



Council of Europe
Conseil de l'Europe

The modernised Convention 108

Council of Europe
Conseil de l'Europe

Convention 108???

- **A common response to collective challenges**
- From EU perspective a “passerelle” between EU and other part of the world
 - Transfer of data
 - Cooperation between authorities
- 20 recommendations, 1 additional protocol and 1 amending protocol – lots of international negotiations and consensus
- Soft law measures equally important through influencing regional, national legislation, jurisprudence
- Convention 108+ has a high level of convergence with EU instruments (GDPR, police Directive)
- Possibility for IGOs to accede, including for the EU
- In the area of public security, it has balanced rules and has the potential of ensuring and international cooperation in the matter
- Influential players in privacy and data protection are all parties (UK, France, Germany) or observers (US, Japan) to its committee
- An essential instrument for guaranteeing the independence of the supervisory authority (see Tunisian example)
- Remarkable standard-setting capabilities (see Argentinian example)
- For non-EU countries it can play an important role in obtaining and/or maintaining adequacy decisions from the EU (which means free flow of data to the EU market)



THE UNIVERSAL DECLARATION OF Human Rights

Preamble recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of justice, peace and good in the world;

Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind, and the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people;

Whereas it is essential, if man is not to be compelled to have recourse, as a last resort, to rebellion against tyranny and oppression, that human rights should be protected by the rule of law;

Whereas it is essential to promote the development of friendly relations among nations;

Whereas the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have

determined to promote social progress and better standards of life in larger freedom;

Whereas Member States have pledged themselves in Article 1, in cooperation with the United Nations, the promotion of universal respect for and observance of human rights and fundamental freedoms;

Whereas a common understanding of these rights and freedoms is of the greatest importance for the full realization of this pledge;

THE GENERAL ASSEMBLY

Recommends that the Universal Declaration of Human Rights be a common standard of achievement for all peoples and all nations, in the end that every individual and every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the peoples of Member States themselves and among the peoples of territories under their jurisdiction.

Article 1 All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

Article 2 Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, birth or other status. No distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be a sovereign State, a territory under its jurisdiction, a self-governing area, or any other limitation of sovereignty.

Article 3 Everyone has the right to life, liberty and security of person.

Article 4 No one shall be held in slavery or servitude; slavery and the trade therein shall be prohibited in all form.

Article 5 No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment.

Article 6 Everyone has the right to recognition everywhere as a person before the law.

Article 7 All are equal before the law and are entitled without any discrimination to equal protection of the law. All are equal in the eyes of the law. Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 8 Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by the law.

Article 9 No one shall be subjected to arbitrary arrest or detention.

Article 10 Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him.

Article 11 Everyone charged with a criminal offence has the right to be presumed innocent until proven guilty according to the law. The rights of the accused shall be fully guaranteed.

Article 12 No one shall be held guilty of any criminal offence on account of his race, colour, sex, religion, or political opinion, or on account of his status as a national, alien, or resident.

Article 13 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. No one shall be subjected to arbitrary arrest or detention. No one shall be subjected to arbitrary exile.

Article 14 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 15 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 16 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 17 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 18 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 19 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 20 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 21 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 22 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 23 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 24 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 25 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 26 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 27 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 28 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 29 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 30 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 31 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 32 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 33 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 34 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 35 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 36 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 37 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 38 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 39 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 40 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 41 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

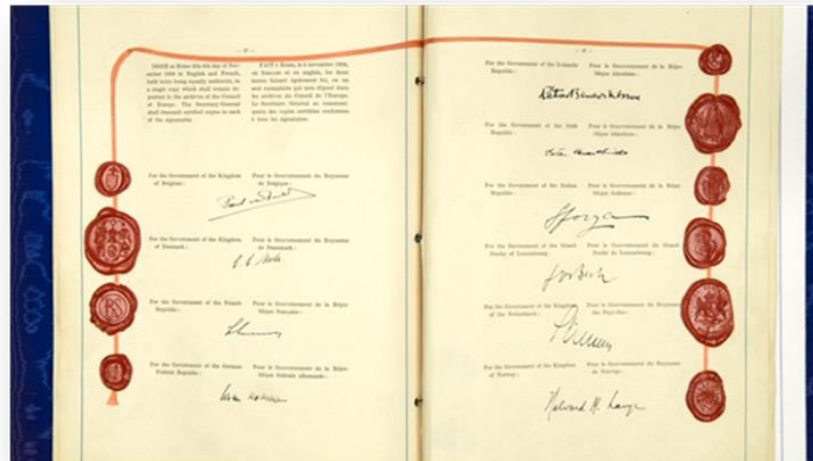
Article 42 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 43 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 44 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 45 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 46 Everyone has the right to a fair and a public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.



Article 8 – Right to private life

- 1. Everyone has the **right** to respect for his private and family life, his home and his correspondence.
- 2. 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 well-being 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.

Data protection : an enabling right

ECHR

Article 1 – Obligation to respect human rights

Article 8 – Right to private life

Article 9 – Freedom of thought, conscience
and religion

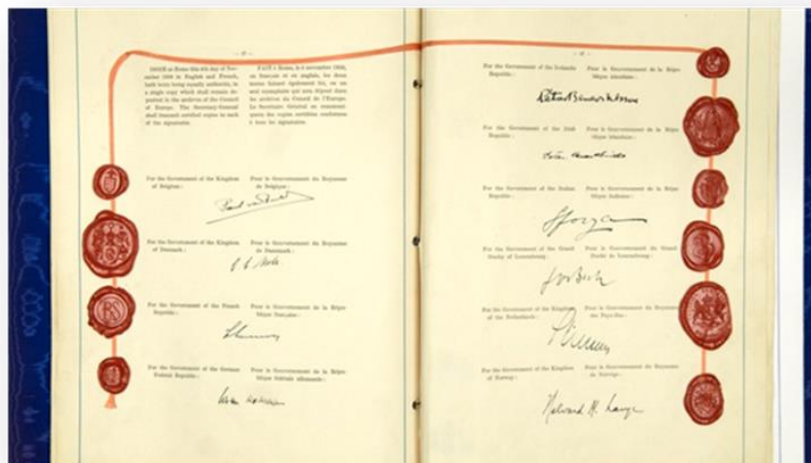
Article 10 – Freedom of expression

Article 11 – Freedom of assembly and
association

Protecting data ? Protecting individuals ?

Convention for the protection of individuals
with regard to the processing of personal
data

CONVENTION 108



Convention 108 (open to signature on 28 January 1981)

UNIQUE (no other international legally binding instrument in the field open to any country)

with a complying data protection legislation

INFLUENTIAL (its principles = data protection principles taken up in all regions of the world)

Convention 108

Article 23 – Accession by non-member States

“1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention [...]”.

Convention 108 today

55 countries bound by the Convention

= Argentina, Cabo Verde, Mauritius,
Mexico, Morocco, Senegal, Tunisia,
Uruguay **+ 47 CoE**

pending: Burkina-Faso and Costa Rica

+ 34 observers (Australia, Brazil, Canada, Chile,
Gabon, Ghana, Indonesia, Israel, Japan, South
Korea, Philippines, USA, New Zealand)

= NEARLY 70 COUNTRIES

Convention 108 - Modernisation

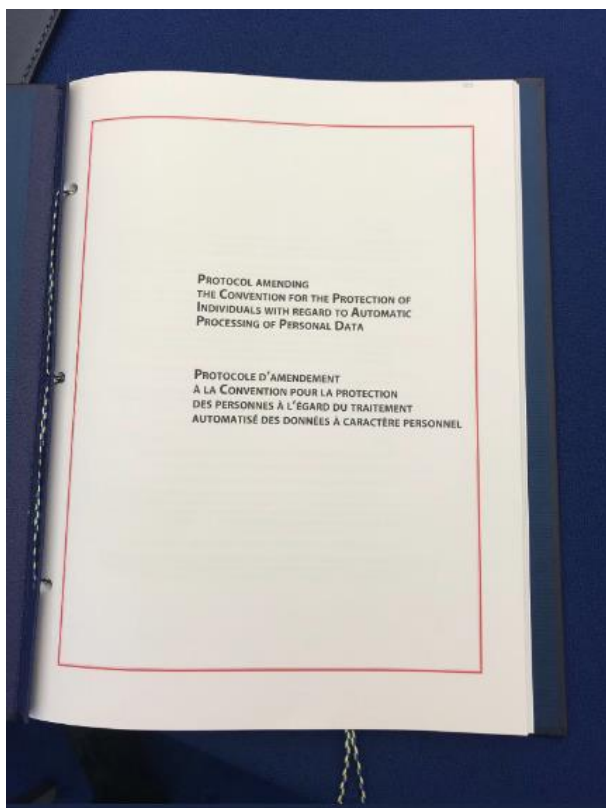
- Reinforce the protection of individuals
 - Strengthen the implementation
-
- **promote** as a universal standard
 - **preserve** general, simple, flexible and pragmatic character
 - **ensure coherence and even convergence** with other relevant legal frameworks (including with the EU)

Convention 108 - Modernisation

January 2011 18 May 2018



Opening for signature CETS 223 10 October 2018



Ratifications

- (32 signatures)
- Bulgaria – 10 December 2019
- Croatia – 18 December 2019
- Lithuania – 23 January 2020
- Serbia – 26 May 2020
- Poland – 10 June 2020
- Mauritius - on 4 September 2020
- Estonia on 17 September 2020
- Cyprus on 21 September 2020
- Malta on 2 November 2020
- Finland – 10 December 2020
- Spain – 28 January 2021

Convention 108+

Preamble

Chapter I – General provisions

Article 1 – Object and purpose

Article 2 – Definitions

Article 3 – Scope

Chapter II – Basic principles for the protection of personal data

Article 4 – Duties of the Parties

Article 5 – Legitimacy of data processing and quality of data

Article 6 – Special categories of data

Convention 108+

Article 7 – Data security

Article 8 – Transparency of processing

Article 9 – Rights of the data subject

Article 10 – Additional obligations

Article 11 – Exceptions and restrictions

Article 12 – Sanctions and remedies

Article 13 – Extended protection

Chapter III – Transborder flows of personal data

Article 14 – Transborder flows of personal data

Chapter IV – Supervisory authorities

Article 15 – Supervisory authorities

Chapter V – Cooperation and mutual assistance

Article 16 – Designation of supervisory authorities

Article 17 – Forms of cooperation

Chapter VI – Convention Committee

Chapter VII – Amendments

Convention 108+

Preamble

“Considering that it is necessary to secure the **human dignity** and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, **personal autonomy based on a person’s right to control of his or her personal data** and the processing of such data;”

Convention 108+

“protect every individual, whatever his or her nationality or residence with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular their right to privacy”

(article 1)

Convention 108+

- Article 3 – scope

"data processing ... **in the public and private sectors...**

... shall not apply to data processing carried out by an individual in the course of purely personal or household activities."

Convention 108+

- Article 4 – Duties of the Parties

“ 3. Each Party undertakes:

- a. to allow the Convention Committee to evaluate the effectiveness of the measures it has taken in its law to give effect to the provisions of this Convention; and
- b. to contribute actively to this evaluation process.”

Convention 108+

- Article 5 - legitimacy of data processing and quality of data

"... shall be **proportionate** in relation to the legitimate purpose pursued and reflect at all stages of the processing a **fair balance** between all interests concerned and the rights and freedoms at stake."

Convention 108+

- Article 5 - legitimacy of data processing and quality of data

"... on the basis of the free, specific, informed and unambiguous **consent** of the data subject or of some **other legitimate basis laid down by law**".

Convention 108+

Sensitive data (article 6)

genetic data, biometric data uniquely identifying a person

“for the information they reveal” – only allowed where appropriate safeguards are enshrined in law, complementing those of the Convention.

+ Ethnic origin, trade-union membership

Convention 108+

Data **Security** (article 7)

obligation to notify, without delay, at least the competent supervisory authority, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

Convention 108+

Transparency (article 8)

obligation for the controller to provide a detailed list of information, as well as any necessary additional information in order to ensure fair and transparent processing

Convention 108+

Rights of the data subject (article 9)

"... not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration"

"...to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her"

Convention 108+

Additional obligations (article 10)

- "... take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate (subject to exceptions)...compliance "
- "examine the likely impact ... prior to the commencement (**PIA**)... and design the processing to prevent or minimise the risk" (**PbD**).
- " implement **technical and organisational measures** at all stages of the processing. (DPO, etc..)
- Adapted according to the context of the data processing (based on potential risks to adapt those measures according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor.)

Convention 108+

Exception: provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

the protection of national security, defence, 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;
the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

Convention 108+

Exceptions and restrictions (Article 11.3)

Processing activities for national security and defence purposes

...each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfil such aim, exceptions to:

- the review mechanism (Article 4.3)
- DPAs' powers with regard to transborder data flows (Article 14.5 and 14.6)
- DPAs' powers (Article 15.2 a,b,c,d)

Convention 108+

Exceptions and restrictions (Article 11.3)

processing activities for national security and defence purposes

"
...

This is without prejudice to the requirement that processing activities for national security and defence purposes are subject to independent and effective review and supervision."

Convention 108 modernised

Provisions possibly subject to exception

- **General principles (fairness, transparency, purpose limitation, data quality requirements: adequate, relevant, not excessive, accurate, up to date, permits only identification no longer that necessary)**
- **Data breach notification to the supervisory authority**
- **Data controller obligation to inform the data subject**
- **Data subject rights**

(Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9)

- **Data controller obligation to inform the data subject**
- **Data subject rights**

(Articles 8 and 9)

In addition to the exceptions above, if provided for by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society:

- **Committee's power to evaluate the effectiveness of the measures taken**
- **To provide information to the supervisory authority on international transfer**
- **To require by the supervisory authority to demonstrate the lawful conditions for international transfer and its ability to intervene**
- **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 4 paragraphs 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d.)

Purposes for which the exception can be enacted

- a. the protection of national security, defence, 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;
- b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.

Processing activities for national security and defence purposes

Convention 108+

Transborder dataflows (Article 14.1)

Limitation to free flow between Parties where (to be applied in specific cases and narrowly)

- real and serious risk that the transfer would lead to circumventing the provisions of the Convention
- Party bound by harmonised rules of protection shared by States belonging to a regional international organisation

Convention 108+

Transborder dataflows (article 14.3 and 14.4)

- Means to secure an appropriate level of protection (*ad hoc* or approved standardised safeguards provided by legally binding instruments)
- Possibilities to transfer in specific cases where consent, specific interests of the data subject, prevailing legitimate interests provided for by law and are necessary and proportionate in a democratic society

Convention 108+

Supervisory authorities (article 15)

"2. ... such authorities:

a. shall have powers of investigation and intervention;

c. shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions;

d. shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention;"

Convention 108+

Supervisory authorities (article 15)

(144 privacy legislation in the world)

"5. The Supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions."

Convention 108+

Cooperation (article 17)

Supervisory authorities “shall co-operate with one another to the extent necessary for the performance of their duties and exercise of their powers, in co-ordinating their investigations or interventions, or conducting joint actions;”

Convention 108+

Evaluation and follow-up mechanism


Objective: *ensure the credibility of Convention 108+ and establish a genuine dynamic of harmonised protection, guaranteeing that data flows occur among Parties offering an appropriate level of protection*

Transparent, effective and impartial

(independent experts / questionnaire / visits)

Ongoing work of the Committee

Work programme 2020-2021

- 
- Evaluation and follow-up mechanism
 - Facial recognition – adopted on 28 January 2021
 - Data processing in Educational settings – adopted on 20 November 2020
 - Recommendation (2010)13 on Profiling
 - Political campaigns and elections
 - Digital Identity
 - Automatic processing of data
 - Guidance Notes (art 11)

Joint Statements by the Chair and the Data Protection Commissioner on

- The right to data protection in the context of the COVID-19 pandemic (published on 30 March 2020)
- Digital Contact Tracing (published on 28 April 2020)
- “Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services” (published on 7 September)

Call for UN member countries to accede

**Joseph A. Cannataci, UN Special
Rapporteur on the right to privacy**



Call for UN member countries to accede

- **Annual report -UN General Assembly (2018)**

- Report A/73/45712

"As an interim minimum response to agreeing to detailed privacy rules harmonised at the global level, ALL UN Member States been encouraged to ratify data protection Convention108+[...]."

- **Annual report -UN Human Rights Council (2019)*=**

- Report A/HRC/40/63

ECHR cases referring to Convention 108

- **Z. v. Finland** (dec.), no. 22009/93, § 95, ECHR 1997-I

Art. 8 (LAW) The Court refers to this treaty in interpreting Article 8 as protecting privacy of personal health data.

- **Amann v. Switzerland** [GC], no. 27798/95, § 65, ECHR 2000-II

Art. 8 (LAW) The Convention as evidence of a broad interpretation of the term "private life". See also: Rotaru v. Romania [GC], no. 28341/95, § 43, ECHR 2000-V; P.G. and J.H. v. the United Kingdom, no. 44787/98, § 57, ECHR 2001-IX.

- **Sofianopoulos and Others v. Greece** (dec.), nos. 1977/02, 1988/02 and 1997/02, ECHR 2002-X

Art. 9 (FACTS) Cited as relevant law.

- **Peck v. the United Kingdom**, no. 44647/98, § 78, ECHR 2003-I

Art. 8 (LAW) The Convention as evidence that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private life (see Z. v. Finland).

ECHR cases referring to Convention 108

- **Von Hannover v. Germany**, no. 59320/00, § 42, ECHR 2004-VI

Art. 8 (FACTS) Cited in Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy.

- **Cemalettin Canlı v. Turkey**, no. 22427/04, §§ 17 and 34, 18 November 2008

Art. 8 (FACTS & LAW) "The Court considers this interpretation of the notion of "private life" to be in line with the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data."

- **S. and Marper v. the United Kingdom**, nos. 30562/04 and 30566/04, §§ 41, 66, 68, 76, 103104 and 107, 4 December 2008

Art. 8 Art. 14 (FACTS & LAW) The Court uses several articles of this convention to assess issues in the case.

- **Uzun v. Germany**, no. 35623/05, § 47, 2 September 2010

Art. 8 (LAW) "The Court has also referred in this context to the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data."

ECHR cases referring to Convention 108

- **Concept of private life – art 2**
 - Amann v. Switzerland; Rotaru v. Romania; Haralambie v. Romania
- **Interpretation of “public information” as part of private life**
 - Haralambie v. Romania; Cemalettin Canli v. Turkey
- **Processing of health-related data - Articles 3 § 2 (c), 5, 6 and 9**
 - Z. v. Finland¹⁵⁴; Peck v. the United Kingdom
- **Processing of personal data revealing ethnic origin – art 6**
 - S. and Marper v. the United Kingdom

ECHR cases referring to Convention 108

- **data subject rights – art 8**
 - Leander v. Sweden
- **case law complementing Convention 108 – art 5 (lawfulness of processing)**
 - unlawful processing defined by the Court
- **Convention 108 as “relevant international law”**
 - **quality of data – art 5**
 - Bernh Larsen Holding AS and Others v. Norway; Khelili v. Switzerland; B.B. v. France; M.M. v. the United Kingdom
 - **processing special categories of data – art 6**
 - B.B. v. France; M.M. v. the United Kingdom
 - **data security – art 7**
 - B.B. v. France
 - **exceptions and restrictions – art 9**
 - M.M. v. the United Kingdom

Guidelines on Artificial Intelligence and Data Protection

(25 January 2019)

- AI may be **a useful tool** for decision making in particular for supporting evidence-based and inclusive policies.
- AI development and use shall respect the rights to privacy and data protection
- AI applications shall not undermine the **human dignity** and the **human rights and fundamental freedoms** of every individual, in particular with regard to the right to data protection
- ECHR & Convention 108+
- Structure: General guidance, guidance for developers, manufacturers and service providers, guidance for legislators and policy makers

I. General Guidance

- I. **protection of human dignity** and **safeguarding of human rights and fundamental freedoms**, in particular the right to the protection of personal data, especially important when AI applications are used in **decision-making processes**
- II. AI development relying on the processing of personal data should be based on the principles of Convention 108+. The **key elements** of this approach are: lawfulness, fairness, purpose specification, proportionality of data processing, privacy-by-design and by default, responsibility and demonstration of compliance (accountability), transparency, data security and risk management.
- III. **Risk based approach** - avoiding and mitigating the potential risks
- IV. **a wider view** of the possible outcomes of data processing should be adopted. This view should consider not only human rights and fundamental freedoms but also the functioning of democracies and social and ethical values (similarly to the Guidelines on Big Data)
- V. **rights of data subjects** shall be respected fully
- VI. **meaningful control by data subjects** over the data processing and related effects on individuals and on society

II. Guidance for developers, manufacturers and service providers

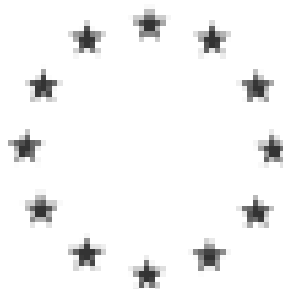
- I. values-oriented approach in the design of their products and services
- II. possible adverse consequences of AI applications on human rights and fundamental freedoms should be assessed, and, considering these consequences, **a precautionary approach** based on appropriate risk prevention and mitigation measures should be adopted
- III. **human rights by-design** approach should be adopted and any potential biases, including unintentional or hidden, and the risk of discrimination or other adverse impacts on the human rights and fundamental freedoms of data subjects should be avoided
- IV. unnecessary, redundant or marginal data during the development, and training phases should be reduced and then the **model's accuracy** as it is fed with new data should be constantly monitored. The use of synthetic data may be considered.
- V. The **risk of adverse impacts** on individuals and society due to de-contextualised data and de-contextualised algorithmic models should be adequately considered
- VI. **Consultation of external bodies** (committees of experts, academic institutions)
- VII. **Participatory forms of risk assessment**
- VIII. right of individuals not to be subject to a decision significantly affecting them based solely on automated processing, without having their views taken into consideration should be ensured
- IX. users' freedom of choice over the use of AI, by **providing feasible alternatives to AI** applications should be guaranteed
- X. forms of **algorithm vigilance** (specific duties on transparency, prior assessment of the impact of data processing on human rights and fundamental freedoms) that promote the accountability should be adopted
- XI. **Data subjects should be informed** if they interact with an AI application and **have a right** to obtain information on the reasoning underlying AI data processing operations applied to them. This should include the consequences of such reasoning.
- XII. **The right to object** should be ensured in relation to processing based on technologies that influence the opinions and personal development of individuals.

III. Guidance for legislators and policy makers

- I. principle of accountability, the adoption of risk assessment procedures and the application of other suitable measures, such as **codes of conduct and certification mechanisms** should be privileged
- II. **algorithm vigilance** should be applied during public procurement procedures
- III. **supervisory authority** should be sufficiently empowered to support and monitor the algorithm vigilance programmes
- IV. **Possibility of human intervention** should be preserved
- V. Supervisory authority should be consulted when AI applications have the potential to significantly impact the human rights and fundamental freedoms of data subjects
- VI. **Cooperation among regulatory authorities** such as consumer protection; competition; anti-discrimination; sector regulators and media regulatory authorities should be encouraged
- VII. **Independence of external bodies** should be guaranteed
- VIII. **Inclusion of stake-holders** in the debate on what role AI should play in shaping social dynamics, and in decision-making processes affecting them
- IX. **Digital literacy, awareness raising, education, training and scientific researches** should be supported

T-PD(2018)01

Practical guide on the use of personal data in the police sector



I - General background

- Convention 108, modernised Convention 108
- Recommendation (87)15 (no to replace but to update)
- acknowledges that the lawful collection and use of personal data for law enforcement purposes are **crucial** in the interests of national security and for the prevention of crime or maintenance of public order.
- emphasises with concrete examples that the prevention and suppression of crime, including through the collection and use of personal data for law enforcement purposes, can be efficiently conducted **in compliance with the law**.

II – General considerations

- The collection and use of personal data for law enforcement purposes constitutes an **interference** with the right to private life and data protection
- it must be based on law (clear, foreseeable and accessible),
- pursue a legitimate aim and be limited to what is necessary and proportionate to this aim pursued
- **Data processing** has to comply with the necessity, proportionality and purpose limitation principles,
 - it should be based on predefined, clear and legitimate purposes set out in the law,
 - it should be necessary and proportionate to these legitimate purposes and should not be processed in a way incompatible with those purposes,
 - It should be carried out lawfully, fairly and in a transparent manner,
- **Personal data** within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes,
 - They should be accurate and up-to-date to ensure **the highest data** quality possible.

III – Practical guidance

- **Collection of data and use of data**

- an evident and direct correlation should exist between the data processing carried out by the police and a situation where individuals have already committed or are likely to commit a crime.
- once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific task of the police) should exist
- distinction in how the police processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses.
- The police should be able **to demonstrate**:
 - The link between the person and the investigation
 - That the data processing is compliant with the data protection rules
 - That it actively implements measures to safeguard and promote data protection in all its activities

III – Practical guidance

- **Subsequent use of data**

- Must meet the applicable legal requirements
- Data should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation
- Data related to vulnerable individuals such as victims, minors, or of those enjoying international protection, should be subject to additional care and legal analysis
- In cases related to trafficking in human beings, drug trafficking or sexual exploitation or where victims' data may subsequently be used also when they are considered as suspects, or where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to enhance their exchange of information on the matter within international or regional police bodies

III – Practical guidance

- **Processing of special categories of data (sensitive data)**

- Can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of an adverse legal effect significantly affecting the data subjects
- A careful balance of interests taking into account the purpose of the investigation, the context and the nature of the data is necessary
- **Data Protection Impact Assessment** – CNIL methodology, ICO, Interpol, etc.
- collection and processing of sensitive data in the context of profiling is prohibited (Principle 3.11 of Recommendation (2010)133) except if these data are necessary for and proportionate to the lawful and specific purposes of processing and as long as domestic law provides appropriate safeguards.

III – Practical guidance

- **Providing information to data subjects**

- **Two-fold obligation:** general information to the public on the data processing, and specific information to data subjects if no restrictions or derogations as described in Point 7 apply to the data processing.
- General information: should be effectively and broadly accessible, should include details about exceptions to data subject's rights and how they could submit an appeal to the DPA or to the judiciary
- Specific information: on the data processing envisaged before the processing or, if it is not possible for objective reasons, after it. Data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.
- If data subjects cannot receive complete information on the processing the police undertake with their data; this should not affect the possibility to exercise of the right of access.

III – Practical guidance

- **Data subject's rights**

- Right of access, Right to rectification and Right to erasure
- Police in principle should **grant access to the data subject** if there is such request, however exceptions, derogations may apply.
- Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified.
- Police should aim to answer even general questions arising from data subjects on the processing activities in relation to their personal data, but can use standardised forms to facilitate communication
- The right of access should, in principle, be free of charge and communicate “in an intelligible form”
- As a rule, domestic law should, ideally, provide for direct access.
- Proposed changes, deletion should be supported by evidence
- Right of redress is to be granted

III – Practical guidance

- **Exceptions from the application of data protection principles**

- Exceptions **have to be foreseen by law** (the law should be public, open and transparent and, in addition, detailed enough) and **their use has to constitute a necessary and proportionate measure in a democratic society**. They can only be used for the purposes defined in Convention 108+.
- The exceptions which have to be incorporated into national legislation **should not be described in a general way**, but should serve a well-defined purpose.
- If the exception, as defined by national law providing specific safeguards is used by the police, **it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim** for which it is being used.
- **The aim of using exceptions by the police should be limited to cases where not using those exceptions would endanger tasks of the police**

III – Practical guidance

- **Use of special investigation techniques**
 - when deciding on their use, some **data protection considerations** could be assessed in order to allow to the police to use the least intrusive means of data processing during its operations
 - **the high potential of severe interference with the right to privacy has to be balanced with the seriousness of the offence** to be prevented or investigated and the cost-effectiveness, the use of resources and the efficiency of investigations

III – Practical guidance

- **Introduction of new data processing technologies**

- **DPIA is advisable** as the introduction of new data processing technologies bears per se such potential risk.
- It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity and that it takes into account accountability considerations.
- **Data security and safety** of communications needs that the highest standard is taken into account when introducing such technologies.
- **IOT:** requires measures such as **data authentication, access control to ensure data security and resilience to (cyber) attacks, strong end-to-end encryption**
- **Big Data:** Council of Europe's Recommendation CM/Rec(2010)13, human intervention and the combination of new analytical methods with traditional ones are highly recommended

III – Practical guidance

- **Storage of data**

- Clear rules have to be established in relation to the handling of different data base with special attention to the analysis of searches resulting in multiple results.
- Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve the police purposes.
- The grounds for retention and processing **should be reviewed periodically.**
- it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judicial procedure terminates completely
- Data should as far as possible be categorised according to the degree of accuracy and reliability in order to assist the police in their activities. It is recommended that handling codes are used to distinguish these categories. A classification system facilitates the assessment of the quality of the data and how reliable it is.

III – Practical guidance

- **Communication of data within the police sector**
 - The police can only communicate personal data within the police sector if a **legitimate interest** exists for such communication within the framework of the legal powers of these bodies
 - There should be clear and transparent rules on how the police grant access to data held by it and on which grounds.

III – Practical guidance

- **Communication of data by the police to other public bodies**
 - If it is **provided for by law** and the data are required by the recipient to enable them to fulfil their lawful task.
 - Mutual assistance agreements foreseen by the law between law enforcement and public bodies allows the public bodies to have access to law enforcement data which would be essential in the fulfilment of their duties and tasks
 - Specific rules should be followed when data are to be transmitted domestically outside of the police (as those data are sensitive data)

III – Practical guidance

- **Communication of data by the police to private bodies**
 - **Only in specific cases, based on law** and only to be done by the authority which is processing the data.
 - Only for the purposes of the investigation or other important police tasks, in the interest of the data subject, for humanitarian reasons or if it is necessary to prevent serious and imminent risk to public order or public security AND an appropriate level of protection which takes into account the sensitive nature of police data is ensured.
 - When sharing data with media, special consideration should be given to the assessment to determine that it is necessary and that such publicity is allowed in the public interest. Appropriate safeguards have to be put in place to ensure the respect for the rights of the individuals involved in the case.
 - Such communication should only be on **a case by case basis** and in each case there must be a clear legal basis providing the necessary procedure (e.g. need for specific authorisation)

III – Practical guidance

- **International transfer**

- As a general rule any **transfer of police data internationally should be limited to police bodies** and should be fit for purpose and in accordance with the law.
- It is required to ensure that proper measures are in place to protect the security of the information.
- **An appropriate level of data protection** should be guaranteed (e.g. through ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments) if data are to be transferred to countries or organisations not participating in Convention 108.
- If there are conditions applied by the sending authority in relation to the use of the data in the receiving state these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout all processing operations and the sending authority should obtain reassurances from the recipient that agreed conditions are respected.

III – Practical guidance

- **International transfer to non-police body**

- As a general rule any transfer of police data internationally should be limited to police bodies and should be fit for purpose and in accordance with the law.
- In this context it is to be noted that in such a case, the **data controller has a double obligation** with respect to the protection of personal data: one imposed by the legal framework of the country where the data controller resides and the one which is related to the data transfer.
- The local police should be informed afterwards.
- The police is required, wherever possible, to make use of existing international legal instruments, in respect of this type of data transfer.
- International transfers may also exceptionally occur where the police communicate personal data for the specific interests of the data subject or for prevailing legitimate interests (such as for instance for humanitarian purposes).

III – Practical guidance

- **International transfer to non-police body**

- The international transfer of personal data to a non-police public body is only permissible **exceptionally and in individual cases** if it is required for the performance of the task of the transferring authority and there is no effective means of transferring the data to a competent police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers especially those related to the requirement of an appropriate level of protection which takes into account the sensitive nature of police data
- **The international transfer of personal data between police and private bodies in a different jurisdiction should be avoided as a general rule.** It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police, it is provided by legal means, where an appropriate level of protection which takes into account the sensitive nature of police data is ensured.
- This might change if the second additional Protocol to the Budapest Convention is adopted (providing for a specific legal basis and appropriate level of protection for individuals)

III – Practical guidance

- **International transfer to non-police body**

- **Additional factors** to be considered for such a transfer are the emergency of the situation, the nature of the crime, its trans-border character and where the involvement of the police would compromise the purpose of the investigation for objective reasons.
- Other facts as data security, the reassurance received as to the use of the data and the lawfulness of the data transfer in the receiving country have to be taken into account.
- In this cases the data controller has **a double obligation** with respect to the protection of personal data: one imposed by the legal framework of the country where the data controller resides and the one which is related to the data transfer.

III – Practical guidance

- **Conditions for communications**

- high level of **data quality**, it is advisable to have in place an additional check before sharing the data with others
- **data security** at the highest level possible

- **Safeguards for communication**

- **necessity and purpose limitation principle**
- any data shared should not be used for anything other than the purpose for which it was sent or received

- **Interconnection of files and on-line access to files**

- they must be authorised or be underpinned by a **legal obligation to comply with the purpose limitation principle**.
- Clear legislation and guidance, which adheres to the data protection principles, should exist for cross referencing of databases. Such **cross referencing should be necessary, purpose bound and proportionate**.

III – Practical guidance

- **Data security**

- When considering data security the police should also take into account factors such as **data localisation**, **adequate certification of service providers and insurance of the availability of data**. It is also advisable to pay attention to data security considerations when **distributing access rights**.
- To report **data breaches** (at least to the DPA)
- DPIA is recommended. The more sensitive the data are the greater protection is required.
- **Authorisation and authentication** mechanisms are essential to protect the data, and sensitive information should always be **encrypted**.
- To have in place an **audit regime** to regularly check that the level of security is appropriate.
- **A Data Protection Officer (DPO)** within the police can play an essential role.
- Identity & Access Management System (IAM) may be recommended to manage employees and third party access to information
- Privacy-by-Design and PETs

III – Practical guidance

- **External control**

- The supervisory body should be **completely independent**
- It should have **sufficient resources** to perform its tasks and duties and should not accept instructions from anybody
- The **personal independence** of its chair/president including political, financial, functional and operational independence, are decisive factors when judging how independent the supervisory body is.
- The legal and administrative tools at its disposal shall be **efficient and its decisions should be enforceable**.
- Supervisory authorities **should have the ability to cooperate** in law enforcement matters bilaterally and also via the Committee of Convention 108.

Recommendation CM/Rec(2019)2 of the Committee of Ministers
to member States
on the protection of health-related data

(27 March 2019)

- Convention 108 and Recommendation No. R (97) 5 of the Committee of Ministers to member States on the protection of medical data
- changed environment due to digitisation and massive exchange of information
- benefits of the increasing digitisation and people's desire to have more control over their data
- increased geographical mobility, IoT, mobile health applications
- health related data are special categories of data
- respect for individuals' privacy and the confidentiality of their information
- the processing of health-related data should always aim to serve the data subject or to enhance the quality and efficiency of care, and to enhance health systems where possible, while respecting individuals' fundamental rights

- **Purpose**
 - regulating the processing of health-related data in order to guarantee respect for the rights and fundamental freedoms of every individual, in particular the right to privacy and to protection of personal data
- **Scope**
 - to the processing of personal data relating to health in the public and private sectors (including via digital tools)
- **Definitions**
 - “personal data”
 - “data processing”
 - “anonymisation”
 - “pseudonymisation”
 - “health-related data”
 - “genetic data”
 - “controller”
 - “processor”
 - “reference framework”
 - “interoperability”
 - “mobile devices”
 - “health professionals”
 - “external data hosting”

- **Legal conditions for the processing of health-related data**
 - principles
 - legitimate basis
 - data concerning unborn children
 - health-related genetic data
 - sharing of health-related data for purposes of providing and administering health care
 - communication of health-related data for purposes other than providing and administering health care
 - storage of health-related data
- **Rights of the data subject**
 - transparency of processing
 - access to data, rectification, erasure, objection to the processing and data portability

- **Security and interoperability**
 - security
 - interoperability
- **Scientific research**
- **Mobile devices**
- **Transborder flows of health-related data**

2020 DATA PROTECTION REPORT

(October 2020)

I. Legal Analysis of the legislative developments

A. Emergency measures

B. Analysis of the impact on specific provision of Convention 108 and Convention 108+

C. Specific legislation and processing of personal data

II. A case-study: the use of digital solutions

A. Digital contact tracing app

B. Other purposes

C. Public engagement and private sector involvement

D. Transparency and Open sources

E. Users' expectations

Legal Analysis of the legislative developments

Convention 108+ allows the lawful use by governments of exceptions without necessarily having to adopt emergency measures (which include exceptional derogations). However, such exceptions must be provided for by law, respect the essence of fundamental rights and freedoms and be necessary and proportionate in a democratic society.

A. Emergency measures

Fundamental rights restrictions

- ▶ Three main approaches : general emergency measures, adoption of emergency measures in specific sectors, adoption of emergency measures without a specific legislative basis.
- ▶ 9 Parties to ECHR made use of article 15 ECHR
- ▶ National and local/regional measures (with different level of transparency).
- ▶ The principles governing a state of emergency (Venice Commission and Secretary General of the Council of Europe) : overarching principle of the Rule of Law, necessity, proportionality, temporariness, effective (parliamentary and judicial) scrutiny, predictability of emergency legislation, loyal co-operation among state institutions.

- Measures such as mandatory quarantines and lockdowns limiting the freedom of movement may be necessary to combat the Covid-19.
- Such measures can be highly invasive and constitute important limitations to fundamental rights (privacy, data protection, freedom of movement and assembly, freedom of speech).
- Impact of emergency measures on right to data protection and privacy depends on nature of the measures adopted, their implementation and on the effectivity of oversight, including the judiciary and the supervisory authorities.

B. Analysis of the impact on specific provision of Convention 108 and Convention 108+

LEGAL BASIS

Article 5 of Convention 108+



The catalogue of legal basis can cover various data process developed in Covid-19 context.

Legal basis : legal obligation and public interest

- Denunciation of process without legal basis (civil society and academia);
- References to health law;
- Use of drones has led to numerous concerns, including legal actions
- National regulation should define the scope and purpose of intended data processing;
- Using voluntary apps (consent) or mandatory apps (with a legal basis);

Legal basis: consent

- Difficulty to obtain a valid consent : health data are sensitive, pressure in Covid-19 context to accept the process;
- In employment and educational context, the consent may not be free because of the existing hierarchy

PURPOSE LIMITATION, STORAGE AND SHARING DATA

Article 5.4.b) of Convention 108+

Compliance with this principles is one of major challenges during the Covid-19 crisis.

In some states, access to certain health data has been opened to police forces, mayors in order to organise and enforce quarantine measures.

The access to data from private and/or public entities is allowed to some Ministers, the police and health authorities, even localisation data and it based on a wide defibition of the purpose.

The publication of some patient data or data of deceased persons (sometimes described as anonymised despite possible subsequent reidentification, and sometimes not anonymised) were observed in several Member States.

The duration of data retention has sometimes been unclear in some Member States, in particular concerning quarantine measures which, based on location data, mostly fall within the scope of Convention 108+ (2 weeks).

PROPORTIONALITY

Article 5 of Convention 108+

Measures that cannot achieve their intended purpose can never be considered proportionate (exam of some measures still underway).

For instance, in Norway, the data protection authority required the suspension of the contact tracing app because of the low numbers of downloads impacting the effectiveness of the tool.

Measures can also be disproportionate if their impact on the private life of individuals is too high, in case for example of a wording very wide.

SECURITY MEASURES

In Covid-19 context, protecting data against unlawful access is very important regarding the sensitive caractere of health data.

TRANSPARENCY

Article 8 of Convention 108+

Data protection authorities insisted, in several Member States, on the need to clearly inform data subjects about aspects of the processing.

20 Countries published the source code of their app of contact tracing, this particular diligence with regard to transparency is appreciated.

RIGHTS OF THE DATA SUBJECTS

Article 9 of Convention 108+

The exercise of rights such as the right of access or opposition can be difficult in the Covid-19 context. In some cases such rights have been formally restrained.

The crisis impact on delay affects rights to data subjects, data protection authorities announced they would take into account extenuating circumstances.

AUTOMATED DECISION MAKING AND USE OF AI

Article 9 of Convention 108+

In the context of the pandemic its concern precisely personal data gathered by apps or e-devices. It may also concern immune passports (or certificates) in some Member States. At this times, WHO cannot guarantee immunity to people who have been infected with Covid and therefore there are doubts about the validity of a decision made on such basis. the same reasoning applies to contamination schemes and contact tracing applications.

ACCOUNTABILITY, PRIVACY IMPACT ASSESSMENT, PRIVACY BY DESIGN AND BY DEFAULT → **Article 10 of Convention 108+**

GOOD PRACTICES : Involving independent actors with an oversight role, Parliamentary working groups participated to contact tracing app development and worked on privacy and data protection, the suspension of certain projects has been ordered pending the impact assessment, Consult data protection authorities prior the development of contact tracing app.

Privacy by design is an essential point.

TRANSBORDER DATA FLOWS

Article 14 of Convention 108+

On a worldwide context of pandemic, sharing data is important in order to combat the coronavirus. The Convention 108+ implies that data transferred from a jurisdiction of a State Party to the Convention to a third State continue to be adequately protected even after that transfer (derogations can be apply after a case-by-case study).

ENFORCEMENT AND SANCTIONS

Article 15 of Convention 108+

During Covid-19 crisis, the data protection authorities was very actives (giving opinions, recommendations and accompanying governments).

Civil society and NGOs have been very active in triggering enforcement actions before courts.

C. Specific legislation and processing of personal data

Legislative measures authorized: use of mobile apps for different purposes, use of data traffic and location data from mobile phones and apps, use of other technical tools (like thermal scans)

MOBILE APPLICATIONS

One of the main technologies used by the Governments (contact tracing, give information to population, medical support, crowd control).

Some countries have used non-specific covid-19 applications.

Opinions and statements from national and regional data protection bodies have been issued.

Only a few countries prepared specific and took the required preliminary steps to limit the impact of the tool on fundamental rights.



USE OF TRAFFIC AND LOCATION DATA FROM MOBILE PHONES AND APPS

To help to predict the spread of the virus, the Joint European Roadmap encourage States to process aggregate and anonymised data from social media and mobile network operators.

Concerns were expressed regarding the irreversibility of anonymisation and potential third-party access to the data.

Authorities have asked (by Law or other tools) to network operators and telecom operators localization and traffic data. In some countries, people who didn't respected the lockdown was obliged to install a tracking app.

STOP AVANT DERNIER POINT 2

OTHER DIGITAL SOLUTIONS

Some examples of tools that have been put in place, often without a specific law, to help monitoring the spread of the virus : websites with health questionnaires; use of eBracelets; use of smart cameras allowing for facial recognition; thermal scans; remote control by drones and robots; mandatory virus testing.

Purposes followed by these examples: The use of websites to obtain some health advice or to encourage self-reporting and to report symptoms are also other digital solutions used during Covid-19 crisis.

Drones and robots surveillance are used to monitor compliance with physical distancing measures in public spaces, record people's temperature, and crowd in public places.

INCREASE OF TELEWORKING AND DISTANCE LEARNING

With lockdown measures, teleworking and distance learning have increased rapidly. As a result of this increase, digital solutions can also lead to additional intrusions in the private life of individuals (coming in intimate sphere of the individuals).

Some of these tools have been used without the necessary privacy precautions : doctors, academics, company employees and students have used them to maintain their activities.

Data protection authorities have expressed concerns about the following issues notably: legal basis for the processing of employees and students' data; risks of constant on-line monitoring; disproportionate access to the terminal and private home of the individual (screenshots); risk of function creep; data security.

II. A case-study: the use of digital solutions

Different tools were used when we started to understand the dissemination of the virus, like apps.

The Council of Europe sent a questionnaire on 27 May 2020 to the 55 Parties to Convention 108 :

- Do public authorities in your country plan to use or already use Covid-19 apps? If so, for what of the mentioned purposes?
- What guarantees will, or do, the Covid-19 apps offer to ensure the right to respect for private life and the protection of the personal data of those concerned?
- To your knowledge, do these apps use artificial intelligence (machine learning) and if so, for what purpose?
- Do public authorities in your country plan to use, or already use, other information technologies to monitor and/or control the spread of Covid-19?
- Is the data protection authority (in the countries where it exists) involved in the development, deployment, control of any app or other technology listed above?

A. Digital contact tracing app

Contact tracing (even manual) has always been used in epidemic monitoring. The mobile apps in the Covid-19 context have been considered as a complementary tool to identify infected people. Sometimes, measures adopted on the basis of these applications may be disproportionate due to a malfunction of the application.

The use of application responds to several protocols concerning the transmission of data but also the digital tracing of proximity contacts, as examples :

- Exposure notification
- Blue Trace/open trace
- Pan European Privacy Preserving proximity Tracing

The protocol can be a centralised data collection by national authorities, or decentralised data processing.

B. Other purposes

Examples of such other purposes are:

- ▶ provide general news and information about the pandemic;
- ▶ help people with self-diagnosis of symptoms;
- ▶ provide instructions to avoid infection;
- ▶ provide information about access to health services;
- ▶ create maps to help people avoid virus hotspots;
- ▶ enforce containment measures;
- ▶ fill in a form about reasons for movement during lockdown;
- ▶ map travel patterns from inhabitants;
- ▶ create daily statistics of recorded cases;
- ▶ record physical passage of visitors at entry and control points;
- ▶ allow users to submit online reports about the violation of rules by other people;
- ▶ provide crowd control.

C. Public engagement and private sector involvement

In some Countries as Sweden, the government didn't launched an application but it is academics who have proposed such a tool, app developpers was also solicited in other States and open development approaches have been implemented.

D. Transparency and Open sources

Many countries have made the source code of their apps open source in order to increase transparency and provide a higher level of trust amongst the general public.

The consequence of such publication is that users confidence increases and provides them means of control of their rights to privacy and data protection.

E. Users' expectations

Trust in such digital solutions is instrumental to the level of adoption, and thus the effectivity of the system. And the respect of data protection is a central element of this trust.

Users expectations are on data minimisation, retention period, clarity in the purpose and legal grounds.

CONCLUSIONS

Even if numerous call to a common action with interoperable systems and join our forces in an international level countries have choose individually their own digital response to the health crisis.

To mitigate the risks of ad hoc measures or fragmented approaches and to contribute to the effectivity of applications by a large uptake, it is essential for governments and other relevant stakeholders to build trust together, closely involving the civil society and the general public in the development of those digital solutions and investing in transparency measures (publication of the source code, dissemination of the findings of data protection impact assessments, organisation of hackathons/appathons, etc).

Ensure that facial recognition does not harm fundamental rights

STRASBOURG | 28 JANUARY 2021



Facial recognition is the automatic processing of digital images containing individuals' faces for identification or verification of those individuals by using face templates. The uses of this technology are many and varied, some of which may seriously infringe the rights of data subjects. For example, integrating facial recognition technologies to existing surveillance systems poses a serious risk to the rights to privacy and protection of personal data as well as to other fundamental rights since the uses of these technologies do not always require the awareness or cooperation of the individuals whose biometric data is processed, considering for instance the possibility of accessing digital images of individuals on the Internet.

On 28 January, the [Committee of Convention 108](#) has adopted [Guidelines on facial recognition](#) that provide a set of reference measures that governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies should follow and apply to ensure that they do not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data.

Contents

I.	GUIDELINES FOR LEGISLATORS AND DECISION-MAKERS	4
1.	Lawfulness	4
1.1.	Strict Limitation by Law of Certain Uses	5
1.2.	Legal Basis in Different Contexts	5
1.2.1.	Integrating Digital Images to the Facial Recognition Technologies	5
1.2.2.	Use of Facial Recognition Technologies in the Public Sector	6
1.2.3.	Use of Facial Recognition Technologies in the Private Sector	7
2.	Necessary Involvement of Supervisory Authorities	8
3.	Certification	8
4.	Raising Awareness	8
II.	GUIDELINES FOR DEVELOPERS, MANUFACTURERS AND SERVICE PROVIDERS	9
1.	Data and Algorithms Quality	9
1.1.	Representativeness of the Data Used	9
1.2.	Data Life Duration	9
2.	Reliability of the Tools Used	9
3.	Awareness	10
4.	Accountability	10
III.	GUIDELINES FOR ENTITIES USING FACIAL RECOGNITION TECHNOLOGIES	10
1.	Legitimacy of Data Processing and Quality of Data	11
2.	Data Security	13
3.	Accountability	13
3.1.	Data Protection Impact Assessment	14
3.2.	Data Protection by Design	15
4.	Ethical Framework	15
IV.	RIGHTS OF DATA SUBJECTS	15

Recalling the need for a legal framework

Facial recognition is a processing of biometric data (= sensitive data).

Only allowed with an appropriate legal basis and additional guarantees provided for by law (Article 6 Convention 108+).

The committee stresses that **certain uses of facial recognition technologies should be banned.** For instance, in order to **avoid any risk of discrimination**, it recommends prohibiting the use of facial recognition for the sole purpose of determining a person's skin colour, religious or other belief, sex, racial or ethnic origin, age, health or social condition, unless appropriate safeguards are provided by law.

This ban should also be applied to **affect recognition** technologies, which can identify emotions and be used to detect personality traits, inner feelings, mental health or workers' engagement, since they pose important risks in fields such as employment, access to insurance or education.

Developers, manufacturers and service providers

should ensure the quality of data and algorithms, ensure the reliability of the tools used and data security, educate users.

Entities using facial recognition technologies

are subject to compliance with the principles and provisions applicable in terms of data protection (legitimacy of the processing, transparency, fairness, accuracy, accountability, minimisation, limited retention period, data security, impact analysis, etc.).

Finally, the **rights of individuals** must be guaranteed (Article 9 Convention 108+).

For example, in the event of false matches, they must be able to request a rectification.

Thank you for your attention



www.coe.int/dataprotection

dataprotection@coe.int