co-operation : the supervisory authorities of the Parties have to form a network in order to organise their co-operation and to perform their duties as specified by the Convention.

### Convention Committee (Articles 22, 23 and 24)

The Convention Committee plays a crucial role in interpreting the Convention, encouraging the exchange of information between the Parties and developing data protection standards.

The role and powers of this Committee is strengthened with the Modernised Convention. It no longer is limited to a “consultative” role but also has assessment and monitoring powers. It will provide an opinion on the level of data protection provided by a state or international organisation before accession to the Convention. The committee is also able to assess the compliance of the domestic law of the Party concerned and determine the effectiveness of the measures taken (existence of a supervisory authority, responsibilities, existence of effective legal remedies).

It is also able to assess whether the legal norms governing the data transfers provide sufficient guarantee of an appropriate level of data protection.