Strasbourg, 20 November 2019 T-PD(2019)8FIN

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

CONVENTION 108

Opinion on the provisional text and explanatory report of the draft Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) on direct disclosure of subscriber information and giving effect to orders from another Party for expedited production of data

Directorate General Human Rights and Rule of Law

1. Background

1. The Cybercrime Convention Committee (T-CY) started in 2017 to work on the drafting of a second Additional Protocol to the Cybercrime Convention, in view of rendering traditional mutual assistance (MLA) under the Convention more effective (including through the provision of video conference hearing and emergency MLA procedures) and introducing the possibility of *direct disclosure* from service providers in other jurisdictions. Such direct disclosure poses new challenges, implying that data protection safeguards inserted in the Protocol must *also* adequately cover the scenario of direct cooperation, in addition to traditional MLA scenarios to obtain data from service providers.

2. It bears relevance to recall that, leading up to the 2018 Octopus Conference, the 36th Plenary of Convention 108 (19-21 June 2018) adopted Provisional Answers to the Discussion paper for the 2018 Octopus Conference. In addition, the available preparatory documents for the 38th Plenary of Convention 108 (13-14 June 2019), were a T-CY discussion paper on conditions for obtaining subscriber information in relation to dynamic versus static IP addresses, a T-CY discussion note for the consultation with data protection experts (consultation which was held in Strasbourg on 26 November 2018, in which both the Secretariat of the Committee of Convention 108 and the expert participated), and an expert note on the inclusion of data protection safeguards relating to law enforcement trans-border access to data in the second Additional Protocol (document T-PD(2019)3). The Committee of Convention 108 recalls that the Second additional Protocol should adequately reflect the Council of Europe *acquis* on fundamental rights and freedoms, in particular on the protection of personal data. It is therefore essential to ensure consistency of the Second additional Protocol with Convention 108+ (Convention 108 as amended by Protocol CETS 223) which applies to all data processing carried out in the public and private sectors. The current opinion draws and expands on a number of elements, listed hereafter, which were already raised in the Committee of Convention 108 provisional answers to the above mentioned discussion paper for the 2018 Octopus conference and/or in the recent expert note:

a. priority must be given to improving traditional MLA procedures, whereas direct cooperation should be kept for specific cases as an expedited procedure;
b. envisaged direct cooperation or expedited MLA procedures should ideally be limited to subscriber information only;
c. when pertaining to subscriber information, the data protection, procedural and rule of law safeguards of at least both the requesting and the requested Parties should be taken into account;
d. if pertaining to traffic information after all, the data protection, procedural and rule of law safeguards of at least both the requesting Party and the Party where the data subject has used the service(s) should be taken into account;
e. envisaged direct disclosure or expedited MLA procedures must be established on a proper legal basis, and be in conformity, as far as transfer of personal data is concerned, with Article 14 of Convention 108+, avoiding systematic reliance on derogations at all price;
f. any newly established cooperation regime must comply with other relevant data protection requirements, such as with regard to the limited storage of data, subsequent use of data, processing of sensitive data, data breach notification, transparency, accountability, and effective independent oversight;
g. any newly established disclosure regime must either be framed in a unified data protection regime, based on Convention 108+, ideally by inviting Parties to join the latter, or in an optional data protection regime, comparable with that of Article 26.3, 2nd indent of ETS 182, allowing for the combined application of the data protection regimes of the relevant Parties, in line with their national and international data pro-

tection commitments, and reflecting compliance with a range of jointly established substantive data protection principles, in line with Convention 108+.

3. In light of the upcoming Octopus Conference of 20-22 November 2019 and related consultation, the T-CY has now released new provisional text of provisions of the draft Second Additional Protocol, as well as a discussion guide for consultations, thereby seeking written comments from stakeholders, including data protection authorities, and the Committee of Convention 108.

4. The present document provides the provisional position of the Committee of Convention 108 on the newly released provisional text and explanatory report of the draft second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185) regarding specifically the provisions on direct disclosure of subscriber information and giving effect to orders from another Party for expedited production of data (other provisional texts of provisions submitted to consultation fall out of the Committee's field of expertise).

5. In a note preceding the draft text and explanatory report of the articles concerned, the T-CY has set out that these "may change as the negotiations develop, depending on the outcome of other provisions that have not yet been prepared and/or other comments received" and that they "should be considered by the [T-CY Protocol Drafting Group and Protocol Drafting Plenary] in order to determine whether further changes are required [...] (in view of the unique circumstances of direct cooperation between authorities and providers) once the ongoing work on conditions and safeguards, including with regard to data protection and privacy, has resulted in a text and explanatory report" [emphasis added].

6. Consequently, the present opinion does not only pertain to the provisional text and explanatory report of both articles concerned, but also provides provisional input of the Committee of Convention 108 for the T-CY's on-going work on conditions and safeguards with regard to data protection. Reference is made here to page 18, point 4.2, para 11, *in fine*, respectively page 29, point 5.2, para 19-20 of the draft explanatory report (to paragraph 2 of the draft article on direct disclosure of subscriber information respectively paragraph 8 of the draft article on expedited production of data between traditional authorities). In these instances, the T-CY explicitly envisages to include an article in the Second Additional Protocol to conditions and safeguards with regard to data protection. The Committee of Convention 108 looks forward to the provisional text of this crucial part of the second Additional Protocol, and highlights that the present opinion is intrinsically dependent on the content of that important part, on which it stresses it wishes to be consulted in as early a stage possible and for which the Committee stands ready to provide its expertise (including on the interpretation of the data protection principles included under 7).

2. Direct disclosure of subscriber information

7. In line with the proposed scoping in the explanatory report (on pages 16-17, in point 4.2, para 4) of subscriber data as potentially inclusive of both static and dynamic IP addresses:

> "Information needed [in specific cases] for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time".

The Committee of Convention 108 recognises that access to both static or dynamic IP addresses may be required in specific cases for the sole purpose of establishing the information as meant in Article 18.3 of the Budapest Convention. It stresses, however, that subscriber data should never be inclusive of any (other) traffic data or content data. The Committee therefore recommends to specify under which circumstances IP addresses could be considered as subscriber information, as meant in Article 18.3 of the Budapest Convention, especially paying due attention to the fact that, depending on the circumstances, an IP address may be evidence of who owns a subscriber account, but does not necessarily identify the individual user at any given time. Moreover, The Committee can only support the potential inclusion of IP addresses under subscriber information if it is specified in the actual Protocol text (both in the articles on direct disclosure and traditional orders for expedited disclosure) and it the corresponding parts of the explanatory report that IP addresses are to be used solely for identification purposes and in specific cases only.

8. The Committee of Convention 108 equally recognises that some Parties currently treat dynamic IP address information as traffic data (for constitutional or other principled reasons, as documented in the T-CY discussion paper on conditions for obtaining subscriber information in relation to dynamic versus static IP addresses). Based thereon, the T-CY has suggested, through the insertion of para 9.b of the draft text, to allow such Parties to reserve the right not to apply the provision on disclosure of subscriber information to "certain types of access numbers" (also reflected in the proposed explanatory report on page 17, in point 4.2, para 4: "Accordingly, paragraph 9.b provides a reservation for some Parties"). The Committee of Convention 108 regrets that the proposed solution might lead to a fragmented regime for criminal cooperation and the protection of personal data, thus impacting the effectiveness of the Protocol.

9. Along the same lines, the Committee of Convention 108 notes the full opt-out possibility (in point 9.a of the draft text) for Parties not to apply the direct disclosure regime. Due to the fragmentation that is likely to arise from the variability of regimes, the "[high] expectations set for the new Protocol", in that it "will need to stand the test of time in order to make a difference in terms of an effective criminal justice response with human rights and rule of law safeguards" (T-CY discussion guide for the upcoming 2019 Octopus Conference, *in fine*), may not be met. If introduced at all, any new direct disclosure regime should be sufficiently straightforward and binding for all ratifying Parties, sustainably building on a common commitment to shared data protection conditions, safeguards or principles (*infra*, under points 6 and 7).

10. The Committee of Convention 108 favours a mandatory notification regime instead of the optional notification possibility foreseen under point 5.

3. Giving effect to orders from another Party for expedited production of data

11. Whilst the explanatory report to paragraph 4 of the proposed text on traditional orders for expedited production of data (page 28, point 5.2, para 14) rightly points out that "under some Parties' domestic laws, the production of traffic data may require further information because there are additional requirements in their laws for obtaining such data", the Committee of Convention 108 questions the position that the only consequence thereof is that "additional information may need to be provided to the requested Party in order for it to give effect to the order". The possibility of an opt-out from the regime as far as traffic data is concerned, as foreseen in paragraph 12 of the proposed text, is equally insufficient.

12. The Committee of Convention 108 believes that the mere reference to potentially higher domestic standards or the opt-out possibility for Parties in relation to obtaining traffic data does not adequately capture the principled and historical distinction the Budapest Convention has made between measures relating to subscriber data vs. measures relating to traffic data. The Committee of Convention 108 believes that such principled distinction should not be sacrificed for alleged reasons of efficiency.

13. Even more fundamentally, and in line with its provisional answers to the discussion paper for the 2018 Octopus Conference, the Committee of Convention 108 takes the position that, as a minimum requirement, a Protocol regime for disclosure of traffic data should allow for the combined data protection, procedural and rule of law safeguards of at least the Party of the requesting competent authority and the Party where the data subject was present whilst using the targeted service(s), if different from the requesting Party or the Party where the service provider is present. A person who is communicating or using services in a Party's territory has a legitimate expectation of privacy under primarily the laws of that Party. As soon as it is possible to establish, based on the prior obtaining of subscriber data, where a person was while using any targeted service(s), it is key for the Protocol to make sure that the data protection, procedural and rule of law safeguards of the latter Party may be applied and complied with. If that Party is the Party where the order originates from, such assurance is implied already. Only in such case, the Protocol may suffice allowing for the combined data protection, procedural and rule of law safeguards of at least the Party of the requesting competent authority and the Party where the service provider [or executing competent authority] is located (as in para 27, *infra*). The Protocol should moreover contain specific provisions which would guide Parties in case of conflict of laws, in that the laws offering the widest protection to the data subject will apply.

4. Insufficient criteria for determining territorial 'presence' of a service provider

14. Both the suggested direct disclosure and traditional cooperation mechanism pertain to the obtaining of data from service providers in another Party's territory. The related draft explanatory report to both mechanisms (respectively in paragraph 10 page 18 and paragraph 5 page 26) reads as follows:

> "[T]he term 'a service provider in the territory of another Party' requires that the service provider be physically present in the other Party. Under this Article, the mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not constitute the service provider being 'in the territory' of that Party. Paragraph 1 requires, in addition, that the data be in the service provider's possession or control."

15. The Committee of Convention 108 insists that further clarification be added, ideally in the text of the draft articles themselves, if not at least in the corresponding parts of the explanatory report, on when a service provider will be considered 'physically present' in a Party's territory. Against the back-drop of the significant jurisprudential contention in the past decade around jurisdiction over service providers abroad, in which a multitude of criteria (a range of 'establishment' criteria, 'offering' criteria etc.) has passed in review, the above two criteria (negatively: that a contractual relationship does not suffice; positively: that data must be in the service provider's possession or control) seem insufficient to bring optimal clarity. The Committee of Convention 108 finds such clarity crucial in order for any future mechanism not to be undermined as well as to avoid forum shopping by authorities/Parties (which would be avoided if mandatory common safeguards were to be incorporated in the Protocol). Not only may the latter confront multinational service providers with parallel orders issued to its establishments or branches in several jurisdic-

tions, it may also encourage authorities/Parties to opt for sending orders to the jurisdiction of presence of the service provider where the lowest data protection standards apply. The Committee of Convention 108 sees relevance in adding more clarity, e.g. by stipulating in the Protocol or in the explanatory report that a service provider will be considered 'physically present' in a Party's territory when it has a stable infrastructure through which it actually pursues an economic activity for an indefinite period and from where the business of providing services is carried out or managed.

5. Confidentiality

16. The explanatory report to paragraph 4.f of the envisaged article on disclosure of subscriber information (page 19, point 4.2, para 17) clarifies that the "special procedural instructions" that need to accompany a disclosure order submitted to service providers are meant to "cover, in particular, any request for confidentiality, including a request for non-disclosure of the order to the subscriber or other third parties". Even if the Committee of Convention 108 sees no difficulty with this, it does however request reconsideration of the opening left in the further explanation given for domestic laws or discretionary policies of service providers that would not guarantee the confidentiality sought ("Therefore, in order to avoid the risk of premature disclosure of the investigation, Parties are encouraged to be aware of applicable law and a service provider's policies concerning subscriber notification, prior to submitting the order under paragraph 1 to the service provider"). Whilst confidentiality may be important to maintain efficiency in criminal investigations, it may equally be vital in safeguarding data protection. The Committee of Convention 108 therefore favours the inclusion of a self-standing provision on confidentiality in the Protocol, for which it suggests inspiration is drawn from:

> Article 26.2 of the Budapest Convention (ETS 185): "Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them";
>
> Article 27.8 of the Budapest Convention (ETS 185): "The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed";
>
> Article 25 of the Second Additional Protocol to the Convention on MLA in criminal matters (ETS 182): "The requesting Party may require that the requested Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting Party".

17. The explanatory report to the envisaged article on traditional orders for the expedited production of data (page 26, point 5.2, para 8) clarifies that "[u]nder paragraph 3.c, the request should also include all special instructions, including for example requests for certification or confidentiality under Article 27.8 of the Convention, at the time of transmission to ensure the proper processing of the request". Whilst the Committee of Convention 108 sup-

ports the reference to confidentiality and to Article 27.8 of the Budapest Convention, it stresses that, from the draft T-CY text as it stands, it cannot be derived that Article 27.8 of the Budapest Convention applies in a Protocol context. The reference, however, underlines the importance, stressed above by Committee of Convention 108, that a self-standing provision on confidentiality be included in the Protocol itself, for both the direct and the traditional mechanism for obtaining information from service providers.

6. Data protection conditions and safeguards

18. In the absence of a draft text for the envisaged article on data protection (*supra*, under para 6), the Committee of Convention 108 raises particular concern regarding the non-insertion in the draft text and explanatory report as they stand of two-directional data protection conditions, including for asymmetrical transfers under the direct disclosure of subscriber information regime (point 4 of the T-CY draft), but equally for traditional MLA to giving effect to orders for expedited production of data (point 5 of the T-CY draft).

19. The Committee of Convention 108 stresses the importance of making sure, at least, that data protection conditions and safeguards be inserted in the Protocol, applicable in two directions, since the receiving entity may be:

- either a competent authority:
  - in the case of traditional MLA: both the requesting and requested authority being the recipient of personal data, i.e. of the personal data provided in the request or of the personal data transferred as a result of the execution of a request;
  - in the case of direct, asymmetrical transfers: the requesting authority being the recipient of personal data transferred by a private data controller (service provider);
- or a private data controller (service provider), which, in the case of direct, asymmetrical transfers is the recipient of personal data provided in the request.

20. The draft text and explanatory report as they stand, remain silent on the matter, save for a double reference in the explanatory report to paragraph 2 of the proposed draft text on direct, asymmetrical disclose of subscriber information (page 18, point 4.2, para 11), and a single reference in the explanatory report to paragraph 8 of the draft article on expedited production of data between traditional authorities (page 29, point 5.2, para 19 and 20). The three references are exclusively targeted at "parties that have data protection requirements" (first two) or would wish to limit or refuse cooperation based on "conditions and safeguards (including with regard to data protection)" (third). The first reference is only a reminder to parties having data protection requirements of their obligation under domestic laws to provide "a clear basis for the processing of personal data" by service providers in response to an order which they directly received. The second reference relates to international data transfers, without, however, stipulating the actual safeguards that a service provider may require (from the recipient Party or authority) to be able to transfer "responsive subscriber information". In contrast, the explanatory text only features a blank cross-reference to a future article on data protection, whilst axiomatically stating that (a Party's implementation law for) the Protocol reflects the "important public interest" of the direct cooperation regime (discussion continued *infra*, under para 20). The framing of the third reference is of concern: the explanatory report (page 29, point 5.2, para 20) warns that "mutual assistance is in principle to be extensive, and impediments thereto strictly limited", so that "accordingly, conditions and refusals should also be limited in line with the objectives of this Article to eliminate barriers to transborder sharing of subscriber information and traffic data and to provide more efficient and expedited procedures than traditional mutual assistance". The Committee of Convention 108 considers

that labelling data protection conditions and safeguards as potential 'impediments' and 'barriers' is inappropriate and does not reflect the balanced functioning of democracies safeguarding human rights and the rule of law. It is furthermore not in line with the case-law of the European Court of Human Rights. It believes – based on tangible experiences – that the efficiency of cooperation would be genuinely enhanced when embedded in a shared commitment to respect common data protection principles.

21. In claiming that the envisaged direct disclosure regime in the Protocol reflects an "important public interest" (*supra*, under 19), the T-CY proposal seeks to base the entire direct disclosure concept exclusively on the derogations provided in Article 14.4.c of Convention 108+ and, as far as EU Member States are concerned, in Articles 49.1(d) *juncto* 49.4 GDPR [emphasis below added]

> *Article 14.4 Convention 108+ – Transborder flows of information*
>
> Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if: [...] c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; [...].
>
> *Article 49 GDPR – Derogations for specific situations*
>
> 1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: [...] (d) the transfer is necessary for important reasons of public interest; [...].
>
> 4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

22. In line with its provisional answers to the discussion paper for the 2018 Octopus Conference and the recent expert note (document T-PD(2019)3), the Committee of Convention 108 disagrees firmly with the above approach, and opposes the envisaged structural and systemic reliance on derogations as a standardised means to allow for direct, asymmetrical transfers.

23. The Committee of Convention 108, in contrast, reiterates its position that the most straightforward, sustainable and widely acceptable way to guarantee an appropriate level of data protection under the Protocol would be the accession by the Protocol Parties to Convention 108+. As a result, an appropriate level of data protection would be generically guaranteed by all Parties to the Protocol and indirectly become a default standard also for the application amongst them of the Budapest Convention itself.

24. In a subsidiary manner, i.e. where the option of accession by the Protocol Parties to Convention 108+ (*supra*) does not prove feasible, the Committee of Convention 108 favours the incorporation in the Protocol (as a legally binding instrument between the Parties) of common mandatory data protection safeguards [list as included *infra*, under point 7], grounded in, closely aligned with and consistently interpreted in line with Convention 108+.

25. In an even more subsidiary manner and as an absolute minimum, the Committee of Convention 108, in line with the recent expert note (document T-PD(2019)3), urges the T-CY to take Article 26 (pertaining to "Data protection") of the Second Additional Protocol to the Convention on MLA in criminal matters (ETS 182) as a point of departure, thus ensuring consistency with at least the Council of Europe's data protection *acquis* in the context of judicial cooperation in criminal matters. This would imply insertion in the Protocol (as a legally binding instrument between the Parties) of an optional regime, comparable with that of Article 26.3, 2nd indent of ETS 182:

> "Any Party may refuse to transfer personal data obtained as a result of the execution of a request made under the Convention or any of its Protocols where [...] the Party to which the data should be transferred is not bound by [Convention 108+], unless the latter Party undertakes to afford such protection to the data as is required by the former Party",

which would need to be rephrased so as to enable two-directional applicability, both in the context of direct transfers and transfers between traditional competent authorities.

26. Further, in case the Protocol Parties were not all to accede to Convention 108+ or no new, mandatory data protection conditions and safeguards were to be inserted in the Protocol, the Committee of Convention 108 suggests, in order to enable and ensure (and if necessary: enforce) compliance by private data controllers (service providers) with the data protection conditions and safeguards in the Protocol (i.e. a public international law instrument, incapable of directly binding private parties), to stipulate in the latter that if a data controller or competent authority of a Party requires an appropriate level of data protection in the receiving Party, such condition shall be considered to be met if:

> "the receiving competent authority or data controller of the latter Party undertakes to process the personal data transferred subject to the conditions and safeguards under the domestic law of the former Party [i.e. the Party from where personal data would be transferred], including obligations upon the latter under Convention 108 and its Protocol and/or other applicable bilateral, regional or international data protection agreements or instruments guaranteeing the protection of individuals by the implementation of at least the following safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+ [list as included *infra*, under point 7]".

27. In doing so, as a minimum requirement, as posited also in the provisional answers to the discussion paper for the 2018 Octopus Conference and the recent expert note (document T-PD(2019)3), a Protocol regime for disclosure of subscriber data should allow for the combined data protection obligations of at least the Party of the requesting competent authority and the Party where the service provider or executing competent authority is located. This would also be seen as a step forward into international harmonisation of data protection requirements in the field of criminal justice cooperation.

28. Since an undertaking as above lacks the "legally-binding and enforceable" character of safeguards as required under Article 14.3.b of Convention 108+, the Committee of Convention 108, in line with the expert note (document T-PD(2019)3), further suggests to introduce an additional obligation in the Protocol for Parties to stipulate in their domestic legislation that violations of such undertaking by a receiving competent authority or data controller in their territory may give rise to all judicial and non-judicial sanctions and remedies available under their laws.

29. The Committee of Convention 108 notes that, whilst paragraph 1 of both of the draft articles on direct and traditional, expedited ordering of information limits the issuing of orders to information which is needed for the issuing Party's specific criminal investigations or proceedings, the draft text remains fully silent on the purposes for which transferred personal data can be used by the receiving competent authority or service provider. The Committee of Convention 108 furthermore recommends in this regard to include explanations at least in the Explanatory Report on a commonly agreed distinction between data processing (including transfers) for criminal investigation purposes and those undertaken for national security purposes in line with the Issue paper "Democratic and effective oversight of national security services" published by the Commissioner for Human Rights of the Council of Europe.

30. The Committee of Convention 108 requests that clear use restrictions be inserted in the Protocol, applicable to both direct and traditional, expedited cooperation. It suggests to phrase such use restrictions based on the provisions of Article 26 of ETS 182 (*supra*), amending them *mutatis mutandis* and extending them to also cover use limitations upon a service provider to which a request is transferred. This could translate in three provisions, in which it is stipulated respectively that:

1. [*mutatis mutandis* adaptation of Article 26.1 ETS 182] personal data transferred by a competent authority or data controller of a Party as a result of the execution of an order issued under the Protocol by a competent authority of the receiving Party, may be used by the latter only:

   a. for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence within the scope of articles 14.2 and 25.1 of the Budapest Convention;
   b. for other judicial and administrative proceedings directly related to the proceedings mentioned under (a);
   c. for preventing an immediate and serious threat to public security;

2. [*mutatis mutandis* adaptation of Article 26.2 ETS 182] such data may however be used by the competent authority for any other purpose if prior consent to that effect is given by either the Party from which the data had been transferred, or the data subject[1].

[1] If solely addressed from a data protection perspective, the consent of the data subject ought to be avoided as a ground for data processing in the context of judicial and law enforcement cooperation in criminal matters. However, it should be stressed that the possibility of reliance on the consent of the person concerned is formally part of the contemporary *acquis* of MLA in criminal matters, both at Council of Europe (Article 26.2 ETS 182) and EU level (Article 23.1, under (d) of the EU MLA Convention of 29 May 2000, which was not abrogated from by the European Investigation Order Directive). It is actually the case that the possibility to rely on consent of the person concerned functions here as an extra guarantee for that person in the context of the so called specialty principle (which is the traditional correlative of the purpose limitation principle in data protection law). The specialty principle traditionally has a trust function: the requesting sate or authority ought not to use data for other purposes than the initial purposes, so as not to betray the trust put in it by the executing state or authority in sending the data concerned for those initial purposes. Since the requested state or authority might have refused cooperation or data transfer for other than the initial purposes, the specialty principle stipulates that additional consent of the executing state or authority must be sought in case of intended use beyond the initial purposes (comparable with the control principle in data protection law). To allow for consent of the data subject as a basis for further use could be supported in the very context of use restrictions in the future Protocol regime.

3. [extension to cover use limitations for service providers] the request received and the information it contains can only be used by the receiving service provider for the purpose of the execution of an order issued under this Protocol.

7. Substantive data protection principles

31. To the extent that the option of accession by the Protocol Parties to Convention 108+ (*supra*, under para 22) does not prove feasible, the Committee of Convention 108 urges that the below safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+, would be incorporated in the Protocol as mandatory common safeguards. In an even more subsidiary manner, the Committee of Convention 108 urges that, as an absolute minimum, the Protocol allows service providers or competent authorities to require, as a precondition before transferring any personal data, the receiving competent authority or service provider to undertake to process the personal data transferred subject to the conditions and safeguards under the domestic law of the Party from where personal data would be transferred, guaranteeing the protection of individuals by the implementation of at least the following safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+ [allowing flexibility as to possible re-ordering, clustering etc.]:

a. purpose legitimacy, purpose specificity and purpose limitation;
b. lawfulness;
c. fairness and transparency;
d. necessity for and proportionality to the legitimate purpose pursued;
e. non-excessive data processing and data minimisation;
f. adequacy, relevance and accuracy of data;
g. data retention limitation;
h. accountability of controllers and processors;
i. logging, data security and data breach notification duty;
j. information security
k. specific, additional safeguards for special categories of sensitive data;
l. lawful use of exceptions and derogations;
m. enforceable data subjects' rights and effective administrative or judicial redress;
n. appropriate protection in (onward) data transfers;
o. effective independent oversight.

31. Finally, the Committee of Convention 108 stresses the importance of the effectivity of the data protection safeguards and ensuring that Parties to the Second additional Protocol effectively apply and enforce them in practice. The Committee proposes that an evaluation of the implementation of the data protection safeguards be carried out, possibly relying on the findings and recommendations of the mechanism introduced in Article 4.3 of Convention 108+ for Parties to Convention 108+, and, for other countries, on Article 23.f of Convention 108+. The articulation of the work of the T-CY and of the Committee of Convention 108+ in that regard should be further examined.

vodafone NL 4G 17:30 49%

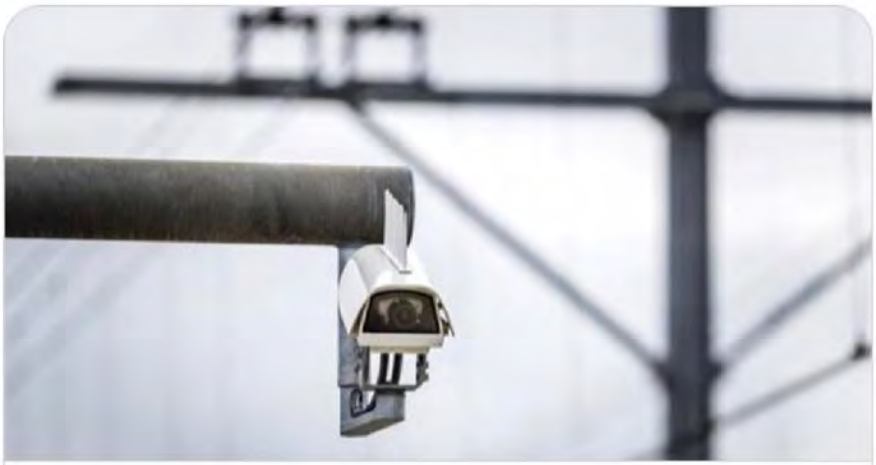
Kathalijne Buitenweg
2.235 Tweets

Tweets | Tweets en antwoorden | Media | I

Kathalijne Buitenweg @kathal... · 2d

Die leuke foto van je dochter op Facebook,
of van je vriendengroep op Twitter,
blijkt te worden gebruikt door de politie.
Om mensen te kunnen herkennen op camerabeelden.
#Clearview In strijd met de wet.

Net vragen gesteld aan @Grapperhaus.



Omstreden gezichtsherkenningsprogramm
nos.nl

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

30 September 2020

T-PD(2020)03rev

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

CONVENTION 108

Facial Recognition

Draft Guidelines

Directorate General of Human Rights and Rule of Law

Contents

Facial recognition is a biometric face recognition technology, based on algorithms that learn to recognise the unique features and characteristics of faces in order to identify or authenticate them.

Facial recognition has rapidly evolved from being a technological novelty to an ever more common feature in our daily lives. Facial recognition technologies are advancing rapidly, and algorithms are becoming more and more accurate.

For Cicero, the face was the mirror of the soul[1]; he was thus underlining the close link between an image (today in the form of a computer template) and the deepest intimacy of the person. The sensitivity of information of a biometric nature was specifically recognised with the inclusion of data uniquely identifying a person under the special categories of data in Article 6 of the modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data[2] (hereinafter "Convention 108+").

The uses of this technology are varied and numerous, some of which may seriously infringe the rights of data subjects. In order to prevent such infringements, the Parties to Convention 108 shall ensure and permit that the development and use of facial recognition respect the right to privacy and the protection of personal data, thereby strengthening human rights and fundamental freedoms.

These guidelines[3] provide a set of reference measures that governments, facial recognition developers, manufacturers, service providers and user organisations should apply to ensure that this technology does not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data.

.

The guidelines are general in scope and do not exclude further details in the legal framework depending on the case of use.

Nothing in these guidelines should be interpreted as excluding or limiting the provisions of the European Convention on Human Rights and Convention 108. These guidelines also take into account the new safeguards provided by Convention 108+

I. GUIDELINES FOR LEGISLATORS AND DECISION-MAKERS

1. Legal basis

a. Strict Limitation by law of certain uses

[1] In *Oratore*, III, 22
[2] Amending Protocol CETS 223 to Convention 108
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
[3] These Guidelines are based on a 2019 report by Sandra Azria and Frédéric Wickert "Facial recognition: current situation and challenges", available at https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1

As provided for by Article 6 of Convention 108+, the processing of special categories of data, such as biometric data, shall be authorised only if such processing relies on an appropriate legal basis and complementary and appropriate safeguards are enshrined in law. These safeguards shall be adapted to the risks involved and to the interests, rights and freedoms to be protected, applied alone or cumulatively.

Despite the precautions provided for in the legislation applicable to facial recognition, and in particular Convention 108+, it appears that its use should in some cases be strictly limited by national laws, or even prohibited where the democratic process led to that decision.

For example, facial recognition for the sole purpose of determining a person's skin colour, religion, sex, origin, age or health condition should be strictly limited, for instance for a medical research project subject to appropriate safeguards enshrined in law.

Similarly, affect recognition is a sub-category of facial recognition that claims to detect aspects such as personality, inner feelings, mental health and workers' engagement from images or videos of faces. Linking recognition of affect to hiring of staff, access to insurance, education and policing may pose risks of great concern, both at the individual and societal levels, and would require careful consideration and safeguards enshrined in law to be authorised..

In addition, many national laws[4] prohibit such processing as a principle. They may be implemented, by way of exception, only in certain specific cases (*e.g.* with the express consent of individuals, to protect their vital interests or on the basis of an overarching public interest) and following safeguards that are appropriate to those risks.

In any event, the necessity of the use of facial recognition technologies will have to be assessed together with the proportionality to the purpose and the impact on the rights of the data subjects.

Without judging the ethical level of different cases of use, they should be categorised, and a legal framework should be in place in respect of facial recognition. The legal framework should determine, according to each different use:

- the detailed explanation of the specific use and the specific purpose;
- the minimum reliability of the algorithm: minimum reliability percentage;
- the retention duration of the photos used for identification;
- the possibility of auditing these criteria;
- the traceability of the process

The legal framework should also set a clear set of rules on developing, deploying and providing facial recognition technology.

2. c. Quality of the consent

Depending on the purpose, particular attention must be paid to the quality of the data subject's explicit consent if it is the legal basis for the processing. Such consent furthermore has to be free, specific and informed according to Article 5 of the Convention 108+. Consent should not be the legal ground used for facial recognition performed by public authorities. Other uses may be similarly incompatible with relying on the consent as a legal basis.

In order to ensure that consent is freely given, data subjects should be offered alternative solutions to the use of facial recognition technologies (for example, using a password or an identification

[4] Article 9 of the European Union General Data Protection Regulation (GDPR)

badge) but also ensure that the said alternative solution be easy to use as, if it appeared to be too long or complicated compared to the facial recognition technology, the choice would not be a genuine one.

If consent is given for one specific purpose, there should be no other use for a second purpose without consent. Similarly, in case of transfer of data to a third party, such transfer should also be subject to specific consent.

d. Other legal basis

For public authorities

Law Enforcement Agencies for the purpose of crime prevention and investigation etc. (public places)

Other public authorities (overriding public interest)

For private companies,

Clearview scenario // comment Slovakia
(what should be the source of facial recognition data? Is it possible to use pictures available online (in the context that people make them manifestly publicly available – art. 9 (2) (e) GDPR) or the "original" datasets need to be acquired in line with data protection rules?)

Private Spaces: possibility of security of the places as a legitimate interest?

Quasi-public spaces (shopping malls/ open gardens managed by private security companies)

Public spaces:

~~3.~~ 2. Necessary involvement of supervisory authorities

In compliance with Article 15(3) of Convention 108+, supervisory authorities are to be consulted on proposals for any legislative or administrative measures implying the processing of personal data by facial recognition technologies. It seems desirable to systematically involve the supervisory authorities and, in particular, to consult them on any possible experimentation or deployment foreseen by any controller.

These authorities could thus be consulted systematically and in advance on envisaged projects in order to shed light on the protection of the data of data subjects. Similarly, they should have access to the impact assessments carried out and also to all audits, reports and analyses carried out in the context of these experiments.

~~4.~~3. Certification

The setting up of independent and qualified certification mechanisms for facial recognition and data protection to demonstrate full compliance of the processing operations carried out, would be an important element in building user confidence.

Such a certification could be implemented at various levels depending on the field of application of artificial intelligence: one level to categorise types of structures (algorithm creator, algorithm integrator, etc.), one level to categorise types of algorithms (computer vision, language: sentence understanding and generation, intelligent search, etc.) and one level to categorise uses (critical or non-critical, for example).

~~5.~~4. Raising awareness of Data Subjects

.

The awareness of data subjects and understanding of the general public of facial recognition technologies should be actively supported through accessible and educational actions.
The idea is to give access to simple concepts that could alert the data subjects before they decide to use a facial recognition technology, to understand what it means to use sensitive data such as biometric data, how facial recognition works: and to alert to potential dangers in case of misuse.

II. GUIDELINES FOR DEVELOPERS, MANUFACTURERS AND SERVICE PROVIDERS

1. Data and algorithm quality

a. Representativeness of used data

Like other applicable regulations, GDPR Article 5 of Convention 108+ provides for a data accuracy requirement.

Therefore, developers or manufacturers of facial recognition tools but also user organisations will have to take steps to ensure that facial recognition data are accurate, in particular to avoid mislabelling, by sufficiently testing their systems and identifying and eliminating significant disparities in accuracy, notably with regard to demographic variations in skin colour, age and gender, and thus avoid unintended discrimination.

Furthermore, in order to ensure both the quality of the data and the efficiency of the algorithms, the algorithms will have to be developed using datasets based on a sufficiently diverse photos of men and women, of different skin colours, different morphology, of all ages and from different camera angles.

Back-up procedures should be provided for in case of system failure if the physical characteristics do not correspond to the technical standards.

Biometric data unnecessarily but unavoidably revealing other sensitive data such as information on a type of illness or physical disability will also be subject to appropriate safeguards.

b. Data life duration

A facial recognition tool requires periodic renewal of data (the photos of faces to be recognised) in order to train and improve the algorithm used.

On the other hand, each algorithm has a percentage of recognition reliability during its development and use. It seems therefore important to date and record this percentage in order to monitor its evolution. Should its reliability deteriorate, it will be necessary to renew the training photos and therefore ask users again to provide photos. This will also enable to protect from the consequences of changes in the shape of faces (due to ageing, to accessories (piercing or other), to accident modifying part of the face, etc.).

These reliability percentage records (global for the algorithm and specific for the user) should be easily available to users in the form of a dashboard for example.

2. Reliability of the tools used

The reliability of the tools used depend on the effectiveness of the algorithm. This effectiveness relies on different factors: false positives, false negatives, performance in different lights, reliability when faces are turned from the camera, impact of face coverings, etc.

The highest possible level of reliability should be ensured considering that the use of a facial recognition system might result in adverse consequences for the individual.

3. Awareness and traceability

Companies developing and selling facial recognition technology software should endeavour to take reasonable steps - such as making recommendations and providing advice - to help organisations or companies [entities ?] using their facial recognition technology to apply transparency and respect for privacy (by providing companies with a sample language for signage of physical locations or mention in their privacy policies, by recommending clear, easy-to-understand signage that states whether facial recognition technology is deployed in a specific space).

Moreover, in addition to this information on the use of this technology, companies developing and providing facial recognition technology software should provide for information to ensure that the data subject is fully informed, while of course respecting business secrecy.

4. Precautionary approach

- Companies developing and providing facial recognition technology software should: integrate privacy protection into the design and architecture of facial recognition products and services, as well as into internal IT systems and the use of dedicated tools, including for example the possibility to provide a local or decentralized face recognition architecture instead of a centralized architecture;

- implement an internal review process designed to identify and mitigate potential privacy risks in products and services that use facial recognition technology before they are made available or deployed;

- integrate such an approach into their organisational practices, including for example, assigning dedicated staff, providing privacy training to employees, and conducting privacy analyses upon the development or modification of facial recognition products and services.

III. GUIDELINES FOR ENTITIES USING FACIAL RECOGNITION TECHNOLOGIES

1. Limitations on use - Proportionality

Entities using facial recognition technology have to demonstrate that the use of facial recognition is necessary and proportionate in the context and that it doesn't interfere unduly with the rights of the data subject.

Entities using facial recognition technology should consider how this use will impact both those who voluntarily use facial recognition technology and those who come into contact with facial recognition products or services.

For example, when facial recognition data is used to match a person's facial print to a set of registered user credentials, the entity should remove all data from the facial recognition template as soon as possible in the event of a non-compatible result.

In addition, the choice of a verification or identification function[8] depends very much on the intended purpose of the facial recognition system and on the circumstances in which it will be used. The instrument must thus serve the purpose for which the data was collected and not be unnecessarily oversized. Therefore, when a verification system also appears possible, the choice of an identification system will require a specific justification.

Finally, the particularity of biometric data for facial recognition is that they often contain more information than is necessary for the verification or identification of persons. Excessive data processing shall be avoided by limiting the storage and use of data. The system must therefore be designed in such a way that the data obtained reveal only the information necessary for its purpose.

Moreover, to avoid the transfer of data to third parties or public dissemination of data (e.g. on social networks), technical and legal means should be identified to avoid other uses than those initially intended. Such measures may include technical degradation of individual images, limitation of automated access to relevant databases and the creation of contractual obligations for partners to respect the legal framework.

2. Data security

Any failure in data security may have particularly serious consequences for data subjects, as unauthorised disclosure cannot be corrected, for example by changing a password.

Strong security measures, both at technical and organisational level, should therefore be implemented to protect facial recognition data and image sets against loss and unauthorised access or use during collection, transmission and storage. Reasonable security should include data encryption, the use of 'cancelable` biometrics and a combination of virus protection, access controls, employee training and other high standards security practices. [++]

Any breach of this obligation should be notified to the supervisory authority and, where appropriate, to the data subjects.

Security measures should evolve over time and in response to changing threats and identified vulnerabilities and should also be proportionate to the sensitivity of the data, to the context in which facial recognition technology is used and its purposes, to the likelihood of harm to individuals and other relevant factors.

Strict retention and disposal practices for facial recognition data, with the shortest possible retention periods should also be defined and applied.

3. Transparency

One of the greatest risks raised by the use of facial recognition is that it can be carried out without the data subject's knowledge.

It is therefore essential to subject such use to a real and effective transparency (Article 8 Convention 108+) with a view to ensuring legal protection.

[8] Verification / identification

The factors that will determine whether transparency is secured include, for example, the information given to individuals, the context of the collection, reasonable expectations as to how the data will be used, whether facial recognition is merely a feature of a product or service and not an integral part of the service itself, and how the collection, use or sharing of facial recognition data is likely to affect individuals, especially when used with persons in vulnerable situations. In particular, it also has to be stated which rights and legal remedies the data subjects are entitled to.

A privacy policy on facial recognition or informational material could include, in addition to the information provided for in Article 8 of Convention 108+, the following information[9]:

- . whether and to which extent facial recognition data can be transmitted to third parties (see below about full identification of third party contractual partners who receive the data in the course of providing the product or service);
- . the retention, deletion, de-identification or re-identification of facial recognition data;
- . the choices of the persons at their disposal regarding their facial recognition data;
- . contact points available for individuals to ask questions about the collection, use and sharing of facial recognition data;
- . full identification of the third-party contractual partners who receive the data in the course of providing the product or service;
- . when collection, use and sharing practices change significantly, companies should update their privacy policy or publicise these changes in light of the context of the change and its impact on individuals.

Transparency reports could be published on a regular basis which will include…

4. Impact analysis and risk assessment

A risk assessment of the potential impact of the processing on fundamental rights and freedoms is necessary to balance the protection of these rights with the different interests involved in the use of facial recognition.

Both public authorities and private companies or other bodies should adopt a precautionary approach based on appropriate prevention and risk mitigation measures, and be required to carry out systematic assessment of existing facial recognition tools, measuring their potential impact on human rights, taking into account the nature, context, scope and purpose of the system. Such analyses should not, of course, be limited to identifying risks, but offer effective significant mitigation solutions.

Where a public authority has not yet acquired or deployed a facial recognition system, this assessment should be carried out prior to the acquisition and/or development of the tool and should be made public. In addition, public authorities should require any potential provider to lift any restrictions on the exchange of information if this has a limiting effect on the impact assessment.

[9] On this point, see the recommendations by Future Privacy Forum "Privacy Principles for Facial Recognition Technology in Commercial Applications" https://fpf.org/2018/09/20/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/

The impact assessment could be carried out either by an independent monitoring body or by an auditor having relevant expertise to help find out, measure or map out impacts and risks over time. The impact assessment should be conducted as openly as possible and with the active engagement of affected individuals and groups.

Such impact assessments should be carried out at regular intervals.

If a risk is identified, the bodies concerned should be able to refer to any existing ethics committees, and to the competent supervisory authorities to examine the human rights risks.

Finally, for the implementation of any new project, this approach should be combined with a "privacy by design and privacy by default" approach, as provided for in point II.

5. Accountability

Accountability and vigilance are central to ensure that practices comply with the legal framework:

- user organisations will be required to implement transparent policies, procedures and practices to ensure that the principles to protect the rights of the data subjects underlie their use of facial recognition technologies;

- this includes implementing training programmes and audit procedures for those in charge of processing facial recognition data;

- it would also be useful to consider setting up internal review committees to assess and approve any processing involving facial recognition data;

- these principles should be contractually extended to third party service providers, business partners or companies using facial recognition technology and thus deny access to third parties that would not comply with them;

- the use of facial recognition by public authorities in particular could be subject to minimum levels of performance in terms of accuracy, especially where public security purposes are concerned;

- similarly, with regard to the public sector, which is already involved in the use of facial recognition, it would be useful to provide for specific transparency and prior evaluation constraints in public procurement procedures with suppliers of facial recognition tools.

6. Ethical framework

To follow the logic as exposed above, giving an ethical framework to the use of this technology seems to be a crucial issue. Indeed, regulation is essential, but companies also "need an internal accountability structure that goes beyond ethical guidelines.[10]" This could take the form of external ethics advisory boards that could carry out audits and publish the results of their research.

Furthermore, in order to avoid human rights abuses, conventions of experts from different fields of expertise would be likely to define the most potentially dangerous cases when using facial recognition technology.

[10] IA NOW 2018 - Report

On this topic, whistleblowers have also an important role to play and employees of companies or organisations developing or using these solutions should be able to benefit from an appropriate protection status, as provided for in particular in Recommendation (2014)7 on the protection of whistleblowers[11].

IV. THE RIGHTS OF DATA SUBJECTS

As facial recognition is based on the processing of sensitive data, all the rights provided for by Article 9 of Convention 108+ are guaranteed to the data subjects, such as the right of access, the right to object, the right to rectification, the right not to be subject to a fully automated decision, etc.

The Explanatory Report to Convention 108+ rightly emphasises that "human dignity requires the establishment of safeguards when processing personal data, so that individuals are not treated as mere objects."

Where the use of facial recognition technology is intended to enable a decision to be taken solely on the basis of automated processing which would significantly affect the data subject, the latter must in particular have the right not to have such processing carried out without his or her views being taken into account.

Data subjects also have the right to know the reasoning underlying the processing operations on data concerning them, which should include the consequences of that reasoning.

Data subjects shall have the right to object at any time, on grounds relating to their situation, to facial recognition processing unless the controller demonstrates legitimate grounds for processing which override their interests, rights and fundamental freedoms.

Supervisory Authorities will cooperate with each other where necessary for enhancing effective mechanisms.

[11] See https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c5ea5

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

12 August 2020

T-PD(2019)07BISrev3

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

CONVENTION 108

Profiling and Convention 108+: Suggestions for an update of Recommendation 2010(13) on profiling

Directorate General of Human Rights and Rule of Law

Contents

Two preliminary remarks:

1. **The number of texts published since the drafting of the recommendations (more than one year and a half ago) –**
   a. **At the EU level:**
      - **The EU HLGE 'Ethics Guidelines for trustworthy AI'**
      - **'WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust';**
      - **EDPB guidelines 8/2020 on the targeting of social media users;**
      - **"PROPOSAL FOR A RESOLUTION FROM THE EUROPEAN PARLIAMENT containing recommendations to the Commission concerning a framework of ethical aspects in artificial intelligence, robotics and related technologies**
   b. **At the UNESCO level, the Ad Hoc Expert Group preliminary report on first draft of the Recommendation on the Ethics of Artificial Intelligence**
   c. **At the CoE level: Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems'**

      AND the setting up of the CAHAI Committee (The Committee (CAHAI) will examine the feasibility and potential elements on the basis of broad multi-stakeholder consultations, of a legal framework for the development, design and application of artificial intelligence, based on Council of Europe's standards on **human rights**, **democracy** and the **rule of law**.)

   What is important as regards these texts:
      - **AI as a global system referring not only to the algorithms used but also to big data and IoT devices**
      - **Underline that the collective risks raised by AI have to be addressed;**
      - **Confirm the need to take into account the category of High Risk systems;**
      - **Pinpoint the problem of the multiplicity of actors**

2. **CoE Recommendations are more than guidelines (strict application of the Convention 108+) but they constitute a non-mandatory text with prospective aspects envisaging how it should be and not how it must be and calling for improvements of the present regulation and their implementation by new legal texts**

Introductory note:

The authors of the report (Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling[1]), on the basis of the structure of Recommendation (2010)13 on profiling (adopted by the Committee of Ministers on 23 November 2010), propose in the present document the amendments and additions they consider necessary to maintain the relevance of the 2010 Recommendation in the light of technological developments, uses made of such technologies and new reference standards, in particular Convention 108+[2] . To be modified in order to underline the contribution of all national delegations and of certain civil liberties associations.

1. Definitions

1.1. for the purposes [of the present Recommendation]

a. The term «personal data» means any information relating to an identified or identifiable natural person (« data subject»). An individual isnot considered "identifiable" if identification requires unreasonable time, economic (IT.)resources or effort in relation to the means at the disposal of the controller.
b. The expression «categories of data processed» means the different types of personal or non-personal data used during the profiling processing, regardless of their source and nature.
c. The terms « processing », « controller » and « processor » refer to the definitions given by Convention 108+ in its Article 2. NOT NECESSARY ? I am not sure It would be a good opportunity to refer to the extended notion of "joint D.Cs" (see in particular the recent EDPB Guidelines on data sharing by social medias providers) and to insert a provision about reciprocal duties of all the participants to the AI chain (data suppliers, algorithms furnishers). Furthermore we need a special attention to data sharing operations (B2B but also B2G)
d. The term « profiling » refers to « *any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements* »
e. The term « profile » refers to *« a set of data characterising a category of individuals that is intended to be applied to an individual.* » FR: set of characteristics attributed to an individual.
f. The term « model » is a mathematical abstraction used (R) for instance in automatic learning methods, which provides a simplified description of the data to solve the task to be performed. GER:
g. Artificial intelligence (AI) refers to any « *set of sciences, theories and techniques whose purpose is to replicate by a machine the cognitive abilities of a human being*».GER / A.N. R: OK to take again the EU HLGE definition

[1] The Guidelines follow and build on the report "Profiling and Convention 108+ : Report on developments after the adoption of Recommendation (2010)13 on profiling" drafted by Yves Poullet, Honorary Rector of the University of Namur, and Benoit Frénay, Associate Professor at the Faculty of Computer Science, Namur Digital Institute, available at: https://rm.coe.int/t-pd-2019-07rev-eng-report-profiling/168098d8aa.

[2] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) adopted in Elsinore on 18 May 2018, available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e

h. The expression « machine learning processing » means processing using particular methods of artificial intelligence based on statistical approaches to give computers the ability to "learn" from data, i.e. to improve their performance in solving tasks without being explicitly programmed for each of them.IT
i. The expression « deep learning » means a set of automatic learning methods that attempt to model data with a high level of abstraction through articulated architectures of different non-linear transformations. IT R: we keep it
   i. A.*N.* "An automated decision-making system is "a system that uses automated reasoning to aid or replace a decision-making process that would otherwise be performed by humans [...] All automated decision systems are designed by humans and involve some degree of human involvement in their operation. Humans are ultimately responsible for how a system receives its inputs (e.g. who collects the data that feeds into a system), how the system is used, and how a system's outputs are interpreted and acted on."
   j. R: the last sentence is prescriptive and might be taken into consideration in the General principles.

j. The expression « online intermediary services » means information society services that enable users to deliver information (online research services), goods or services or to establish relations (social network access service).
k. The expression « high-risk profiling » refers to:

   i. profiling whose operations entail legal effects or have a significant impact on the data subject or on the group of persons identified by the processing;
   ii. profiling which, because of the target public or the context, involves a risk of manipulation of the data subjects; (PR. INT. difference between manipulation and marketing strategy. Suggestion: "includes profiling which, because of the target public or the context or the purpose of profiling, involves a risk of manipulation of the data subject"
   iii. profiling involving data qualified under article 6 of Convention 108+ as special categories of data or having for purpose to detect or predict them;
   iv. profiling performed by largely established online information services on the basis of the use made of their services for their own usage or for third parties usages. (UK too broad – See the recent guidelines for targeting users of social media)

2. General principles

2.1. The respect for fundamental rights and freedoms, notably the rights to human dignity (JPW) and to privacy and the principle of non-discrimination, but also the imperatives of social justice, cultural diversity and democracy, should (FR) be guaranteed during the processing of personal data subject to this recommendation. Profiling should (FR/GER)t contribute both to the well-being of individuals and to the development of an inclusive, democratic and sustainable society. (or UK "Profiling should not negatively impact the well being") R we prefer a positive formulation

2.2. Member states should encourage the design and implementation of procedures and systems in accordance with privacy and data protection, already at their planning stage (privacy by design) and during the whole duration of the processing (JPW) notably through the use of privacy-enhancing technologies. They should also take appropriate measures against the development and use of technologies which are aimed, wholly or partly, at the illicit circumvention of technological measures protecting privacy.

2.3. (According to the 4th recital of the Preamble of Convention 108+: *"Recalling that the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms,..."*) JPW, profiling must not result in discrimination against individuals, groups or communities. They may neither undermine the dignity of persons, nor democracy.

2.4. Profiling should not be carried out for the purpose of manipulating data subjects, including the manipulation of their choices or opinions (A.N.).

The use of automated decision-making systems should preserve the autonomy of human intervention in the decision-making process.At least when the data subject's consent is required, service providers and, in particular, intermediary services should give data subjects the possibility to opt in or OUT (ARG: see however the possibility 3.4 to invoke the legitimate interest? (R Yes but it is not the case. We are dealing here only with D.S. consent) as regards the profiling and the choice between the different profiling purposes or degrees. 1. JPW ' Prohibition except when it is mandatory or provided by the law' 2. AN: "[A para here would be important to recognise that there are areas in which profiling (by ADMs) should be prohibited – and then this can be mirrored in a recommendation later on." (R 1 and 2: to put elsewhere) 3. ARG: What about the consequence as regards the services obtained free of charge? R: The DS must be informed of the consequences of this or her choice and if a remuneration is proposed, that remuneration must be proportionate to the loss of benefits incurred by the DC

2.5. Member States should ensure that the regulation of profiling keeps it proportionate to the purposes pursued, to the nature and gravity of the risks incurred by the data subjects, the targeted groups or the general interest.

2.6. Profiling involves different actors whose quality and role must be analysed in order to determine their responsibilities.

2.7. The use of artificial intelligence technologies (see (R; OK A.N automated decision making systems based on 'deep learning' for profiling purposes poses an additional risk due to possible errors, biases and the difficulty of making the justifications for decisions taken or proposed transparent, and consequently to the full exercise of the rights of the data subjects. Their design, development and implementation require special and continuous attention with regard to the risks created and their assessment by multidisciplinary, independent teams.

3. Conditions for the processing of (personal) AN (R: OK) data in the context of profiling

A. Lawfulness

3.1. The processing of personal data in the context of profiling should be fair, lawful and proportionate, and for specified and legitimate purposes

3.2. Personal data used in the context of profiling should be adequate, relevant and not excessive in relation to the purposes for which they are collected or for which they will be processed.

In machine learning systems, it is difficult to know *a priori* which data will allow significant correlations and, moreover, it is important to limit the profiling to categories of data that the data subject can reasonably expect (legitimate expectations) to be taken into account in view of the purposes of profiling (as a negative example: profiling for housing access priorities that would take into account the consumption of soap operas on an online film platform(JPW/IT to be put in a footnote).

A.N: ". The objectives of machine learning systems should be scientifically sound, and the highest scientific standards must be enforced especially when systems are to be used in domains such as policing or social welfare." (e.g. the facial recognition and the emotional states) –
R: vagueness of the concepts used (scientifically sound; highest scientific standards; …)

3.3. Personal data used in the context of profiling should be stored in an anonymised form and where that is not possible stored in a (A.N.) (R: What's about the added value of profiling taking into account past data?) form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are collected and processed.

3.4. Except what may be stated below, processing of personal data in the context of profiling may only be performed:

- if it is explicitely provided for by law;
- if the data subject or her or his legal representative has given her or his free, specific, (JPW) not ambiguous and informed consent. In case of high-risk profiling, the consent ought to be explicit;
- (A.N): "in the following cases if the data subjects is informed and has the possibility to object the use of profiling" R: redundancy of the A.N. proposal.
    - if it is necessary for the performance of a contract to which the data subject is a party or for the implementation of pre-contractual measures taken at the request of the data subject;
    - if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the personal data are disclosed;
    - if it is necessary for the purposes of the legitimate interests of the controller or the third party or parties to whom the profiles or data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subjects. The necessity should be explicitly motivated by the controller (Arg.underlines that it must be possible);

if it is necessary in the vital interests of the data subject or of another person.

3.5. When the profiling has to be legitimated by consent, the processing of personal data in the context of profiling of persons who cannot express themselves their free, specific and informed consent should be forbidden except when the consent is given by the legal representative or when this processing is in the legitimate interest of the data subject, or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law.

3.6. In order to be free, consent implies for the data subject the possibility of an informed choice. As far as possible, service providers and platforms should offer different services that are more or less profiled (P.Int.) personalised instead of profiled (R: OK) or even non-

profiled depending on the service offered, in order to guarantee to the data subject a choice as regards the intensity of profiling. Consent to the profiling should not be required as a condition for the performance of a service. Where consent is required, it is incumbent on the controller to prove that the data subject has agreed to the profiling beyond what was necessary for the performance of the service, on an informed basis, as set out in Section 4.

3.7. As much as possible, and unless the service required necessitates knowledge of the data subject's identity, everyone should have access to information about goods or services or access to these goods or services themselves without having to communicate personal data to the goods or services provider. (IT) (R OK).

3.8. In order to ensure free, specific and informed consent to profiling, providers of information society services should ensure, by default, non-profiled access to information about their services.

3.9. The distribution and use, without the data subject's knowledge, of software aimed at the observation or the monitoring in the context of profiling of the use being made of a given terminal or electronic communication network should be permitted only if they are expressly provided for by (FR) law and (JPW) only if constitutes a measure necessary and proportionate within a democratic society and if they are accompanied by appropriate safeguards.

B. Quality of data and algorithms

3.10. Appropriate measures should be taken by the controller to correct data inaccuracy factors and limit the risks of errors and bias inherent in profiling.

3.11. The controller(s) and, where applicable the processors, should periodically and within a reasonable time re-evaluate the quality of the data and of the statistical inferences used (A.N) "as well as the impact that the use of profiling is having on data subjects rights". R: to be inserted art. 8.

3.12. When acquiring data or algorithms from a third party, the controller(s) shall obtain from the third party the documentation necessary to check the quality of the data and of the algorithms and their suitability to the purpose of the processing. (IT: consistency with GDPR ?) R precisely enlargement to the suppliers

3.13. Where the envisaged profiling is a high-risk processing, the controller(s) should (UK : 'may') notify it AN 'to the data subject to') and make the control and corrective measures taken available to the supervisory authority.

C. Special categories of data

3.14. The processing of special categories of data in the context of profiling is prohibited except if these data are necessary for the lawful and specific purposes of processing and as long as domestic law provides specific appropriate safeguards as regards processing of these data.

3.15. Processing for the purpose of detecting or predicting racial or ethnic origin political affiliation, GER trade union membership, religious or other beliefs and opinions, health or sexual life should likewise be subject to appropriate safeguards. See FR proposal to take again the art.22 GDPR wording." *4. Les décisions visées au paragraphe 2 ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9,*

paragraphe 1, à moins que l'article 9, paragraphe 2, point a) ou g), ne s'applique et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place. » R : Two Objections: the principle is enunciated here positively and not negatively. 2. The data envisaged covers also the inferred data.

See Pr. Int. 'PI believes that processing of political opinions/views should be prohibited unless very specific and narrow conditions are met.'

4. Information

4.1 Where personal data are collected in the context of profiling, the controller should provide the data subjects with the following information (GER: "Where personal data relating to a data subject are collected from the data subject in the context of profiling, the controller should, at the time when personal data are obtained, provide the data subjects with the following information (R: what's about the other cases?)

Pint: "PI suggests for a requirement to be added to the list in paragraph 4.1. for the user be notified of the result of any such profiling, which at a minimum should include any data inferred and/or any resulting categorisation." R: Is that realistic? Is that necessary? What is important is the obligation to explain the final decision and outcomes? See anyway art. 5.1

4.2 :

a. that their data will be used or are intended to be used in the context of profiling by themselves and/or by third parties;
b. the legal basis and the purposes for which the profiling is carried out;
c. the categories of personal and non-personal data used in the context of the profiling;
d. the identity of the controller and habitual residence or establishment of the controller and, if necessary, her or his representative;
e. the existence of appropriate safeguards UK in case it is required notably for special categories of data;
f. the categories of persons or bodies to whom or to which the personal data or the results of the profiling may be communicated, and the purposes for doing so;
g. the conditions of exercise of the right of access, objection, (TUR) erasure or correction, as well as the right to bring a complaint before the competent authorities;
h. all information (GER: recall that information might be furnished by icons) that is necessary for guaranteeing the fairness of recourse to profiling, such as:

– the possibility, where appropriate, for the data subjects to refuse or withdraw consent and the consequences of withdrawal;
– the persons from whom or bodies from which the personal data are or will be collected;
– the compulsory or optional nature of the reply to the questions used to collect the data and the consequences for the data subjects of not replying;
– the duration of storage of the personal data;
– where applicable, the potential impact of the profiling on the data subject.

4.2. When personal data are processed in the context of profiling, the controller should 'or could (UK) indicate the existence of a profiling activity with an icon. This icon should make it possible for anyone to automatically obtain the information listed in Principle 4.1 by linking to the website of the controller.

4.3. Where the personal data are collected from the data subject, the controller should provide the data subject with the information listed in Principle 4.1 at the latest at the time of collection.

4.4. Where personal data have not been collected from data subjects, the controller should, provide the data subjects with the information listed in Principle 4.1 as soon as the personal data are recorded or, if it is planned to communicate the personal data to a third party, at the latest when the personal data are first communicated 'ARG/GER: How to inform in practice? .Pint.: "to include a requirement from the controller to tell the data subject where their personal data was obtained from/who it was provided by, and on what legal basis that data was shared with controller."

4.5. Where the personal data are collected without the intent of applying profiling methods and are processed further in the context of profiling, the controller should have to provide the same information as that foreseen under Principle 4.1.

4.6. The provisions under Principles 4.3, 4.4 and 4.5 to inform the data subject do not apply (ARG) 'only' if:

a. the data subject has already been informed;
b. it proves impossible to provide the information or it would involve disproportionate effort;
c. the processing of personal data for profiling is expressly provided for by domestic law (AN) and certain specific uses as subject to limited exceptions to the right to information. (GER b and c) available only in case of data collected from third parties)

In the cases set out in b and c, appropriate safeguards should be provided for.

4.7. The information provided to the data subject should be delivered in a comprehensible manner and adapted to the circumstances.

Data subjects' rights

5.1. The data subject who is being, or has been, profiled should be entitled to obtain from the controller, at her or his request, within a reasonable time (AN within a month from his or her request R difficult for SME) and in an understandable form, information concerning:

a. her or his personal data and the categories of pseudonymised or anonymised data used in the processing operation; PI suggests for a requirement to be added to the list in paragraph 5.1.. The user should have access to the result of any such profiling, which at a minimum should include any data inferred and/or any resulting categorisation (R What happens in case of implicitly inferred data or categorisation?)
b. the logic underpinning the processing of her or his personal data and that was used to attribute a profile to her or him, at least in the case of an automated decision and, in the case of the use of processing based on machine learning, the model (UK **'information about the model that is accessible in plain language' R OK .**. In this case, the information must be such as to enable the data subject to understand the justification for the decisions or proposals for decisions regarding him/her; (GER

remark about the structure of the text: to move all provisons about profiling with AI to the art. 8. It will make the text more readable) R OK / A. N: and information about the system, including its objective function (R there are multiple objective function), how it was trained and how the training data was collected and labelled (R: it would be better to have an obligation for D.C. to produce a document available at the DPA office; See 8.8.)
Por: "However, it is not clear where the duty to clarify referred to in point 5, b, will not conflict with arguable protect trade secrets or intellectual property" (R: See also 8.9.)

c. the purposes for which the profiling was carried out;
d. the categories of persons or bodies to whom personal data, the profile or the result of the processing may be communicated as well as the right to object to it.

5.2. Data subjects and DPA are (FR) should be entitled to obtain immediate deletion or blocking of their personal data, A.N. including when profiling is performed in non-conformity with the appropriate provisions of domestic law, which enforce the provisions set out in Convention 108+ (especially, as regards the profiling using special categories of data (point 3.12)). (to be deleted JPW/ IT)

5.3. Unless the law provides for (A.N) limited use of profiling (R implicit) (GER: "..which lays down measures to safeguard data subject's legitimate interests"), the data subject should be entitled to oppose (FR including to the controller) the processing of her or his personal data, at any time, on grounds concerning him or her. Unless the controller demonstrates legitimate grounds for the processing, which override the interest or fundamental human rights and freedoms (JPW) of the data subject, the profiling should no longer involve the use of the personal data of the data subject. Where the purpose of the profiling is direct marketing, no justification should be requested from the data subject.

5.4. If there are any grounds for restricting the rights set out in this section in accordance with Section 6, this decision should be communicated to the data subject by any means that allows it to be put on record, with a mention of the legal and factual reasons for such a restriction.
This mention may be omitted when a reason exists which endangers the aim of the restriction. In such cases, information should be given to the data subject on how to challenge this decision before the competent national supervisory authority, a judicial authority or a court.

5.5. Where a person is subject to a decision having legal effects concerning her or him, or significantly affecting her or him, taken on the sole basis of profiling, she or he should be able to object to the decision unless:

a. this is provided for by law, which lays down measures to safeguard data subjects' legitimate interests, particularly by allowing them to put forward their point of view;
b. the decision was needed to ensure the performance of a contract to which the data subject is party or to the implementation of pre-contractual measures taken at the request of the data subject and that measures for safeguarding the legitimate interests of the data subject are in place.

5.6. In any event, and not only in the cases referred to in Principle 5.5, when the profiling system issues a decision or a draft decision, it is recommended that:

a. the controller considers all the particularities of the data and not only rely on decontextualised information or results of the processing;
b. in the event of high-risk profiling (IT), the controller sets up a service where a person will inform the data subject of the algorithmic operations underlying the data

processing, including the consequences of these operations for him/her. In that case, the information should be such as to enable the data subject to understand the justification for the decisions or proposals for decisions regarding him/her. This requirement is highly dependent on the consequences of the impact of the output for the data subject (principle of explicability) ;

c. in that case, the person appointed by the controller must be able, on the basis of reasonable arguments, to decide not to rely on the results of the recommendations resulting from the use of profiling;
d. where there are indications of direct or indirect discrimination based on the functioning of the profiling operation, controllers and processors shall provide evidence of the absence of discrimination.

5.7. Persons affected by a decision based on profiling have the right to receive useful explanation of the decision (UK For background we'd refer to the ICO's AI Explainability Guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence/part-1-the-basics-of-explaining-ai/what-goes-into-an-explanation/) and to challenge it in front of a competent authority having access to all the information about the profiling and its functioning.

5.8. Unless explicitly consented to, the data subject must be able to object by an easy means to the transfer or sharing of data, either for profiling purposes by third parties or of the results of profiling.

6. Exceptions and restrictions

6.1. Where it constitutes a necessary and proportionate measure in a democratic society for reasons of national security, defence, public safety (and other grounds listed in Article 11 of Convention 108+) provisions set out in Sections 3, 4 and 5 are not applicable. Such an exception has to be provided for by law and respect the essence of the fundamental rights and freedoms.

7. Remedies

7.1. Domestic law should provide appropriate sanctions and remedies in cases of breach of the relevant provisions of domestic law. (IT: do we need that general provision?)

8. Data Security

General provisions

8.1. Appropriate technical and organisational measures should be taken, in particular on the basis of the principles of 'privacy by design' and 'privacy by default', to ensure the protection of personal data processed in accordance with the provisions of domestic law enforcing the principles set out in Convention 108+ (JPW), to guard against accidental or unlawful destruction and accidental loss, as well as unauthorised access, alteration, communication or any other form of unlawful processing.

8.2. These measures should ensure a proper standard of data security having regard to the technical state of the art and also to the sensitive nature of the personal data processed

in the context of profiling and evaluating the potential risks. They should be reviewed periodically and within a reasonable time.

8.3. The controllers should, in accordance with domestic law, lay down appropriate internal regulations with due regard to the relevant principles of this recommendation.

8.4. If necessary, the controllers should appoint an independent person (A DPO? (IT)) responsible for the security of information systems and data protection, and qualified to give advice on these matters.

8.5. Controllers should choose processors who offer adequate safeguards regarding the technical and organisational aspects of the processing to be carried out and should ensure that these safeguards are observed and that, in particular, the processing is in accordance with their instructions.

8.6. The controllers should assess the risk of re-identification taking into account the time, effort or resources required with regard to the nature of the data, the context of their use, the available re-identification techniques and the corresponding costs. Controllers should demonstrate the adequacy of data pseudonymisation or anonymisation measures and guarantee their effectiveness. Technical measures may be combined with legal or contractual obligations in order to prevent any possible re-identification of the data subjects. Controllers should regularly reassess the risk of re-identification, in view of technological advances in disanonymisation techniques.

Special provisions for profiling based on AI systems (GER) using automatic learning processes

8.7. In order to ensure trust in AI systems, controllers and, where applicable, processors shall ensure the use of reliable and safe systems, in particular with regard to the setting up of procedures both in the event of breakdown, error or inconsistencies during all life cycle of the system (AN: via audits and public reports R: too broad and difficult for SME. OK for high risk processing). They shall ensure on a regular basis and throughout the life of the system that it is reliable and that its results are consistent with the model and reproducible.(A.N) Results themselves shall also be assessed to evaluate their impact on DS , including the right of non discrimination (R to put into 8.8.) The system ought to be robust against attacks or other manipulation of the data or the algorithms. ES: "The systems must allow operational human intervention if necessary" (R: to put elsewhere)

8.8. Controllers and, where applicable, processors shall ensure a critical assessment of the quality, representative nature and quantity of the data used by eliminating unnecessary data and any data that could bias the results. They ensure the robustness of the model in case of new data input,.(GER) In particular, certain minimum thresholds of correctness, accuracy of results must be met.

8.9. Controllers and, where applicable, processors shall ensure the transparency of the functioning of the systems and the traceability, reproducibility and, if needed, the reversibility of the processing results. They will ensure that their intellectual property rights and trade secrets are only minimally opposed ((UK): to,replace by **'The type of information given to data subjects under the right to transparency is unlikely to infringe intellectual property rights or to risk revealing trade secrets' R: better art. 5.7.)** and, in no way will they be able to oppose the request of a data subject or of a group to be able to understand the decisions or proposed decisions taken from the profiling operations. (GER) The data subject who is being, or has been, profiled should be entitled to obtain from the controller, at her or his request, within a reasonable time and in an understandable form, information concerning the data which was used for

his/her specific profile ("input data"), the model on which the AI system operates and the data with which the model was trained. (R: Redundant) AI applications should allow effective control of the effects of its applications on individuals, groups and society by both concerned data subjects and groups.

8.10. For the purposes of a continuous assessment of both individual and collective risks, and in any case when it comes to high-risk profiling operations, controllers and, where appropriate, processors should (GER) be obliged to continuously document ex ante the training of the model as well carry out regular impact assessments addressing the specific risks of profiling based on AI systems (R: too detailed). For this purpose, they shall surround themselves with a multidisciplinary assessment team and consult representatives of the interests involved in profiling, including profiled people. Such an evaluation process should be conducted by qualified and adequately knowledgeable professionals who would assess the various impacts, including their legal, social, ethical and technical dimensions. (AN): Add :"Specific outcomes - including the potential pause or withdrawal of the application carrying out the profiling via automatic learning processes - should be predefined and linked to this assessment process. R: implicit

9. Supervisory authorities

9.1. Member states should mandate one or more independent authorities to ensure compliance with the domestic law implementing the principles set out in this recommendation and having, in this respect, the necessary powers of defining the procedures and the content of the evaluation of the assessment as foreseen under point 8.10. Furthermore, these authorities should be competent for any investigation and intervention, in particular the power to hear claims lodged by any individual person. SLO: "*Member states should ensure that authorities have sufficient financial and personal resources in order to be able to exercise their tasks properly.*"

9.2. Furthermore, in cases of processing that use profiling and entail high risks with regard to the protection of privacy and personal data, member states may foresee either:

a. that controllers have to make available to the supervisory authorities all the documents relating to the procedure followed and to the evaluation itself or;
b. that controllers have to notify these documents to the supervisory authority in advance of the processing; or
c. that this processing is subject to prior checking by the supervisory authority.

9.3. In the implementation of this recommendation, supervisory authorities should cooperate as far as possible with consumer and competition protection authorities as well as with institutions responsible for equal opportunities or for the promotion of democracy. When an independent multidisciplinary national authority to assess the risks associated with artificial intelligence and in particular with profiling processing using machine learning processes exists, the supervisory authority should coordinate its work with this institution.

9.4.When analysing profiling operations, the supervisory authorities should make sure to extend their competence to the analysis of collective risks and risks to the society and its democratic functioning and to ensure the respect of principle 2.1. Their opinions should mention such risks and their decisions should take them into consideration. Authorities should draw the attention of member states on the importance of broadening their expertise in this field. (Alternative suggested by UK: "**'the field of inquiry of supervisory authorities should be broadened to include collective and societal risks'. R: OK)**

Explanation:

They will ensure that their opinions mention such risks and that they are factored into their decisions. Where appropriate, they will initiate debate on the subject. They will draw the attention of member states to the importance of broadening their remit in this area. To some degree this could happen today given the existing scope of the SAs' legal remit, i.e. when a controller is assessing whether proposed processing activity is "within the public interest" under the GDPR they could cite broader ethical considerations to support their assessment when weighing the broader societal benefits (i.e. the public interest) against any infringement upon the in-scope individuals' rights and freedoms.

> In this context, supervisory authorities should be entitled to receive and investigate complaints from associations concerning the collective interest of a group or the general interest. If necessary, the authorities should make recommendations in this regard.

The above authorities should inform the public of the application of the legislation implementing the principles set out in this recommendation.

10. Additional measures

Labelling and certification of AI and data protection systems

10.1. Member states and supervisory authorities should encourage the setting up of independent and qualified ex ante (GER) (R: to be discussed) certification mechanisms for AI and data protection systems, (GER) in particular the training and resulting model on which profiling is based and related labels and marks to demonstrate that processing operations carried out by controllers and processors comply with this recommendation. The specific needs of both micro, small and medium-sized enterprises and different sectors should be taken into account. (FR: To be included within the recommendation?) (A.N. Add: "However, if the profiling activities carried out by a system are of a high-risk nature, the same level of strictness should be applied regardless of the size of the enterprise." (R: OK with the AN suggestion)°

10.2. Member states may lay down conditions for the approval of bodies, which would set up the control mechanisms referred to in Principle 10.1.

10.3. Certification is voluntary and accessible through a transparent process. A certification under this Principle shall not reduce the liability of the controller or of the processor to comply with this recommendation or with applicable laws.

10.4. Data controllers and processors, whose systems are certified or labelled will affix the certification or label mark at least on their website and on the information for data subjects. They shall ensure that, via such a mark, access to the certificate or label is accessible to anybody. (AN) add: Necessary review on a regular basis by the competent supervisory authority. (R: Validity of the certification may be limited in time!)

With regard to profiling operations carried out by public authorities

> 10.5. The profiling operations carried out by public authorities both to define their strategies and to apply them must be based on a clear, proportionate and necessary law in (GER) careful consideration of all fundamental rights concerned within a democratic society, according to the understanding of the case law of the Council of Europe.

In accordance with Principle 10.1., the design, development, implementation and monitoring of AI systems, in particular profiling systems, should be submitted to the mechanism competent (UK: competent authority / R: OK) for risk assessment of AI.

The requirements for access to administrative documents (IT Are we referring to the access to data held by public sector?) and the reasons for public decisions require that computerised decision-making or decision-support systems be transparent and that individuals may, notwithstanding any technical or legal arguments, have access to the reasoning based on the algorithm. (GER) Add: "Otherwise, effective legal protection against the decisions would not be guaranteed."

Public authorities shall ensure that the requirements of these recommendations, in particular those specific to them, are communicated to their processors as part of their terms of reference.

Provisions regarding research and education

Member states should encourage, independent, interdisciplinary and open, including fundamental research, in particular on the reliability, auditability, robustness and transparency of AI systems including by allocating resources. (AN): Add "Such research should not be solely academic, but should include representatives from civil society and representatives of groups likely to be adversely impacted by AI systems, and by profiling systems in particular;" (R: When relevant, that research should be lead in dialog with civil society representatives)

Member States should encourage open source initiatives for design and free dissemination of algorithms.

Member States should allocate resources to multidisciplinary digital literacy at all levels of education in order to raise people's awareness of digital issues and, in particular, AI. They should likewise encourage professional training, training of administrations and business managers to the technical aspects and societal and human rights issues of the systems used in profiling, in particular through interdisciplinary courses to be included in education and post-graduation curricula for digital professions.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

26 October 2020

T-PD(2020)03rev

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

CONVENTION 108

Facial Recognition

Draft Guidelines

Directorate General of Human Rights and Rule of Law

Contents

Facial recognition is the automatic processing of digital images containing individuals' faces by using face templates for identification or verification of those individuals.

The sensitivity of information of a biometric nature was recognised explicitly with the inclusion of data uniquely identifying a person under the special categories of data in Article 6 of the modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data[1] (hereinafter "Convention 108+").

The context of the processing of images is relevant to the determination of the sensitive nature of the data as not all processing of images involve the processing of sensitive data. Images will only be covered by the definition of biometric data when being processed through a specific technical mean which permits the unique identification or authentication of an individual[2].

These Guidelines cover uses of facial recognition technologies, including live facial recognition technologies. The uses of this technology are varied and numerous, some of which may seriously infringe the rights of data subjects. Legislation authorising vast surveillance of individuals are to be considered contrary to the right to respect for private life.[3]

Integrating facial recognition technologies to existing surveillance systems poses a serious risk to the rights to privacy and protection of personal data since the uses of these technologies does 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.

In order to prevent such infringements, the Parties to Convention 108+ shall ensure and permit that the development and use of facial recognition respect the rights to privacy and to data protection, thereby strengthening human rights and fundamental freedoms by implementing the principles enshrined in the Convention in the specific context of facial recognition technologies.

These guidelines[4] 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 these technologies do not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data.

The guidelines are general in scope and cover uses in the private and public sectors and do not exclude that further protective measures be required in the applicable legal framework depending on the case of use. The guidelines assess various uses of these technologies in

---

[1] Amending Protocol CETS 223 to Convention 108
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

[2] Paragraph 59 of the Explanatory Report to Convention 108+

[3] Declaration of the Committee of Ministers of the Council of Europe on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, adopted on 11 June 2013, available at
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068460d

[4] These Guidelines build upon a 2019 report by Sandra Azria and Frédéric Wickert "Facial recognition: current situation and challenges", available at https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1

different sectors by taking into account the purposes of these uses and their potential impact on the right to data protection and other fundamental rights.

Law enforcement purposes mean in these guidelines the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties. This includes the maintenance of public order by the police (hereinafter referred to as "law enforcement purposes")[5].

Nothing in these guidelines should be interpreted as excluding or limiting the provisions of the Convention 108[6]. These guidelines also take into account the new safeguards provided by Convention 108+.

I. GUIDELINES FOR LEGISLATORS AND DECISION-MAKERS

1. Lawfulness

As provided for by Article 6 of Convention 108+, the processing of special categories of data, such as biometric data, shall only be authorised if such processing relies on an appropriate legal basis and complementary and appropriate safeguards are enshrined in law. These safeguards shall be adapted to the risks involved and to the interests, rights and freedoms to be protected.

Some national laws[7] have enacted the prohibition of such processing as a rule and only allow its implementation by way of exception, in certain specific cases (*e.g.* with the explicit consent of individuals, to protect their vital interests or on the basis of an overarching public interest) and subject to safeguards that are appropriate to those risks.

The necessity of the use of facial recognition technologies has to be assessed together with the proportionality to the purpose and the impact on the rights of the data subjects.

The different cases of use should be categorised, and a legal framework should be in place which will determine, according to each different use:

- the detailed explanation of the specific use and the purpose;
- the minimum reliability of the algorithm: minimum reliability percentage;
- the retention duration of the photos used;
- the possibility of auditing these criteria;
- the traceability of the process;
- the safeguards.

1.1. Strict Limitation by Law of Certain Uses

[5] Law enforcement purposes corresponds to 'police purposes' in the practical guide on the use of personal data in the police sector, see Committee of Convention 108, , Practical guide on the use of personal data in the police sector (T-PD(2018)01) available at https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

[6] Evidently, for Parties to the Convention which are Council of Europe member states, nothing in the guidelines can furthermore be interpreted as excluding or limiting the provisions of the European Convention on Human Rights

[7] See Article 9 of the European Union's General Data Protection Regulation (GDPR)

The level of intrusiveness of facial recognition, and related infringement on the rights to privacy and data protection will vary based on the particular situation of their uses and there will be cases where national law will strictly limit it, or even completely prohibit it where the democratic process will have led to that decision.

The use of live facial recognition technologies in uncontrolled environments[8], in light of the intrusiveness it bares upon the right to privacy and the dignity of individuals, coupled with a chilling-effect on other human rights and fundamental freedoms, should be subject to a moratorium pending complete analysis and democratic debate on its use.

The use of facial recognition for the sole purpose of determining a person's skin colour, religion, sex, origin, age or health condition should be strictly limited[9].

Similarly, affect recognition can also be carried out with facial recognition technologies to detect personality traits inner feelings, mental health or workers' engagement from face images. Linking recognition of affect to hiring of staff, access to insurance, education and policing may pose risks of great concern, both at the individual and societal levels and would require careful consideration and safeguards enshrined in law to be authorised.

1.2. Legal Basis in Different Contexts

The legal framework shall consider:

- the different phases of the use of facial recognition technologies;
- the sectors in which these technologies are used;
- the purposes of the biometric processing;
- the intrusiveness of types of facial recognition technologies, while providing clear guidance on the lawfulness.

1.2.1. Integrating Digital Images to the Facial Recognition Technologies

Legislators and decision-makers shall ensure that images available in a digital format cannot be processed to extract biometric templates or integrate them into biometric systems without a specific legal basis for the new processing, when those images were initially captured for other purposes (from social media for instance).

As extracting biometric templates from digital images involves sensitive data processing, the possible legal basis considered below, varying for different sectors and uses must be secured.

Specifically, using digital images that were uploaded on Internet, including social media or online photo management websites or were captured passing through the lens of video surveillance cameras cannot be considered lawful on the sole basis that the personal data were made manifestly available by data subjects.

Legislators and decision-makers should ensure that existing digital image databases initially used for other purposes can only serve to extract biometric templates and integrate them into biometric systems when it is for law enforcement purposes and it is provided by law and strictly necessary and proportionate for these purposes.

---

[8] The notion of "uncontrolled environment" covers places freely accessible to individuals, where they can also pass through, including public and quasi-public spaces such as shopping malls, hospitals, or schools.

[9] It could for example be authorised for a medical research project, subject to appropriate safeguards enshrined in law.

1.2.2. Use of Facial Recognition Technologies in the Public Sector

Consent should not, as a rule, be the legal ground used for facial recognition performed by public authorities considering the imbalance of powers between data subjects and public authorities.

The lawfulness of the use of facial recognition technologies shall be based on the purposes of the biometric processing provided by law and necessary safeguards complementing the Convention 108+.

Legislators and decision-makers have to lay down specific rules for biometric processing by facial recognition technologies for law enforcement purposes. These laws will ensure that such uses must be strictly necessary and proportionate for these purposes and prescribe the necessary safeguards to be provided.

Law enforcement authorities

Biometric data processing by facial recognition technologies for identification purposes in a controlled[10] or uncontrolled environment should be restricted to law enforcement purposes and carried out solely by the competent authorities (hereinafter "law enforcement authorities").

Laws can provide different necessity and proportionality tests depending on whether the purpose is verification or identification, considering the potential risks to fundamental rights and as long as individuals' images are lawfully collected. .

For identification purposes, the strict necessity and proportionality must be observed both in the creation of the database (watchlist) and deployment of (live) facial recognition technologies in an uncontrolled environment.

Laws should provide objective criteria such as the fact of being suspected of severe offences or presenting a risk to the public security by which law enforcement authorities can create databases (watchlist) for those specific, legitimate and explicit purposes.

In the phase of deployment of the live facial recognition technologies in uncontrolled environments, the law will ensure that law enforcement authorities demonstrate that a variety of factors, including the place and timing of deployment of these technologies, justify the strict necessity and proportionality of the uses, considering the intrusiveness of these technologies.

Other public authorities

Legislators and decision-makers will lay down specific rules for biometric processing by facial recognition technologies for other substantial public interests by public authorities that are not pursuing law enforcement purposes.

Laws can provide different necessity and proportionality tests depending on whether the purpose is verification or identification, considering the potential risks to fundamental rights and as long as individuals' images are lawfully collected.

Considering the potential intrusiveness of these technologies, legislators and decision-makers have to ensure that an explicit and precise legal basis provides the necessary

[10] The notion of "controlled environment" covers places where access is restricted.

safeguards for the processing of biometric data. Such legal basis will include the strict necessity and proportionality of these uses, and will take into consideration the vulnerability of the data subjects and the nature of the environment where these technologies are used for verification purposes.

For example,ensuring security in controlled or uncontrolled environments, including schools or other public buildings, should not, as a rule, be considered strictly necessary and proportionate where alternative mechanisms that are less intrusive exist.

1.1.3. Use of Facial Recognition Technologies in the Private Sector

The use of facial recognition technologies by private entities requires the explicit consent of data subjects whose biometric data is processed.

Considering the requirement for an explicit consent of data subjects, the use of facial recognition technologies can only take place in controlled environments for verification or for categorisation[11] purposes. Passing through an environment where facial recognition technologies are used cannot be considered as an explicit consent.

Depending on the purpose, particular attention must be paid to the quality of the data subject's explicit consent when it is the legal basis for the processing. Such consent furthermore has to be free, specific and informed according to Article 5 of Convention 108+.

In order to ensure that consent is freely given, data subjects should be offered alternative solutions to the use of facial recognition technologies (for example, using a password or an identification badge) but also ensure that the proposed alternative be easy to use as, if it appeared to be too long or complicated compared to the facial recognition technology, the choice would not be a genuine one.

If consent is given for one purpose, there can be no other use of the data for any other purpose, except where consent is sought and given in respect of such other purpose. Similarly, in case of disclosure of data to a third party, such disclosure should also be subject to specific consent.

Private entities cannot not rely for the biometric data processing on the derogatory regime of data made manifestly available by data subjects.

Private entities shall not deploy facial recognition technologies in uncontrolled environments such as shopping malls or open gardens to identify persons of interest, for marketing purposes or for security purposes.

2. Necessary Involvement of Supervisory Authorities

In compliance with Article 15(3) of Convention 108+, supervisory authorities are to be consulted on proposals for any legislative or administrative measures implying the processing of personal data by facial recognition technologies. It seems desirable to systematically involve the supervisory authorities and, in particular, to consult them on any possible experimentation or deployment foreseen.

These authorities could thus be consulted systematically and in advance on envisaged projects. Similarly, they should have access to the impact assessments carried out and also to all audits, reports and analyses carried out in the context of these experiments or projects.

[11] Biometric categorisation means 'the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action'.

Legislators and decision-makers should ensure effective cooperation between various supervisory authorities competent for the oversight of different aspects of these data processing where different authorities are responsible for the control of the compliance of such processing activities with the law.

3. Certification

Legislators and decision-makers should use different mechanisms to ensure the accountability of the developers, manufacturers, service providers or entities using these technologies.

The setting up of independent and qualified certification mechanism for facial recognition and data protection to demonstrate full compliance of the processing operations carried out would be an essential element in building user confidence.

Such a certification could be implemented at various levels depending on the field of application of artificial intelligence used by the facial recognition technology: one level to categorise types of structures (design of algorithm, integration of algorithm, etc) one level to categorise types of algorithms (computer recognition, intelligent search, etc.) and one level to categorise uses (critical or non-critical).

4. Raising Awareness

The awareness of data subjects and the understanding by the general public of facial recognition technologies and of their impact on fundamental rights should be actively supported through accessible and educational actions.

The idea is to give access to simple concepts that could alert the data subjects before they decide to use a facial recognition technology, to understand what it means to use sensitive data such as biometric data, how facial recognition works and to alert to potential dangers, notably in case of misuse.

Legislators and decision-makers should facilitate public engagement in the development and use of these technologies and adequate safeguards to protect fundamental rights at stake while using facial recognition technologies.

II. GUIDELINES FOR DEVELOPERS, MANUFACTURERS AND SERVICE PROVIDERS

This section of the guidelines specifically covers issues related to the development and manufacturing phases of facial recognition technologies. Where developers, manufacturers and service providers process biometric data for their own purposes in the development phase, they will furthermore be concerned by Section III of the guidelines on entities using such technology.

1. Data and Algorithms Quality

1.1. Representativeness of the Data Used

Like other applicable legal instruments, Article 5 of Convention 108+ provides for a data accuracy requirement. Therefore, developers or manufacturers of facial recognition

technologies, as actually also entities using them, will have to take steps to ensure that facial recognition data are accurate. In particular, they will have to avoid mislabelling, by sufficiently testing their systems and identifying and eliminating significant disparities in accuracy, notably with regard to demographic variations in skin colour, age and gender, and thus avoid unintended discrimination.

Furthermore, in order to ensure both the quality of the data and the efficiency of the algorithms, the algorithms will have to be developed using datasets based on sufficiently diverse photos of men and women, of different skin colours, different morphology, of all ages and from different camera angles. Back-up procedures should be provided for in case of system failure if the physical characteristics do not correspond to the technical standards.

Biometric data unnecessarily but unavoidably revealing other sensitive data such as information on a type of illness or physical disability will also be subject to complementary appropriate safeguards.

1.2. Data Life Duration

A facial recognition system requires periodic renewal of data (the photos of faces to be recognised) in order to train and improve the algorithm used.

Each algorithm has a percentage of recognition reliability, both during its development and use. It therefore seems important to date and to record this percentage in order to monitor its evolution. Should its reliability deteriorate, it will be necessary to renew the training photos and therefore ask more recent photos to be provided. This will also enable to protect from the consequences of changes in the shape of faces (due to ageing, to accessories (piercing or other), or to other modifications of the face).

These reliability percentage records could be made easily available to interested customers or entities using facial recognition technologies, in the form of a dashboard for example, to facilitate their choice of acquisition and deployment of a specific technology.

2. Reliability of the Tools Used

The reliability of the tools used depends on the effectiveness of the algorithm. This effectiveness relies on different factors, among others: false positives, false negatives, performance in different lights, reliability when faces are turned from the camera, impact of face coverings.

The highest possible level of reliability should be ensured, considering that the use of a facial recognition system might result in very significant adverse consequences for the individual.

3. Awareness

Companies developing and selling facial recognition technologies should take reasonable steps - such as making recommendations and providing advice - to help the entities using their facial recognition technology to apply transparency and respect for privacy (by providing them with a sample language for their privacy policies or by recommending clear, easy-to-understand signage that indicates that a facial recognition technology is deployed in a specific space).

4. Accountability

Companies developing and selling facial recognition technologies should:

- integrate data protection into the design and architecture of facial recognition products and services, as well as into internal IT systems and integrate the use of dedicated tools including the automatic deletion of the raw data after extracting biometric templates;
- offer a certain level of flexibility in the design of these technologies to adjust the technical safeguards according to the principles of purpose limitation, data minimisation and limitation of the duration of storage of data;
- implement an internal review process designed to identify and mitigate the potential impact on the rights and fundamental freedoms of products and services that use facial recognition technologies before they are made available;
- integrate a data protection approach into their organisational practices, including assigning dedicated staff, providing privacy training to employees, and conducting data protection analyses upon the development or modification of facial recognition products and services.

III. GUIDELINES FOR ENTITIES USING FACIAL RECOGNITION TECHNOLOGIES

Entities[12] have to comply with all the applicable data protection principles and provisions while processing biometric data in their use of facial recognition technologies. Entities using facial recognition technologies have to demonstrate that this use is strictly necessary, and proportionate, in the specific context of their use and that it does not interfere unduly with the rights of the data subjects.

Entities can rely on the exceptions provided in the applicable legislation complying with Article 11 of Convention 108+ (provided for by law, pursuing a specific legitimate aim, e respecting the essence of the fundamental rights and freedoms and constituteing a necessary and proportionate measure in a democratic society).

Entities using facial recognition technologies should consider how this use will impact both those who voluntarily use the technology and those who happen to come into contact with it with no such intention.

1. Legitimacy of Data Processing and Quality of Data

Entities will rely on different legal basis according to their sectors and the purposes of the use of facial recognition technologies mentioned in Section I.

Transparency and Fairness

As the facial recognition technologies can be used without any intention of or cooperation with data subjects, the transparency and fairness of the processing is of the upmost importance and will have to be duly considered by entities using them.

[12] In this section of the Guidelines, the term "entities" covers data controllers, and where applicable processors, in both the public and private sectors.

The entities will have to provide all the necessary information about the processing as detailed in Article 8 of Convention 108+.

The factors that will determine whether transparency is ensured include, for example, that the information is given to individuals, the context of the collection, reasonable expectations as to how the data will be used, whether facial recognition is merely a feature of a product or service or instead, an integral part of the service itself. They should also be informed on how the collection, use or sharing of facial recognition data is likely to affect them, especially when they concern persons in vulnerable situations. The information provided also has to state which rights and legal remedies the data subjects are entitled to.

Privacy policies on facial recognition or the informational material regarding the technologies could include, in addition to the information provided for in Article 8 of Convention 108+, the following information[13].

- whether and to which extent facial recognition data can be transmitted to third parties (and where such is the case, information on the identity of the third-party contractual partners receiving the data in the course of providing the product or service);
- the retention, deletion or de-identification of facial recognition data;
- contact points available for individuals to ask questions about the collection, use and sharing of facial recognition data;
- when the collection, use and sharing practices change significantly, entities should update their privacy policy or publicise these changes in light of the context of the change and its impact on individuals.

In the creation of databases, for identification or verification purposes by law enforcement authorities, the transparency obligation may be proportionally restricted to not prejudice the law enforcement purposes, in accordance with Article 11 of Convention 108+ and subject to its requirements.

When live facial recognition technologies are deployed in an uncontrolled environment, law enforcement authorities can take a layered approach to providing the necessary information to data subjects passing through the uncontrolled environment.

The first layer of the provision of the information will contain readable and intelligible information about the purpose of the processing, the authority using the technology, duration of the processing and perimeter concerned and will be in the appropriate vicinity of the place where these technologies are deployed.

The second layer of the provision of information will contain all necessary information required according to Article 8 of Convention 108+, to be displayed at the entry points of the place of deployment.

Covert use of live facial recognition technologies by law enforcement authorities can only be used if it is strictly necessary and proportionate to prevent imminent and a substantial risk to public security, which should be documented before the covert use.

[13] On this point, see the recommendations by the Future Privacy Forum "Privacy Principles for Facial Recognition Technology in Commercial Applications" https://fpf.org/2018/09/20/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/

Purpose Limitation, Data Minimisation and Limited duration of storage

Personal data undergoing processing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes according to Article 5(4) of Convention 108+.

Furthermore, before any subsequent processing, entities will have to consider whether the purposes of the new processing are compatible with the purposes initially defined. Otherwise, the legal basis for the new processing will require a distinctive legal basis.

Entities have to comply with the data minimisation principle, which requires that only the required information be processed, and not all information available to the entities.

Entities also have to set a retention period, which cannot be longer than what is necessary for the specific purpose of the processing and ensure the deletion of biometric templates upon completion of that purpose. While determining the retention period, the biometric nature of the personal data must be taken into account.

In the deployment of live facial recognition technologies, entities furthermore have to ensure that different storage limitation periods apply to the different phases of the processing :

- if there is no match of the biometric templates, the biometric template of individuals passing through an uncontrolled environment cannot be retained and have to be automatically deleted;

- if the match occurs, the biometric templates can be retained for a strictly limited time provided by law with necessary safeguards and match reports including personal data can also be retained for a limited time;

- and in any case, deletion of the watchlist and biometric templates upon completion of the purpose for which live facial recognition technologies were deployed.

Accuracy

Entities have to ensure that the biometric templates and digital images are accurate and updated. For instance, the quality of images and biometric templates inserted in watchlists must be checked to prevent potential false matches since images having low quality can cause an increase in the number of errors. This is directly linked to the sources of the images compiled in the watchlist, which require strict respect of the data protection principles (legal basis: no use of social media source. Purpose specification and limited retention: no use of custody images that should have been deleted.)

If false matches occur, the entities will take all reasonable steps to correct future occurences and ensure the accuracy of digital images and biometric templates.

2. Data Security

Any failure in data security may have particularly severe consequences for data subjects, as unauthorised disclosure of such sensitive data cannot be corrected.

Strong security measures, both at the technical and organisational levels, should therefore be implemented to protect facial recognition data and image sets against the loss and unauthorised access or use of the data during all the processing stages, be it the collection, transmission and storage.

Entities will take measures to prevent technology-specific attacks, including presentation attacks and morphing attacks.

Any breach of the security of data has to be notified to the supervisory authority and, where appropriate, to the data subjects.

Security measures should evolve over time and in response to changing threats and identified vulnerabilities. They should also be proportionate to the sensitivity of the data, to the context in which a specific facial recognition technology is used and its purposes, to the likelihood of harm to individuals and other relevant factors.

Strict retention and disposal practices for facial recognition data, with the shortest possible retention periods, also contribute to reducing security exposures.

3. Accountability

Entities will take all appropriate measures to comply with their obligations and to be able to demonstrate that the data processing under their control complies with those, as foreseen in Article 10 of Convention 108+.

The following organisational measures have to be taken into account by entities using facial recognition technologies:

- implementation of transparent policies, procedures and practices to ensure that the protection of the rights of data subjects underlie their use of facial recognition technologies;

- setting up and delivery of training programmes and audit procedures for those in charge of processing facial recognition data;

- establishment of internal review committees to assess and approve any processing involving facial recognition data;

- contractual extension to third-party service providers, business partners or other entities using facial recognition technology of the applicable requirements (and denial of the access to third parties that would not comply with them);

- in the public sector: prior evaluation constraints in public procurement procedures with suppliers of facial recognition tools, assessment of minimum levels of performance in terms of accuracy, especially where law enforcement purposes are concerned;

Entities will take the necessary technical measures to ensure the quality of biometric data by following internationally agreed technical standards, depending on the context of their uses.

3.1. Data Protection by Design

Data protection by design covers the whole value chain of processing by facial recognition technologies. Entities using facial recognition technologies for identification or verification purposes have to ensure that the products or services they are using are designed to process biometric data in compliance with the principles of purpose limitation, data

minimisation and limited duration of the storage, and integrate all other necessary safeguards in the technologies.

When entities set the technical features of these technologies, they implement these principles into their design, to ensure that the deployment of these technologies will be respectful of the rigtht to data protection.

3.2. Data Protection Impact Assessment

Entities using facial recognition technologies have to carry out impact assessments before the processing as the use of these technologies involves biometric data processing and presents high risks to the fundamental rights of data subjects.

During the preparation of the impact assessment, the entities will not only recognise the risks arising from the potential processing but also address the necessary mitigating measures to tackle these risks by taking the necessary technical and organisational measures. In this assessment, they will explain, among other things:

- the lawfulness of the use of these technologies;
- which fundamental rights are at stake in the biometric processing;
- the vulnerability of data subjects;
- how these risks can be effectively mitigated.

Specifically, while considering the deployment of facial recognition technologies in uncontrolled environments, law enforcement authorities will have to:

- assess and explain in their assessment the strict necessity and proportionality of the deployment of these technologies;
- address the risk to different fundamental rights, including data protection, privacy freedom of expression, freedom of assembly, freedom of movement or anti-discrimination, depending on the potential uses in different places.

The impact assessment could be carried out either by an independent monitoring body or by an auditor having relevant expertise to help find out, measure or map out impacts and risks over time.

During the preparation of the impact assessment, entities have to engage with stakeholders, including affected individuals, to assess the potential impact from their perspective.

Such impact assessments have to be carried out at regular intervals.

If a risk is identified, the entities concerned should be able to refer to any existing ethics committees, and to the competent supervisory authorities to examine the potential risks.

After completion of this assessment, entities should publish their assessment to receive views from the public on the potential deployment of facial recognition technologies.

4. Ethical Framework

Complementary to the respect of legal obligations, giving an ethical framework to the use of this technology seems to be a crucial issue. This could take the form of external ethics advisory boards that could carry out audits and publish the results of their research.

Furthermore, in order to avoid human rights abuses, conventions of experts from different fields of expertise would be likely to define the most potentially difficult cases when using facial recognition technologies.

On this topic, whistleblowers also have an important role to play, and employees of entities using these solutions should be able to benefit from an appropriate protection status, as provided for in particular in Recommendation (2014)7 on the protection of whistleblowers.

IV. RIGHTS OF DATA SUBJECTS

As facial recognition is based on the processing of personal data, all the rights provided for in Article 9 of Convention 108+ are guaranteed to the data subjects, such as notably the right of information, right of access, the right to obtain knowledge of the reasoning, the right to object, the right to rectification.

These rights can be fully or partially restricted if it is provided for by law and necessary and proportionate for legitimate purposes (such as law enforcement purposes), according to Article 11 of Convention 108+.

In the case of limitation of the rights of data subjects, law enforcement authorities have to inform data subjects about their right to lodge a complaint with supervisory authorities, and their general right to have a remedy.

In the case of false matches, data subjects can request the rectification to avoid further/repetitive false matches.

Where the use of facial recognition technologies is intended to enable a decision to be taken solely based on automated processing which would significantly affect the data subject, the latter must, in particular, have the right not to have such processing carried out without his or her views being taken into account.

In the deployment of live facial recognition technologies, if human operators solely act upon matches of these technologies, it can be considered as solely automated decision making which would significantly affect the data subject due to the consequences of possible false matches. The data subject can thus request that his or her views be taken into account.