
Strasbourg, 19 June 2025 T-PD(2021)7rev13

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

**Convention 108**

# Guidelines on the general principles of Article 11 of the Modernised Convention 108

www.coe.int/dataprotection

## 1. Introduction

The European Convention on Human Rights (ECHR), entered into force on 3 September 1953, enshrines that: "*Everyone has the right to respect for his private and family life, his home and his correspondence*" and sets out the conditions for restricting those rights, notably in Article 8.2 when it provides that: "*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*." These principle-based conditions were substantiated primarily by the European Court of Human Rights (ECtHR) through its abundant case-law on Article 8 and by other organs and institutions of the Council of Europe, such as the Venice Commission. These confirmed the right to privacy in the jurisdictions concerned, as an individual, universal human right that is inalienable and imprescriptible. Such developments can also be observed through the case-law of the Inter-American Court of Human Rights[1].

On the Council of Europe side, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), was opened for signature on 28 January 1981 in Strasbourg. The objective of this convention was to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them[2].

When it comes to exceptions, Article 9 of Convention 108 already contained specific provisions for the lawful use of exceptions under the Convention in line with Article 8.2 of the ECHR and the evolution of the case-law[3].

An important development started in 2011 in this area, namely: the modernisation process of the Convention for the protection of individuals with regard to the processing of personal data (ETS No 108, "Convention 108"), which has had at least three objectives: a) to secure the human dignity of individuals in the digital age by ensuring an appropriate protection of their privacy, and other human rights, notably through the protection of their personal data; b) to facilitate transborder flow of personal data and c) to establish a common regime for the use of exception from data protection principles and rules for its Parties. By doing so the Protocol CETS No 223 amending Convention 108 (referred in this document as "the Convention", "Convention 108+") in the form of international public law was to provide a legal base for the basic requirements of Article 8.2 of the ECHR in a more modern and concrete form, thus involving indirectly the evolving jurisprudence on that provision.

[1] Case of Tristan Donoso v Panama, case of Nadega Dorzema et al. v. Dominican Republic, case of Garcia Rodrigez et al. v. Mexico.

[2] The Explanatory Report specifies that as it was largely agreed at the time that such legal rules were needed in view of the increasing use made of computers for administrative purposes with a vastly superior storage capability and possibilities for a much wider variety of transactions, which they can perform at high speed. On the other hand, it was agreed in the 70s' that "Information power" should bring a corresponding social responsibility of the data users in the private and public sector. It was also deemed essential that those responsible for these files should make sure that the undeniable advantages they can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored.

[3] It stated that: "*Exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of Article 9 has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention*."

Historically, during further evolution in the case-law of the ECtHR another important aspect was emerging: states not only have a negative obligation not to interfere with human rights and fundamental freedoms, but a positive obligation to guarantee them and that they can be exercised at their fullest[4] which is again an important element to consider while transposing general principles on the use of exceptions.

Parties that have already ratified the Protocol CETS No 223 or are in the middle of the process may have faced difficulties in transposing those elements into their national legal framework, which very often implied the amendments of legislative instruments in other areas as well. Conscious of these difficulties at national level and ambitious to provide a harmonised interpretation which could also contribute to a quick entry into force and further accessions to Convention 108+, but also to establish a good basis for further, more specific guidance, the Committee of Convention 108 pursuant to Article 19 of Convention 108 and in line with the Article 23 of Convention 108+ decided to issue guidelines on the possible transposition, implementation of the general principles laid down in Article 11.1 taking into account the already existing best practices of the Parties[5].

## 2. Purpose and scope of the Guidelines

- Purpose of the document

These Guidelines are of an interpretative nature and do not create new rights or obligations. They aim to help and support the ratification of the Protocol CETS No. 223 amending the Convention ETS No. 108 for the protection of individuals with regard to the processing of personal data ("Convention 108+") as provided by Article 37 of the amending Protocol. The Guidelines can also help future Parties to interpret and eventually transpose the general principles laid down in Article 11.1 into the domestic legislation during an accession process to Convention 108+ as set out in Article 33. Furthermore, they could provide a model for any future guidance required by other provisions of this Convention.

These Guidelines provide a general explanation of principles and rules contained in Article 11.1 of Convention 108+, when possible, by giving examples in an abstract manner to contribute to a more harmonised interpretation and implementation of the provisions of Convention 108+. By doing so they aim to aid the application of this Convention and increase trust and confidence among Parties.

- Scope

The current version of Convention 108 allows, by unilateral declaration addressed to the Secretary General of the Council of Europe for the possibility of excluding specific files or processing activities from the scope of its application. Article 3 of Convention 108+ brought

[4] KU v Finland; Soderman v Sweden; A and B v Croatia; X and others v Bulgaria; Silva Monteiro Martins Ribeiro v Portugal; etc.

[5] The Guidelines rely on principles which reflect the case-law at international, regional and national levels, notably by the European Court of Human Rights, the Inter-American Court of Human Rights and African Court on Human and Peoples' Rights.

an important change to this area. Upon the entry into force of Convention 108+ the possibility of removing specific areas, sectors (such as national security, defence, law enforcement, etc.) from the application of data protection principles and rules by unilateral declaration by Parties will no longer be possible. Instead limited restrictions from the provisions of Convention 108+ are possible.

Therefore the scope of these Guidelines follows the broad scope of Convention 108+ which applies to the processing of personal data both in the public and private sectors. No exceptions or derogations can be made to its scope of application by Parties unilaterally; the conditions for the use of exceptions are regulated in Article 11.

There are other important changes too: Article 11.1 of Convention 108+ while following Article 9 of Convention 108 logic and construction contains more conditions for the legitimacy of the use of specific exceptions. At the same time it allows for broad range of other essential objectives of general public interest related exceptions with regard to the legitimate purpose of data processing. It is worth noting that it also contains a very specific regime allowing for wider exceptions in case of data processing for national security and defence purposes. However, when that is applied, a new provision in Article 11.3 requires Parties to ensure an "*independent and effective review and supervision under the domestic legislation*".

The list of conditions is complemented by the criterion "*respects the essence of the fundamental rights and freedoms*" which is applicable to all processing subject to an exception. Its modalities are further explained in this document.

In conclusion, Article 11 sets out, compared to Article 3 and 9 of Convention 108, concrete conditions for the legislator to transpose into the domestic legal framework which would only allow data controllers to use exceptions from a specific provision of the Convention for a list of legitimate purposes.

It should be noted that any possible exceptions provided for in Article 11 should be linked to a specific data processing and meet the requirements of Article 11.1. This implies that a weighing of the interests involved between the need to provide for exceptions to certain provisions of the Convention and respect for the human rights and fundamental freedoms of individuals must be carried out and justified for which these Guidelines aim to provide support and some simple methodology.

In this respect one should firstly observe that Article 1 of Convention 108+ states that individuals are to be protected when their personal data is processed, regardless their nationality or residence which may have some bearings with the transposition of those provisions. The logic behind is that the protection of private life is a universal human right recognised in Article 8 of the European Convention on Human Rights and other international human rights instruments[6], as well as in the constitutions of most of the Parties to the Convention. Therefore the Guidelines will concentrate on general principles of data protection but will, when applicable, raise the awareness of the Parties on the impact of the

[6] Such as Article 12 of the Universal Declaration of Human Rights (UNDHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 11.2 of the American Convention on Human Rights (ACHR), Article 4 of the African Charter on Human and People's Rights (ACHPR), Article 7 and 8 of the Charter of Fundamental Rights of the European Union

processing of personal data on the right to privacy and other human rights and fundamental freedoms.

For the scope of these Guidelines the definitions contained in Article 2 of Convention 108+ are of particular relevance and should be referred to.

3. Structure of Article 11

Article 11 sets the limits for any possible exceptions from specific provisions of the Convention. Within the scope of the Convention, other provisions remain applicable in case one of the exceptions of Article 11 is used.

Article 11 establishes three regimes of exceptions depending on the purpose of the processing that are subject to some objective conditions and that contain respectively a list of provisions of the Convention that can be affected by exceptions and restrictions.

- The three regimes of exceptions

The regimes below are described based to the extent to which they allow exceptions to the provisions of the Convention for the three main categories of legitimate purposes: General public interest, archiving, research and statistics and national security and defense:

1) General public interest exceptions:
    a. Legitimate purposes for which they can be used:
        i. The protection of national security, defense, public safety, important economic and financial interests of the state, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;
        ii. The protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

    b. General conditions for the use of exception:
        i. Provided for by law;
        ii. Respects the essence of the fundamental rights and freedoms;
        iii. Constitutes a necessary and proportionate measure in a democratic society.

    c. Provisions that can be made subject to a restriction or derogation:
        i. General principles such as fairness, transparency, purpose limitation, data quality requirements: adequate, relevant, not excessive, accurate, up to date, permits only identification no longer than necessary (Article 5, paragraph 4);
        ii. Data breach notification to the supervisory authority (Article 7, paragraph 2);
        iii. Data controllers' obligation to inform the data subject (Article 8, paragraph 1);

iv. Data subject's rights (Article 9).

2) Archiving, research and statistics exceptions:
   a. Legitimate purposes for which they can be used:
      i. Archiving purposes in the public interest;
      ii. Scientific or historical research purposes;
      iii. Statistical purposes.
   b. General conditions for the use of exception:
      i. Provided for by law;
      ii. When there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.
   c. Provisions that can be made subject to a restriction or derogation:
      i. Data controller's obligation to inform the data subject (Article 8);
      ii. Data subject's rights (Article 9).

3) National security and defense additional exceptions:
   a. Legitimate purposes for which they can be used:
      i. National security;
      ii. Defense.
   b. Additional conditions for the use of exception:
      i. provided for by law;
      ii. to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfil the aim.
   c. Provisions that can be made subject to a restriction or derogation
      i. Conventional Committee's competence to evaluate the effectiveness of the measures taken to give effect to the provisions of the Convention (Article 4, paragraph 3);
      ii. To provide information to the supervisory authority on international transfer (Article 14, paragraphs 5);
      iii. To require by the supervisory authority to demonstrate the lawful conditions for international transfer and its ability to intervene (Article 14, paragraphs 6);
      iv. Supervisory authority's power to investigate and intervene, functions relating to international transfer, power on taking regulatory decisions and sanctions, to turn to the judiciary (Article 15, paragraph 2, litterae a, b, c and d).

The following provisions are applicable under any exception regime:

- Article 4 (paragraph 1) and (paragraph 2): Parties shall take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application.

- Article 5 (paragraph 1) to (paragraph 3): No exception is applicable for the proportionality, legitimacy of the processing, and the legitimacy of the purpose of the processing principles. That implies that the proportionality of the data processing has to be ensured, as well as the requirements to process personal data on a valid legal basis and for a legitimate purpose.

- Article (paragraph 6): Special categories of data enjoy special protection which requires safeguards complementing those already in place for the processing activities. Those have to guard against the risks of infringing data subjects' interests, rights and fundamental freedoms, notably from the risk of discrimination.

- Article 7 (paragraph 1): Data security: The obligation to take measures to ensure data security applies without any exception;

- Article 10: Accountability measures are to be foreseen: Obligation of data controllers to demonstrate that appropriate measures have been taken to comply with the provisions of the Convention as well as to examine the likely impact of intended data processing and to apply the privacy-by-design approach as well as other recommended measures to mitigate the risk(s) of unlawful interference still needs to be ensured in the domestic legal framework;

- Article 12: No exception to the applicability of judicial and non-judicial sanctions as well as to remedies to be made available for the violation of the provisions of the Convention;

- Article 13: Wider protection for data subject can be afforded by a Party;

- Article 14 (paragraph 1) to (paragraph 4): Transborder data transfers rules apply;

- Article 15 (paragraph 2, litterae (e) to paragraph (10): i) awareness raising activity by the supervisory authority, ii) to be consulted on legislative/administrative measures, iii) to deal with the request and complaints lodged by the data subject, shall keep them informed, iv) shall act in complete independence and impartiality, v) shall have sufficient resources, vi) shall prepare annual report, vii) confidentiality obligations for members of staff, viii) decisions to be appealed, reviewed by a court, ix) no review of the judiciary.

## 4. General principles of Article 11

### *4.1. Provided for by law*

The criterion "provided for by law" implies that the exception in question must be enshrined in law in the broadest sense[7]. Where these Guidelines refer to a law, this does not necessarily require a legislative act to be adopted by a parliament, without prejudice to

[7] This criterion should be interpreted in line with Article 4.1 of Convention 108+, as further specified in Paragraph 32 of the Explanatory Report (the term "law of the Parties") and applicable case-law from ECtHR Article 8.2 ("in accordance with law") and should not entail further requirements. Another important reference to the interpretation of the "broadest sense of the law" would be Paragraph 50 of Explanatory Memorandum 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.

requirements pursuant to the constitutional order of the Parties concerned. In line with the domestic legal system of the Party the law is understood in a general way and can mean several pieces of law or legal provisions, whether of statute law or case law, including but not limited to 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 law provided they are in force and fully applicable, and that they respect the principle of the rule of law. Paragraph 91 of the Explanatory Report of Convention 108+ ("Explanatory Report") furthermore specifies that: *"such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed"*.

This can imply, inter alia, that a country's law should be sufficiently detailed in view of its legitimate aim and set out purposes, conditions, limitations and safeguards, so that individuals are appropriately protected against misuse and abuse. The law must also be clear and available to the public so that individuals are able to consider the potential impact of the use of exceptions in given circumstances on their right to privacy, other human rights and fundamental freedoms.

The level of details of the law could vary however depending on the level of interference with human rights and fundamental freedoms allowed by the provisions. The *"Report Digital solution to fight Covid 19"*[8] recommends that countries pay particular attention to, the time limit of the extraordinary measures, legal sunset clauses, purpose limitation, the necessity and proportionality of the measure and the involvement of data protection authorities throughout the process[9]. Paragraph 56 of the Explanatory Report suggests that in case of the processing of sensitive data for legitimate purposes, the appropriate safeguards that complement those already applied have to be put in place. Such requirements can have a bearing on the level of details of the law too, i.e. to explicitly refer to the additional safeguards when such data are to be processed[10]. It follows from the above and from Paragraph 32 of the Explanatory Report 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*."

In terms of accessibility as a criterion of the law, one should note that as the use of exception could very likely result in an interference with the right to private life of individuals, the fact that it should be grounded in domestic laws and being publicly accessible, represent the first important safeguard against arbitrary interference by public authorities. These laws should furthermore include safeguards, which can be legal, procedural, operational, or technical in nature, to ensure that exceptions are applied lawfully, in relation to the purpose of the processing and in compliance with the specific rule of law and data protection requirements and considerations mentioned earlier. The requirement "*sufficiently detailed*" does not mean however, that a Party is required to make publicly available every safeguards or elements thereof that apply at operational level to a covert or secret processing activity, in order to use an exception in regard to national security.

[8] https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c

[9] Including when deciding on the level of details to be published or the level of overall transparency of the legislative measures taken.

[10] Such safeguards comprise for example 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).

These principles also apply *a fortiori* when exceptions are applied to a covert or otherwise secret processing activity, for example where a data subject may not be aware of the processing activity taking place. Therefore the law should contain clear rules for the use of such exceptions, to meet the qualitative requirements of accessibility and previsibility (or "foreseeability").

### *4.2. Respect of the essence of the fundamental rights and freedoms*

Human rights and fundamental freedoms guarantee particular values that are considered universal. The essence of those rights and freedoms are the main characteristics and core values that are required to be protected by states. For example, the right to human dignity and the right that no procedure should lead to inhuman or severely degrading treatment of individuals. In other words, an action taken by public authorities, even if taken on a legitimate ground in the public interest cannot lead to the removal of the protection by the states of the rights guaranteed to individuals.

In line with these criteria, when drafting exceptions in the law, the legislator needs to factor their limits and direct, immediate impacts. Therefore an exception in the law could not lead to the deprivation of privacy of an individual in an unlimited, unconditional or irrevocable manner or to a complete negation or permanent refusal of the data subject's rights (For example, where the right of access to personal data has been refused or restricted at a given time, access may be given at a later time provided that the circumstances surrounding the refusal or restriction have changed.). There may be different ways of restricting the right of access for example taking into account the different contexts where such exceptions are to be used. Generally, the data subject should be kept informed of the progress upon request, and sufficient information as long as it does not hinder the purpose underlying the use of exception should be made available to the data subject.

Neither the introduction nor the application of an exception in law automatically equates to a violation of human rights or fundamental freedoms. However, due regard should be given when introducing the exception in law and when applying it, to the effect that the restriction could have on the data subject, which should not lead to the absolute, indefinite deprivation of human rights and fundamental freedoms as explained above.

### *4.3. Necessary and proportionate in a democratic society*

The obligation to ensure that derogations and exceptions are necessary and proportionate is often interlinked with the way the state exercises its core functions: to protect individuals, ensure public order, safety and the well-functioning of democratic institutions. Obligations of state institutions however cannot be achieved by all available means, arbitrarily or outside the public interest functions. A real and substantive threat to those obligations/core functions of the state should justify the use of provided exceptions. In such cases states would be compelled/authorised in line with the domestic legislation and with their public interest related mandate to for example, protect the population, state institutions, properties, monetary and financial interests, re-establish public order, public safety, ensure the functioning of the judiciary, etc. Furthermore, states should ensure the protection of other human rights and fundamental freedoms, notably the freedom of expression in line with Article 11.1.b when acting in (other) public interest. According to Paragraph 96 of the

Explanatory Report: *"These protections should concern the rights and fundamental freedoms of private parties, such as those of the data subject themself (for example when a data subject's vital interests are threatened because they are 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."*

Therefore, to meet the criterion of necessary and proportionate in a democratic society, the legislator should assess whether the use of power and/or capability underlying the use of data protection exception is drafted in law, whether it pursues a legitimate aim, and thus meets a pressing social need which cannot be achieved by less intrusive means (Paragraph 91 of the ER). The assessment should conclude that there are no alternatives for "less intrusive or less burdensome means" available to achieve it and, the measures themselves are to be justified as necessary and proportionate with the view of the interest(s) at stake in a particular situation and context. As per Article 5.1 "*data processing shall (…) reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake*". Therefore it is always recommended to check whether the use of exception is efficient and effective in response to the specific pressing social need, and such effectiveness and efficiency would not be achieved by less intrusive means. It also seems to be of high importance to ensure under secondary legislation or other appropriate means that only the necessary and proportionate interference with the rights to the protection of privacy and personal data is made in practice. Such impact limitation could be made by describing the intended data processings as detailed as possible and their potential/reasonably expected impact to the interests, rights and freedoms that are at stake.

The interest of the states in taking certain measures must be balanced against the seriousness of the interference with individuals' right to respect for their private life.

Therefore, the legislator should apply a three-step-test in relation to exceptions to guarantee that the underlying domestic legal framework ensures these general conditions for the use of an exception, i.e.: the exception is a) for a legitimate aim, b) necessary to achieve this aim and c) proportionate in doing so. The ways such conditions once defined by law are to be applied or implemented by data controllers will be likely discussed in further guidelines, guidances. For the legislator however it remains highly recommended to check if the law prescribes, enables or makes possible explicitly or implicitly actions, operations that would allow the use of an exception from the provisions of Convention 108+ and if they are in line with the three-step-test.

Checking of first condition seems to be the most straightforward one as the tasks and functions of national authorities are well regulated, often at the highest level (in national Constitutions). So, it is logical that in order to assess if a data processing is carried out for a legitimate aim as defined in Article 11.1, the legislator is invited to check if the purposes for which the exception can be used are defined by and in line with law.

The second condition requires a so-called necessity assessment which is suggested to be conducted to prove that the application of an exception is suitable with regard to the legitimate aim of the processing. In other words, the use of exception needs to be necessary to achieve the defined legitimate purpose, it has to be essential for that or to the avoidance of harm or prejudice to such an objective or legal purpose and that it does not

only represents a mere advantage. This latter can be easily checked by assessing if there are no less burdensome alternatives available. It is recommended that the assessment, should incorporate a collection of independent evidence sources and comparative practices.

The third condition suggests a proportionality assessment which is to be taken in a strict sense and during which the public interest in pursuing a legitimate aim (including protecting other human rights and fundamental freedoms) should be measured against the seriousness of an interference with individuals' right to respect for private life. Such assessment should be conducted to factor all adverse impacts of a measure on the rights to privacy and data protection (including unintended third parties) and that the interference is not excessive in relation to the advantages obtained. In other words, to demonstrate that these can be justified as not excessive with relation to the positive impact that is essential (as justified by the previous criterion) to respond to a pressing social need. The legislator should choose the less intrusive measures to achieve the legitimate purpose so that they can be regarded as proportionate ones.

Finally, it is important to consider that, according to the case-law of the European Court of Human Rights, states have a margin of appreciation to decide on the most appropriate measures and means in achieving the pre-defined legitimate objectives. The legislator in the domestic laws could rely on a margin of appreciation within the above detailed parameters and is invited to consider that the exception used remains within that margin. It is advisable to assess the necessity and proportionality of the particular measure taken, using the methodology proposed above.