COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

7 May 2021 T-PD(2020)06rev3

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

CONVENTION 108

INTERPRETATION OF PROVISIONS[1]

Directorate General of Human Rights and Rule of Law

[1] The present opinion of the Committee of Convention 108 contains guidance aimed at facilitating ratification of the amending protocol to the Convention

The present document aims at responding to the request made by one delegation during the 39th Plenary meeting (19-21 November 2019) of the Committee of Convention 108, as complemented by an additional request during the 50th Bureau meeting of the Committee (28-30 September 2020).

See paragraphs

- 2.16 of the Abridged report of the 39th Plenary meeting: interpretation of the terms 'arithmetical operations' (Article 2, definition of the 'data processing'), the distinction between the legal status of the 'controller' and 'recipient', and in relation to an 'identified or identifiable individual', guidance with regard to anonymisation and pseudonymisation", and

- 2.14 of the Abridged report of the 50th Bureau meeting: clarification on the notions of 'disclosure' and of transborder data flows.

The interpretation of concepts is of a guiding nature and is designed to assist state Parties to Convention 108 in ratifying the Protocol amending Convention 108.

1) "arithmetical operations" (Article 2.b of Convention 108+)

"data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or **arithmetical operations** on such data.

(a similar wording is to be found in Convention 108)

The terms 'arithmetic and / or logic' refer to one of the basic components of a computer processor which is called the Arithmetic-Logic Unit (ALU).

An ALU is a combinational digital circuit that performs arithmetic and bitwise operations on integer binary numbers. It is a fundamental building block of many types of computing circuits, including the central processing unit (CPU) of computers.

The arithmetical operations would in that case be the data inputs, to be operated on, with the result of the performed operation being the output.

2) Distinction between the legal status of "controller" and "recipient"

Definitions of Controller and Recipient in Convention 108+ are as follows:

d. "controller" means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;

e. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available.

According to paragraph 22 of the Explanatory Report of Convention 108+,: "*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*".

Paragraph 24 of the Explanatory Report of Convention 108+ provides that "*The "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*."

Paragraph 23 of the Explanatory Report of Convention 108+ stipulates that "*The "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.*"

The term "recipient" is thus used to refer to "controllers" or "processors" as the case may be, to whom personal data is disclosed or made available, without any specification to their relation or legal status in the chain of the processing (i.e. as a controller or processor). As such, the person or legal entity it refers to can be either a "controller" or "processor" based on their respective data processing operations. Therefore the term "recipient" cannot be regarded as a legal status (underpinned by rights and obligations) but as a term which describes a situation where an additional layer in the relationship of the data subject and the controllers and processors are added by the operation(s) of the initial controller.

It is to be noted nevertheless that in relation to article 8.1.d of Convention 108+ the controller has to inform data subjects – among others – on the recipients or categories of recipients of the personal data. Additionally, according to article 14.2 of Convention 108+ a State Party shall ensure that "an appropriate level of protection based on the provisions of this Convention is secured" by and in relation to all recipients in a country or international organisation which is not Party to the amending Protocol CETS223 irrespective of their legal status and relationship (i.e. controller of processor, or other status) afforded to them by their national legislation.

Concrete examples: Controller / [Processor] / Recipient

- A university is hired by the government to develop research on the economic development of the population. All personal data will be provided by the government which will also determine the purposes and main means of the processing. Even though the university has the academic autonomy therefore a certain margin of manoeuvre to define how the research will be done in terms of methodology, the university will not collect any personal data, the research will be done through the database provided by the government.

  - ➢ In this case, the university is the processor and the government the controller.

- To improve the safety of its students, a school plans to hire a security company to be responsible for entering the school. The company will provide cameras and electronic badges to the students.

  The collection of the personal data is done by the school, and the school shares with the security company the personal data necessary to allow students to enter.
  At no time does the company define what data will be collected, it only receives the necessary data from the school to allow students to enter.

  - ➢ The school is the controller and the company is the processor.

- An international organisation defending human rights is planning to do a mission in a refugee camp . It is necessary to collect various types of personal data to understand the refugee scenario and to provide to the refugees medicines, food, clothes, etc.

  For this mission, the international organisation decides to hire a company to store the data and another company to help with the analysis of the data and to provide statistics about the type and quantity of medicines needed for all refugees.

  - ➢ The international organisation is the controller and the other two companies the processors.

- A private firm agent is carrying out a regular passport and other personal data assessment process to see if it is possible for a person to enter a country.

  The agent needs to share this information with a government system to verify that the person is not a criminal or someone who is not allowed to leave the country for security reasons.

  - ➢ The government in this case is the recipient acting as a separate controller and the agent the processor on behalf of the entity that contracted the agent's services.

- Company Alpha is subject to fiscal obligations and is sharing payroll data with public authorities for tax purposes.

  The public authority in this case is a recipient (and as a separate controller for its own processing after receiving the data) and the company is a controller.

- A cloud service is provided by a company for the processing of human resources related personal data of another company. The company providing the cloud services needs to inform the requesting company on all its partners it will transfer data to in the framework of the performance of the cloud servicing contract.

- The company requesting the cloud services is the data controller, the company providing cloud services is the processor whereas its business partners are recipients.

3) “identified or identifiable individual” - guidance or collection of best practices on the process of anonymisation, pseudonymisation

Paragraph 18 of the Explanatory Report to Convention 108+ reads as follows “*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*.”

Paragraph 19 the Explanatory Report to Convention 108+ provides that “*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*.”

Paragraph 19 the Explanatory Report to Convention 108+ sets forth that “*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 no longer, identifiable. They should be regularly re-evaluated in light of the fast pace of technological development*”.

It follows from the above that anonymisation of personal data could be not only reached through a process which would result in an impossibility of the reidentification of the data subject but also if the process would lead to data through which the reidentification of an individual would require “*unreasonable time, effort or resources, taking into consideration the available technology at the time of the processing and technological developments”*. As technology changes fast and circumstances and the context can vary considerably it seems not to be advisable to describe in concrete terms and numbers what should constitute an “*unreasonable time, effort or resources”,* nor to give any examples for such a situation. Departing from the principle that a data controller is responsible and accountable for the data processing it carries out with personal data it would amount to its responsibility to categorise personal data and non-personal (i.e. anonymised) before initiating the processing. In case of doubt, as it could be of fundamental importance, the supervisory authority could advise whether or not a data, data set, is conveniently anonymised . It would do so however without any prejudice to the responsibility of the controller if the data, data set in question could be used to identify individuals again (by a new technology, technique, a joint controller, etc.)

In an effort of harmonising practices in anonymisation procedures the national data protection supervisory authorities are encouraged to issue guidelines and recommendations[2].

4) Disclosure

References to a disclosure in Convention 108+ are the following:

In article 2b: “data processing” means any operation or set of operations performed on personal data, such as (…) **disclosure** (…)

In article 2 e: “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are **disclosed** or made available

In article 7.1: “Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or **disclosure** of personal data.”

Furthermore, the Explanatory Report of Convention 108+ also refers to disclosure in the following paragraphs:

paragraph 23: “…**disclosure** from public authorities…”
paragraph 64: “…the **disclosure** of data covered by professional confidentiality,…”
paragraph 102: “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.”

On the basis of the above, “disclosure” is meant to be a data processing operation performed by the data controller, making the personal data known to the general public or to a recipient.

The other signification of this term involves actions performed by the controller such as sending, revealing or granting access to personal data. In this sense, paragraph 23 of the Explanatory Report gives the example of a “request for disclosure” by a public authority which refers to an official access request made by a public authority to a data held in a private database.

[2] For more information on anonymisation and pseudonymisation, see:
Opinion 05/2014 on Anonymisation Techniques by Article 29 Data Protection Working Party: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

European Data Protection Supervisor (EDPS) and Agencia española de protección de datos (AEPD) joint paper : “Introduction to the hash function as a personal data pseudonymisation technique” regarding anonymisation: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en

Guidance on Anonymisation and Pseudonymisation by Ireland DPA from June 2019: https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation

Anonymisation: managing data protection risk code of practice by the ICO: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwipk7GSrK_sAhXLDuwKHb4wDUUQFjAAegQIAhAC&url=https%3A%2F%2Fico.org.uk%2Fmedia%2F1061%2Fanonymisation-code.pdf&usg=AOvVaw3e_7fB2B38Tfpyx66OXh9s

Guidance by the Uruguayan DPA (in Spanish): https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-criterios-disociacion-datos-personales/guia-criterios-disociacion

In general, its use as a separate definition will depend on the logic of the national legislation. In this, possible constitutional requirements that personal data can only be disclosed if provided for by law needs to be taken into account (e.g. public authorities cannot disclose personal data in a given situation without being authorised by law. In such situations, the law will stipulate all recipients and purposes for such a disclosure.).

Paragraph 23 recalls that disclosure should respect applicable data protection rules, notably in relation to the form of the request, proportionality, necessity and purpose limitation.

5) <u>Transborder data flows</u>

Article 14 of Convention 108+ reads:

1. Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation.

2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured."

Explanatory Report

"*102. (…) 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. (…)

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."

Article 14 of Convention 108+ which provides for transborder flow regime applies when personal data is transferred out of the jurisdiction of a Party (to another Party, be it a State or an International Organisation, or to a State or International Organisation which is not Party to the Convention). Whilst all personal data "subject to the jurisdiction" of a Party (Article 3) should be afforded the protections under Convention 108+, it should be noted that Article 14 applies specifically to data exports rather than imports.

Regarding this notion of “jurisdiction”, the legal opinion provided by the Legal Advisor (DLAPIL02/2021_JP/DG[3], “Legal Opinion”) can be of relevance.

In light of the applicability of Convention 108+ and in particular of both articles 3 and 14, the term jurisdiction, in addition to the rule of territoriality, should be interpreted as *encompassing “all situations in which a party has the lawful power to effectively legislate and enforce rules relating to the processing of personal data*” in line with paragraph 35 of the Legal Opinion. In doing so Parties may consider at the time of legislation and when implementing Convention 108+ the cooperation of supervisory authorities as described in article 17 providing a unique tool for the collective enforcement of rights protected under Convention 108+ and for the facilitation of free flow of data between Parties.

[3] https://rm.coe.int/legal-opinion-dlapil02-2021-the-interpretation-of-the-notion-of-jurisd/1680a19c58