Strasbourg, 12 December 2023 TPD(2023)2rev3Comp

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

CONVENTION 108

Compilation of Comments on Draft Guidelines on the protection of individuals with regard to the processing of personal data for the purposes of voter registration and authentication

***

www.coe.int/dataprotection

Table of Contents

ARGENTINA

Comments to the updated version of the draft Guidelines on the protection of individuals with regard to the processing of personal data for the purposes of voter registration and authentication", (T-PD(2023)2rev3).

In the first place, it is convenient to clarify that Argentina considers that the subject matter of this Guide, related to ensuring that there are sufficient safeguards in the registration and authentication of voters that incorporate biometric techniques -in line with the principles and provisions of the modernized Convention 108-, is an issue of utmost importance to guarantee the conditions that make the democratic systems of the different States.

Although most countries do not use these techniques today, we are aware that, in the future, it is very likely that the different jurisdictions will progressively begin to introduce them, which is why we consider it very appropriate to address these topics in advance.

Secondly, we inform you that, in our country, biometric techniques for identification and authentication of voters have not been introduced so far, and also that National Law No. 19.945 establishes the rules applicable to the election system through the National Electoral Code, being universal, secret, free and compulsory suffrage.

In effect, said norm is a legal basis that legitimizes the publicity of the voters' registry with the corresponding legal provisions of privacy.

In particular, article 25 of said Law contemplates the provisional registers, determining that "the National Voter Registry and the subregistries of voters of all districts are public in nature, with the corresponding legal privacy provisions, to be susceptible to corrections by the voters registered in them. The provisional registers are made up of data from the sub-registrations of voters by district, including the new ones registered up to one hundred and eighty (180) days before each general election, as well as people who turn sixteen (16) years of age up to the same. election day. The provisional voters' registers will contain the following data: number and type of civic document, surname, name and address of those registered. "They must be ordered by district and section".

In an amplifying manner, article 26 related to the "Dissemination of provisional registers", details that the National Electoral Chamber will publish the provisional registers and those of residents abroad ten (10) days after the closing date of the registry for each election, on its website and/or by other means that it considers convenient, with the corresponding legal privacy provisions, with the purpose that it is susceptible to corrections by the voters registered in it, as well as the advertising is founded to that voters can consult the registry to find out in which institution they can vote.

On the other hand, regarding the authentication of voters regarding their identity at the time of voting, we note that currently, in accordance with art. 86 of Law No. 19,945, voters may vote only at the vote receiving table where they are seated and the president of the table is the one who verifies whether the voter to whom the enabling civic document belongs appears on the electoral roll, checking whether the data match. personal data recorded in the register with the same information contained in the identity document.

Regarding electoral campaigns, it is worth mentioning that article 8 of Law 26,951 "National Do Not Call Registry" acts as a legitimizing basis, since it establishes as an exception the electoral campaigns established by the National Electoral Code (Law 19,945). That is to say, in these cases, the companies that carry them out are not covered by the National Do Not Call

Registry, unless they are directly or indirectly used for a commercial purpose and could not be carried out twenty-five (25) days prior to the date set for the holding of primary elections, open and simultaneous, and the general election.

Finally, it is worth mentioning that through Resolution No. 86/2019, the Agency promptly published the “Guide on the processing of personal data for electoral purposes”, whose objective is to ensure the integrity and protection of the personal data of participating citizens. in electoral processes, establishing a series of basic guidelines to be taken into account by groups, political organizations, candidates, think tanks, consultants and anyone who processes personal data in relation to an electoral campaign.

It is highlighted that this guide was prepared taking into account the work carried out by different organizations such as the Information Commissioner's Office (ICO) of the United Kingdom, the Spanish Data Protection Agency (AEPD) of Spain and the European Data Protection Committee, among others, which have addressed the relationship between personal data and the communication of political organizations towards voters, in a context of technological development and search for greater transparency.

Among some of its main guidelines, we highlight:

-The Principles of protection of personal data within the framework of the National Law on Protection of Personal Data No. 25,326: The data must be treated in accordance with the purpose declared at the time of obtaining them. The data may be used for other purposes that are compatible with the main purpose, if they may have been reasonably foreseen by the data owner (art. 4, subsections 1 and 3 of Law No. 25,326). The data collected must be proportional and not excessive in relation to the declared purpose (art. 4, subsection 1 of Law No. 25,326). The data must be accurate and must be updated, completed or deleted in the event of error, inaccuracy or infringement of another right of the data owner. Those who carry out any processing must periodically examine their database and, when appropriate, make the necessary corrections (art. 4, subsections 1, 4 and 5 of Law No. 25,326). Data collection cannot be done through unfair, fraudulent means or that in any way contradict the law (art. 4, subsection 2 of Law No. 25,326). The data must be stored in a way that allows its access by the owner (art. 4, subsection 6 of Law No. 25,326). The data must be destroyed when they are no longer necessary or relevant for the purposes for which they were collected (art. 4, subsection 7 of Law No. 25,326).

-Personal data that will be used to send electoral propaganda, such as email, social network account, instant messaging service or other similar information, must have been obtained lawfully, covered by one of the the legal bases contained in arts. 5 or 7 of Law No. 25,326.

-Personal data that reveal political opinions are considered sensitive data (art. 2 of Law No. 25,326). As a general criterion, the processing of sensitive data is prohibited (art. 7, subsection 3 of Law No. 25,326). This type of data may only be processed when there is consent, publication of the data, the processing has statistical purposes or there are reasons of general interest, provided by law, that justify it (arts. 5 and 7 of Law No. 25,326).

-It was highlighted that the guide must be interpreted and complemented with the full reading of Law No. 25,326, Regulatory Decree No. 1558/2001, Convention 108 for the Protection of Persons with respect to the Automated Processing of Personal Data and its Additional Protocol, and the regulations issued by the Agency for Access to Public Information, available on the web (https://www.argentina.gob.ar/aaip/buscador-normativa).

Finally, regarding the content of the Guidelines submitted for consideration, it is emphasized that Argentina considers the contributions made in this document very valuable, since it provides clear guidelines regarding the legitimacy of processing, special categories of personal data, security, transparency, rights, electoral management bodies and additional obligations for the processing of biometric data, taking into account that the legal frameworks might vary in the different States.

ARMENIA

In response to your letter sent on the 20 November 2023 we have analyzed the Draft Guidelines on the protection of individuals with regard to the processing of personal data for the purposes of voter registration and authentication.

In the present letter we would like to point out the importance of the explicit mention in the Guidelines about publication of list of voters who have already voted. Despite the fact that public authorities may provide legal basis for making special categories of personal data publicly available and try to provide appropriate guarantees to ensure the protection of personal data and privacy of individuals, nevertheless it is unlikely that in such case the rights of data subjects will be protected for the below mentioned reasons.

Firstly, the publication of list of people who have already voted reveals political choices of data subjects. Moreover, the abstention may also indicate a political choice (when people who have not voted are excluded from the list). This type of personal data processing represents serious risk of voter harassment and pressure. Secondly, such a publication of personal data significantly increases the risks of unlawful interference with the right to personal data protection, in particular, it increases the possibility of identity theft because a wide range of personal data, such as passport data or signatures, becomes publicly available.

Taking into account abovementioned reasons, we suggest to add a provision in 4.2. section, which will state that **the publication of the list of the voters who actually participated in the elections should be avoided.**

CABO VERDE

(…)

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

(…)

The statistical processing of personal data on voting trends by demographic or geographic variables would normally be considered a "compatible purpose" provided other safeguards exist to ensure the anonymisation or pseudonymisation of the data [1] Such processing should respect the secrecy of the ballot and should not lead to a disproportionate interference with the voters' interests, rights, and freedoms.

No ~~undue~~ influence or pressure should be exerted on a voter or potential voter to provide personal data for the purpose of voter registration.[2]

Commented [A1]: Encouraging moderate participation to provide personal data for voter registration purposes seems to us to be in the public interest in a democratic rule of law. On the other hand, registration in the electoral process can be used to determine the number of mandates to be elected and there are also cases of mandatory and automatic electoral registration.

4.2. Rights of data subjects (Article 9)

(…)

Data subjects shall have the right not to be subject to decisions significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration. For example, where data subjects are deregistered from a voting register (for reasons of [age], mental capacity, criminal record), they have the right to be informed of the reasons for the decision.

Commented [A2]: People who are incapacitated due to mental illness should be aware of the fact that communicating the reason for file deletion may cause serious inconvenience to data subjects. These are situations in which information can be provided to representatives.

[1] Explanatory report, para 50.
[2] Explanatory report, para. 42.

FINLAND

1. Introduction

Any jurisdiction that conducts elections needs reliable methods to ensure that only those eligible to vote are included in official electoral registers and that those who vote on election day are indeed, "who they say they are". Over time, different democratic countries have relied on a range of methods to support the goals of reliable and accurate voter registration and identification, and voter authentication. For more established democratic countries, systems of voter registration and authentication tend to be rooted in distinct institutional and administrative practices that produce strong legacies.

(…)

Biometric data is just one category of ~~sensitive~~ special categories of data given special protection by international instruments such as the Council of Europe's Convention for the protection of individuals with regard to the automatic processing of personal data (ETS No. 108) as amended by Protocol CETS No. 223[3] ("Convention 108+", "Convention") whose processing can lead to a variety of individual and social risks to privacy, and to other human rights. There are risks to the secrecy of the ballot, of voter intimidation and discrimination, of disenfranchisement of eligible voters, of security and data breaches, of the uses of official registration data for campaigning activities, and of the integration of voter registration databases with other national identifications systems.

(…)

This guidance addresses questions about the data ~~captured~~ collected and managed by official electoral management bodies (EMBs) and other authorities or bodies for the purpose of voter registration and authentication. The data controllers (or, where applicable, data processors) are therefore not political parties or other campaigning organisations, but the organisations (including EMBs) responsible for processing personal data on eligible voters for the purposes of voter registration, and voter authentication at the time and place that a ballot is cast in an election.

(…)

~~Supervisory~~ Relevant oversight authorities (could include~~ing~~ EMBs, data protection authorities (DPAs), and other oversight agencies) may wish to adapt these guidelines to their particular electoral systems. They may also wish to consider developing domestic codes of practice on voter registration and authentication, alone or in cooperation, sensitive to their domestic political systems, and consistent with ~~their~~ the responsibilities of DPAs under Article 15 of Convention 108+.

2. Scope and Purpose

(…)

Apply mainly to Electoral Management Bodies (EMBs) and/or to other regulatory and/or ~~supervisory~~ other authorities or bodies responsible for the protection of personal data as data

Commented [A3]: Finland: The "voter authentication" is defined later in the text, as referring to the verification of the eligibility to vote.

However, it could be useful to draw a distinction between voter authentication and voter identification. Particularly the draft guidance contains a section on the use of biometric data (or other means of uniquely identifying a natural person), it would be useful to even refer to the voter identification (or "verification of identity").

Depending on what methods of collecting voter data are used, the voter authentication may even take place without particularly identifying or verifying the voters, while the identity may be verified at the moment of voting.

Commented [A4]: Finland: data security?

Commented [A5]: Finland: Are only "identification systems" meant, or is there an intention to also refer to national population registers? (The latter are referred to in the draft guidelines below.)

If so, such risks could be managed by keeping the voter register separate from the population register, even where the data is derived from the latter.

Commented [A6]: Finland: It is not excluded that data processors could be used in some jurisdictions. Perhaps it could be taken into account.

Commented [A7]: Finland: The oversight authorities are defined below in the draft guidelines. However, it may still be confusing to speak of "oversight authorities" in the same sense as of DPAs. While it is possible that in some jurisdictions EMBs are given even a supervisory role as regards the processing of personal data, as there could be more than one DPA in a jurisdiction, it might still be advisable to draw a clear distinction between EMBs and DPAs.

Commented [A8]: Finland: Suggest deleting "supervisory" as "supervisory authorities" does not seem to work here, as they are most often understood as referring to DPAs. It is also difficult to see how DPAs could be "data controllers" which has been added to the text.

[3] Council of Europe (2018), *Convention for the protection of individuals with regard to the processing of personal data* (2018) at: https://rm.coe.int/convention-108-for-the-protection-of-individuals (hereafter Convention 108+).

controllers, thereby contributing ~~for the purposes of~~to the protection ~~ng~~ of the right to vote in a free and equitable manner.

Apply solely to the processing of personal data on voters (or potential voters). They do not apply to the processing of personal data on candidates, potential candidates, or employees and volunteers.

Recognise that most countries are experimenting with new forms of remote voting methods. These methods require new, and sometimes, different forms of authentication from those used for in-person voting.

Recognise and support the broader global development on rights to a digital identity and complement the Guidelines on National Digital Identity adopted by the Consultative Committee of Convention 108.

Recognise that voter registers and voter lists may be assembled and maintained in a variety of ways and locations using both digital and non-digital media by a range of national and local authorities.

Recognise that the names and addresses of voters in the voters lists (based on the voter register) are legally shared in some jurisdictions with registered political parties and candidates for campaigning purposes, and that their use should be restricted by law to legitimate purposes of campaigning activities.

Recognise that different administrative and institutional factors shape the conduct of elections and the personal data processing practices in elections: the electoral system; the party system; the relationship between central and local party organisations; the existence of "primary elections"; the frequency of referendums; and others.

Recognise that many countries have introduced, or will introduce, biometric forms of identification to register and authenticate voters, and that safeguards are necessary against the risks that the processing of biometric data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination. (Such safeguards should be considered already before introducing biometric forms of identification, even where the introduction of biometrics is not being actively ~~considered~~implemented).

3. Definitions for the purposes of the Guidelines

In addition to the definitions stipulated in Article 2 of Convention 108+, the guidelines use the following terms to ensure a uniformity of definition:

"~~Supervisory~~ Relevant oversight authorities" refer to those independent regulatory agencies that might have oversight responsibility for the processing of personal data for electoral purposes, ~~and includes~~including data protection authorities (DPAs) and election management bodies (EMBs)

"Electoral Management Bodies" (EMBs) refers to those national authorities responsible for the regulation of the safe and efficient conduct of elections, the implementation of election finance provisions, and (where applicable) for the development and management of the national voter register as a data controller.

Voter registration refers to the process for collecting, assembling, and maintaining relevant information on individuals included in the voter register.

Commented [A9]: Finland: Suggest adding "or processors" (see above).

Commented [A10]: Finland: In case the guidance will apply to the processing of personal data in the context of both in-person and remote voting, should it be made more specific e.g. at the beginning of this section – or is it evident that the scope covers both?

Commented [A11]: Finland: Not only such further use should be restricted by law, but even the processing of voters' personal data for electoral purposes, for which they have been collected, should have a legitimate basis laid down by law (Article 5). In addition, the processing should be lawful.

Commented [A12]: Finland: Suggest adding some text from Article 6 to clarify what is meant by safeguards.

Commented [A13]: Finland: Could this be clarified – e.g. by using a separate sentence? It is difficult to see what is meant by "actively considering". The sentence could be formulated differently, depending on what is meant by the author.

Commented [A14]: Finland: See also our comment above. It is not excluded that in some jurisdictions the responsibility for overseeing the lawfulness of processing of personal data is vested in an authority or agency other than the DPA. It is nevertheless important that those two are not confused. However, it would be more customary to understand the role of EMBs as referring to the conduct of elections. At the same time, the EMB may be defined (by law) as a data controller.

It might be better to define DPAs (having responsibility for supervising the processing of personal data) and EMBs (having responsibility for the conduct of elections etc.), instead of "relevant oversight authorities" and EMBs.

Commented [A15]: Finland: Suggest separating the last part of the sentence to draw a clearer distinction with the electoral functions and those relating to the role of a data controller.

Commented [A16]: **SECRETARIAT** : **The changes in this commented part of the paragraph** is made by the secretariat.

Commented [A17]: Finland: As an observation, there may be different solutions even as regards the collection of voter data. For example, in Finland the data is derived from the population register, although the final voter register is separate.

Voter registers are the consolidated, official lists of all persons eligible to vote and the underlying personal data processed for this purpose ~~[.]~~

Voter lists refer to the list of all persons registered to vote in a particular electoral district or constituency for a particular election.

Depending on the jurisdiction, different data controllers (or processors) might be responsible for the management and processing of voter registers and voter lists including: national and regional EMBs; local government authorities responsible for population registration and the conduct of elections; and statistical agencies.

(…)

Personal data revealing "political opinions" are a special category of data under Article 6 of the Convention and may include data on voting activity, including: whether the voter has voted; taking into account the underlying context and/or together with other personal data the place of voting; and the method of voting.

Commented [A18]: Finland: The added elements are important to highlight that not all information on voters/ voting activity express a political opinion. However, there is still uncertainty as to how the information on whether the voter has voted, the place of voting and the method of voting would express a political opinion, unless data on "which candidate the voter has voted for" is revealed at the same time.

Biometrics refers to data resulting ~~to~~ from the automated recognition that is a specific technical processing of data concerning ~~of~~ individuals based on their distinguishing and repeatable biological (physiological), biological and/or behavioural characteristics which allows the unique identification or authentication of the individual, when it is precisely used to uniquely identify the data subject.

Commented [A19]: Finland: This text is a bit confusing. The Convention does not include a detailed definition of biometric data, whereas the GDPR definition reads as follows:
"'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;"

Is "biometrics" rather a different concept? If we wish to define "biometric data", it might be better to use that concept, and even using the GDPR definition which is the closest source.

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

(…)

The legitimate purpose of voter registration and authentication is to enable the right to vote for all ~~legitimate~~ eligible voters in a given electoral district. These purposes and means should be stated as precisely and fully as possible in publicly available documents, according to the transparency principle (Article 8). Further processing should be compatible with this stated purpose, under Article 5(4)b.

A "legitimate basis laid down by law" (Article 5(2)), for the collection of personal data, should ~~normally~~ be included in an applicable electoral legislation. Where the public interest in democratic engagement is the legitimate basis for processing, ~~those interests~~that interest should be clearly stated by law and duly referenced in the privacy policy of EMBs.

Where consent is necessary for voter registration, (Article 5(2)), the processing of personal data should be based on the free, informed, and unambiguous consent of the data subject. Consent should not be inferred through "silence, inactivity or pre-validated forms or boxes."[4]

Unless prohibited by law, the voter may withdraw his or her consent to be included in the voter register at any time.[5]

Personal data on voters' registration should not be used for other purposes unless there is a legitimate basis laid down by law, and should not be further used for "undefined, imprecise or

Commented [A20]: Finland: There could be legitimate further processing purposes defined by law, not only the campaigning purpose referred to in the introductory part of the guidance. In any case, the purpose should be based on law, and the processing should be limited to what is necessary and proportionate.

[4] Explanatory report, para 42
[5] Explanatory report, para. 45.

vague purposes"[6]. A reliance on the concept of "compatible uses" should not hamper the transparency, legal certainty, predictability or fairness of the processing. [7]

Commented [A21]: Finland: On occasion, the concept of "compatible purposes" is also confused with that of "derogation from the principle of purpose limitation", which should be as narrow as possible.

Personal data on voters should not be further processed in a way that the voter might consider "unexpected, inappropriate or otherwise objectionable."[8]

The following paragraphs are to be interpreted in line with the generally recognised principle of the secrecy of elections and are without prejudice to domestic rules on access to public information. Where political campaign organisations and their candidates legally acquire the official voters list from the EMB to assist their campaigns, the law should stipulate who is entitled to access these data, for what purposes, and for how long. The sharing of voters' lists should be limited to what is necessary for engaging with the electorate with clear prohibitions and appropriate sanctions for using the data for any other purposes.

Commented [A22]: Finland: It is important to refer to the domestic rules on access to public information. This sentence is particularly useful.

Personal data contained in official voters list are not to be further processed or shared with third parties without express authorisation in law/appropriate legal basis. Unless specifically approved by law, name and addresses from the official voters list should not be combined with other sources of personal data processed by political parties or other campaign organisations to create profiles of voters for micro-targeting purposes.

The statistical processing of personal data on voting trends by demographic or geographic variables would normally be considered a "compatible purpose", provided ~~other~~ that appropriate safeguards exist to ensure the protection of personal data, particularly through the anonymisation or pseudonymisation of the data [9]. Such processing should respect the secrecy of the ballot, and should not lead to a disproportionate interference with the voters' interests, rights, and freedoms.

No ~~undue~~ influence or pressure should be exerted on a voter or potential voter to provide personal data for the purpose of voter registration.[10]

EMBs or other agencies might be required to collect and report information on donors to the campaign under relevant election financing laws. Personal data collected under this legal authority should only be used for purposes stipulated in applicable election or party financing legislation, and consistent with applicable data protection law.

Commented [A23]: Finland: Should this paragraph be rather placed at the end of the section? It is correct that such requirements may exist, although they may be based on separate legislation. It is not always the EMBs that have this obligation – they might not even have the relevant data. There may also be specific registers established for the purpose of maintaining information on donors.

Where EMBs obtain personal data from other authorities (such as tax authorities, or population registries) those data should only continue to be used based on a legitimate base, for the defined and specified purpose and should only be retained for as long as necessary to register the voter.

In states where those under the age of 18 may legally vote, EMBs should take special care to protect the personal data of young people according to Article 15(e).[11]

EMBs have the responsibility to ensure that personal data is accurate, complete and where necessary kept up to date.

[6] Explanatory report, para 48.
[7] Explanatory report, para 49.
[8] Explanatory report, para. 49.
[9] Explanatory report, para 50.
[10] Explanatory report, para. 42.
[11] Explanatory report, para. 125.

The EMB should not be transferring those data to other organisations for processing even in aggregate form, unless there is ~~outside of the~~a controller-processor relationship, without having a legal basis or obtaining the express consent of the voter.

Commented [A24]: Finland: Would this formulation be better?

4.2. Processing of special categories of data (including biometric data) that uniquely identifies an individual for voter registration and authentication (Article 6)

All personal data on voters which reveals the political opinion of an individual in the context of voting, or on occasion in the context of voter registration and authentication, should be considered a special category of data.

Commented [A25]: Finland: The Plenary discussed the aspect that not all voter data is necessarily a special category of personal data, i.e. where it does not reveal a political opinion. It is rather typical that it is only the vote that expresses the political opinion. It is also typical that the personal data are kept separate from the ballot expressing the vote, to ensure secrecy.

Should the voting process be covered here?

According to Article 6(1) of Convention 108+, “personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of the Convention.” According to Article 6(2): “Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.”[12]

According to Article 6(1) “biometric data uniquely identifying a person” is also a special category that shall also “only be allowed where appropriate safeguards are enshrined in law, complementing those of the Convention.” (see 4.7 below)

In the context of voter registration, the recording of information on whether or not the individual voted in a particular election is information that may reveal political opinions, unless it is kept separate from the ballots expressing the votes. The recording over time of voting histories is also information that may reveal political opinions. These are all personal data falling within the special categories of data under Convention 108+. The processing of ~~those~~that information might also fall under the domestic legislation on access to official documents.

Commented [A26]: Finland: Drafting suggestion.

In some countries, various individuals might be legitimately prohibited from voting on the grounds of criminal record, mental capacity, [] . These data are special categories data which can lead to unlawful discrimination and are therefore subject to the highest safeguards.

The processing of personal data revealing political opinions entails severe risks of voter discrimination and can lead to voter suppression and intimidation. The knowledge of who has, and has not, voted can (in some societies) also affect the provision of government services. The processing of special categories of personal data needs to be accompanied by safeguards appropriate to the risks at stake of voter discrimination and of the interests, rights and freedoms protected and has to take into account the domestic legislation on access to official documents as well.

Commented [A27]: Finland: It is important to take into account the domestic legislation on access to official documents. There may also be specific provisions on publicity also in the legislation on elections, but “legislation on access to official documents” would to our understanding cover both. However, would it be better to have a more general separate sentence (in the same way as on page 6), to cover all the necessary processing contexts referred to in this chapter?

The legislation on access to official documents typically includes provisions on secrecy obligations, which could cover e.g. special categories of personal data. Despite that, the second addition might not be understood correctly.

(…)

4.4. Transparency of processing of personal data for voter registration and authentication (Article 8)

(…)

In countries in which registration is self-directed, the individual should be clearly informed at the time of registration how his/her personal data will be used, the purposes for which it is processed, and any third-party processors to whom it might be communicated.

Commented [A28]: Finland: Could this be clarified?

[12] Convention 108+, Article 6

In countries that pursue voter registration drives at household levels, individuals should be clearly told the purpose of the data collection, and the legal basis for the registration.

(…)

4.5. Rights of data subjects (Article 9)

(…)

Data subjects have to be given the possibility ~~-~~to request rectification or erasure, if applicable ~~and/or concerning the inaccurate data~~, as the case may be, if the data is inaccurate, obsolete or incomplete.[13]

(…)

Data subjects should be able to object to the processing of data on him or her with an EMB or the competent authority at any time to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms.

Commented [A29]: Finland: Could this be clarified? Also, does it mean the same as self-directed?

Commented [A30]: Finland: "inaccurate" is mentioned twice.

Commented [A31]: Finland: It is not sure if "at any time" works here. For those applying the GDPR, the legal basis of processing could be a legal obligation of the controller (Article 6(1)(c)), which in principle excludes the possibility of objecting to the processing. Instead, where the legal basis of processing is a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e)), this addition would work.

The Convention does not go into as many details as the GDPR.

[13] Explanatory report, para. 72.

~~and to request rectification or erasure, as the case may be, if the data is inaccurate, obsolete or incomplete.[14]~~

(…)

4.6. Additional obligations and recommendations for Election Management Bodies and other authorities (Article 10)

The ~~obligation rests with the~~ data controller and, where applicable, the processor should ~~to~~ ensure adequate data protection and ~~to~~ should be able to demonstrate that data processing ~~follows~~ is in conformity with the data protection law and other applicable laws. The ~~accountability~~ responsibilities of data controllers and data processors should be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10(1) of Convention 108+.

Commented [A32]: Finland: This could be written even more in line with Article 10(1).

Commented [A33]: Finland: The term "responsibilities" would be better (as in the GDPR).

EMBs and ~~the~~ any processors used should provide a full record of how personal data has been obtained and is being processed, as well as demonstrate compliance of any third-party organisation that processes personal data on their behalf.

EMBs should assess the likely impact of intended data processing on the rights and fundamental freedoms of the voter, prior to collection and the commencement of data processing and should design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms (Article 10(2)).

Data protection assessments should assess the specific impact the intended processing on data subjects' rights but also consider whether ~~the~~ specific processing ~~is~~ operations are in the best interests of broader democratic values and the integrity of democratic elections.

Commented [A34]: Finland: Drafting suggestion. The processing as such is most likely based on the statutory obligation of the controller (particularly in the case of the EMB). However, there could be reason to assess specific methods of processing or even individual processing operations, particularly in the light of the risks (e.g. whether the use of biometrics is necessary as required by the Convention, and in that case whether there are appropriate safeguards in place).

Article 35 of the GDPR could be used as a source of inspiration, as the Convention does not go into details about the impact assessment.

(…)

4.7. Additional Obligations for processing of biometric data for voter registration and authentication

Biometric data, ~~using~~ resulting from specific technical ~~means~~ processing relating to the physical, physiological or behavioural characteristics of a natural person, ~~to~~ which allow to uniquely identify an individual, is classified as a special category of data under Article 6 of Convention 108+.

Commented [A35]: Finland: Suggest supplementing the text. See also above the comment on "biometrics".

(…)

Biometric forms of identification for voter registration and authentication purposes should be assessed in light of the proportionality and necessity of the processing, and should only be introduced if other existing (legacy) forms of identification and authentication have been demonstrably shown to be inadequate, inaccurate and/or contrary to the rights of the individual.

The application of biometrics for the purposes of voter registration and authentication should only be grounded in a legal framework which should specify: the specific purpose of the biometric; standards on the minimum reliability and accuracy of the specific technology or algorithm used (such as the false positive and false negative error rates); the retention period of the biometric form used; the requirement for ~~auditing~~ prior consultation by a supervisory

Commented [A36]: Finland: In case it is not always an algorithm that is used.

Commented [A37]: Finland: The supervisory authorities are typically (e.g. under the GDPR) consulted, whereas auditing could be carried out by a specific body (certified body).

authority; the traceability of the use and sharing of the biometric form; and the safeguards used.[15]

The application of biometric forms of identification (~~and~~ especially facial recognition) should only be for purposes of voter registration and authentication and should not be processed to infer race, ethnic origin, age, health or other social conditions.

Where facial recognition is used, no digital images should be used that were uploaded to the internet or social media sites, or captured by video surveillance.[16]

No biometric data should ever be shared with political parties, political candidates or campaign organisations, unless explicitly authorised by law.

Developers and manufacturers of biometric technologies for the purposes of voter registration or authentication ~~shall~~ should take steps to ensure that the biometric data are accurate under Article 5. This involves continual testing their systems to eliminate disparities, particularly according to ethnicity, age and gender. They should integrate data protection by design principles into the manufacture of biometric products and services. They should also examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of the data processing and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms. The moreover should implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

In compliance with Article 15(3), supervisory authorities ~~shall~~ should be consulted on proposals for the introduction of biometric forms of identification for voter registration and authentication. These authorities ~~shall~~ should be consulted ~~systematically and~~ in advance of the deployment of biometric voter registration schemes.

Commented [A38]: Finland: It is difficult to see what would be the legitimate need even if authorised by law. It would be useful to hear examples from the expert.

Commented [A39]: Finland: This appears to be the only paragraph to be applied to developers and manufacturers. Should there be a separate section (with the heading "Developers and manufacturers")?

Commented [A40]: SECRETARIAT : This change is made by the secretariat.

Commented [A41]: Finland: Suggest deleting "systematically" as it might be read as meaning more than what is required e.g. by the GDPR. It is clear, however, that the use of biometric forms would easily fall within a category of processing for which prior consultation would be required.

[15] Guidelines on facial recognition, p. 7.
[16] Guidelines on facial recognition, p. 9.

GERMANY

1. Introduction

(…)

Biometric data is just one category of special categories of data given ~~special~~ additional protection by international instruments such as the Council of Europe's Convention for the protection of individuals with regard to the automatic processing of personal data (ETS No. 108) as amended by Protocol CETS No. 223[17] ("Convention 108+", "Convention") whose processing may entail a particular risk for data subjects and can lead to a variety of individual and social risks to privacy, and to other human rights. In the context of these Guidelines t~~T~~here are especially risks to the secrecy of the ballot, of voter intimidation and discrimination, of disenfranchisement of eligible voters, of security and data breaches, of the uses of official registration data for campaigning activities, and of the integration of voter registration databases with other national identifications systems.

Commented [A42]: Editorial to avoid repetitive use of "special"

Commented [A43]: See Explanatory Report of the Convention (ER) 57

Commented [A44]: This is a general data protection concern and does not really fit in with the others – could be deleted

(…)

Other recent guidelines on the application of Convention 108 may also relate to the processing of personal data for purposes of voter registration and authentication: on digital identity; on political campaigning; on artificial intelligence;[18] and on facial recognition.[19]

Commented [A45]: Footnotes missing

(…)

2. Scope and Purpose

(…)

Recognise and support the broader global development on rights to a digital identity and complement the Guidelines on National Digital Identity adopted by the Consultative Committee of Convention 108.

Commented [A46]: Footnote missing

(…)

3. Definitions for the purposes of the Guidelines

(…)

"Electoral Management Bodies" (EMBs) refers to those national authorities responsible for the regulation of the safe and efficient conduct of elections, the implementation of election finance provisions and (where applicable) the development and management of the national voter register ~~as a data controller~~.

Commented [A47]: This addition in the definition part seems like an unnecessary

Voter registration refers to the process for collecting, assembling, and maintaining relevant information on individuals included in the voter register.

[17] Council of Europe (2018), *Convention for the protection of individuals with regard to the processing of personal data* (2018) at: https://rm.coe.int/convention-108-for-the-protection-of-individuals (hereafter Convention 108+).

[18] Council of Europe (2019). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on artificial intelligence* and data protection. Strasbourg: Council of Europe (adopted 25 January 2019)

[19] Council of Europe (2021). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on Facial Recognition.* Strasbourg: Council of Europe (adopted 2021)

Voter registers are the consolidated, official lists of all persons eligible to vote and the underlying personal data processed for this purpose

Commented [A48]: It is unclear what is meant here

(…)

Personal data revealing “political opinions” are a special category of data under Article 6 of the Convention and may include data on voting activity, including: whether the voter has voted;~~ taking into account the underlying context and/or together with other personal data the place of voting~~; and the method of voting.

Commented [A49]: Even with the addition (context…)it is not exactly clear why the place of voting reveals a “political opinion”

Processing of b~~B~~iometric data~~s~~ refers to data resulting from ~~the automated recognition that is~~ a specific technical processing of data concerning the physical ~~individuals based on their distinguishing and repeatable~~ biological or ~~(~~physiological~~), biological and/or behavioural~~ characteristics which allows the unique identification or authentication of the individual, when it is precisely used to uniquely identify the data subject.

Commented [A50]: See definition in ER 58 Convention 108+

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

Personal data on voters should be processed lawfully and in accordance with the principles set out in Article 5 of Convention 108+: proportionality, lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, and security. Processing should be proportionate in relation to the legitimate purposes of the data processing, reflecting the rights and freedoms at stake.

The legitimate purpose of voter registration and authentication is to enable the right to vote for all legitimate voters in a given electoral district. These purposes and means should be stated as precisely and fully as possible in publicly available documents, according to the transparency principle (Article 8). Further processing should be compatible with this stated purpose, under Article 5(4)b.

Commented [A51]: This could moved to 4.4

A “legitimate basis laid down by law” (Article 5(2)), for the collection of personal data, should be included in an applicable electoral legislation. Where the public interest in democratic engagement is the legitimate basis for processing, those interests should be clearly stated by law and duly referenced in the privacy policy of EMBs.

Where consent is necessary for voter registration, (Article 5(2)), the processing of personal data should be based on the free, informed, and unambiguous consent of the data subject. Consent should not be inferred through “silence, inactivity or pre-validated forms or boxes.”[20]

Commented [A52]: As the explanatory does not explicitly refer to voter registration, this should be reflected in the footnotes → “cf.”

If the voter registration was based on consent and ~~U~~unless prohibited by law, the voter may withdraw his or her consent to be included in the voter register at any time.[21]

Commented [A53]: To clarify about what scenario we are speaking here

Commented [A54]: The data minimization [Article 5 (4) c] Convention 108+] may be essential to promote confidentiality to take part in elections without fear.

The principle of purpose limitation (Article 5 (4)(b)) foresees that personal data shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes. Personal data on voters’ registration should – in general - not be used for other purposes, and should especially not be further used for “undefined, imprecise or vague purposes”[22]. When considering “compatible uses” a~~A~~ reliance on the

Commented [A55]: Addition suggested to lay down the principle even more clearly

[20] Cf. Explanatory report, para 42
[21] Cf. Explanatory report, para. 45.
[22] Cf. Explanatory report, para 48.

concept ~~of “compatible uses”~~ should not hamper the transparency, legal certainty, predictability or fairness of the processing.[23]

(…)

Personal data contained in official voters list are not to be further processed or shared with third parties without express authorisation in law/appropriate legal basis. Unless specifically approved by law, name and addresses from the official voters list should not be combined with other sources of personal data processed by political parties or other campaign organisations to create profiles of voters for micro-targeting purposes.

(…)

Where EMBs obtain personal data from other authorities (such as tax authorities, or population registries) those data should only continue to be used based on a legitimate base, for the defined and specified purpose and should only be retained for as long as necessary to register the voter or to keep the register up to date.

(…)

4.2. Processing of special categories of data (including biometric data) that uniquely identifies an individual for voter registration and authentication (Article 6)

All personal data on voters which reveals the political opinion of an individual in the context of voter registration and authentication should be considered as a special category of data.

(…)

In some countries, various individuals might be legitimately prohibited from voting on the grounds of criminal record or~~,~~ mental capacity~~,~~ [] . These data are special categories data in accordance with Article 6(1) which can lead to unlawful discrimination and are therefore subject to the highest safeguards.

(…)

[EMBs should not use data in the voter register for purposes of promoting democratic participation and encouraging voter turnout unless permitted by law. If consent can be an appropriate legal basis for such processing the consent shall be free, informed, and unambiguous]

4.3. Data security and confidentiality (Article 7)

Applying appropriate security measures to voter registration data, for each processing, and its processing environments both at rest and in transit, is vital to ensure voters’ data are protected to the highest standards. Security measures should take into account the current state of the art data-security methods and techniques in the field of data processing. [Their [cost] should be commensurate with the seriousness and probability of the potential risks.][24]

Risk assessment prior to processing should assess whether data is protected against unauthorised access, modification and removal/destruction taking into account inter alia the high potential adverse consequences for the individual, the sensitive nature of the personal data, the volume of personal data processed, the degree of the vulnerability of the technical architecture used for the processing, the need to restrict access to the data, requirements concerning long-term storage. Risk assessment should seek to embed these high standards

Commented [A56]: Independent from the legal basis, what could justify to combine these personal data to create personal political profiles?

Commented [A57]: editorial

Commented [A58]: We would be in favor of deletion as this is not strictly necessary for the Guidelines and could be misunderstood.

Commented [A59]: See ER 62

Commented [A60]: As this is verbatim from ER 63, this could be kept in.

Commented [A61]: See ER 62

[23] Cf. Explanatory report, para 49.
[24] Cf. Explanatory report, para 63.

of security throughout the processing. Such an assessment should be informed by considerations of necessity and proportionality, and the fundamental data protection principles across the range of risks including physical accessibility, networked access to devices and data, and the backup and archiving of data.

Commented [A62]: We suggest to move the paragraph up here for systematic reasons.

Commented [A63]: This seems unclear and a bit mixed up with requirements of Article 10(2)

The authentication of voters during an election often involves the sharing of data on voters with large numbers of volunteers, contractors and employees during the intense period of elections. EMBs should take appropriate security measures to ensure against accidental or unauthorised access to, destruction, loss, use, modification, or disclosure of personal data.

Security measures should include: training in privacy and security; access controls; confidentiality agreements; controls on physical access to places, ~~possibility of checking the resilience of security measures under a false name~~ and equipment where personal data in the voter register or the voter lists are stored. This could also e. g. include the possibility of checking the resilience of security measures under a false name.

Commented [A64]: This is one possibility to ensure security measure. See suggestion for rewording

EMBs should train all workers and volunteers in the importance of privacy and data security measures with regard to the voter register and the voters lists. Each employee or volunteer should have to be under confidentiality obligations. The voter register and voter lists should be protected by strong access controls for different categories of employees and volunteers.

Commented [A65]: As the paragraph above refers to the training in privacy we suggest to move the paragraph here

EMBs should report to supervisory authorities as prescribed by Convention 108+ and to the data subjects themselves in the event of data breaches which may seriously interfere with the rights and fundamental freedoms of voters in accordance with Article 7(2) of the Convention 108+. Notification should include adequate and meaningful information about possible measures to mitigate the adverse effects of the breach.[25]

Where voter registration data is processed by third party service providers, these should be carefully selected in accordance with the applicable law. EMBs need to be~~should remain~~ aware of their ongoing responsibilities as data controllers. Controllers should be able to demonstrate, that processors comply with their obligations in accordance with Articles 7(1) and where applicable 10 of the Convention 108+.

Commented [A66]: For clarification purposes

~~Risk assessment prior to processing should assess whether data is protected against unauthorised access, modification and removal/destruction. Risk assessment should seek to embed high standards of security throughout the processing. Such an assessment should be informed by considerations of necessity and proportionality, and the fundamental data protection principles across the range of risks including physical accessibility, networked access to devices and data, and the backup and archiving of data.~~

~~EMBs should train all workers and volunteers in the importance of privacy and data security measures with regard to the voter register and the voters lists. Each employee or volunteer should have to be under confidentiality obligations. The voter register and voter lists should be protected by strong access controls for different categories of employees and volunteers.~~

4.4. Transparency of processing of personal data for voter registration and authentication (Article 8)

Personal data has to be processed fairly and in a transparent manner (Article 5(4)(a). ~~The~~ This means personal data ~~[]~~shall be processed fairly and in a transparent manner at all stages of the electoral process, especially considering the potential for the manipulation of voters.

Commented [A67]: Suggestion to recall the principle from the Convention

[25] Cf. Explanatory report, para 66.

~~Depending on the source of the voter register,~~In principle EMBs should inform voters ~~(in a privacy policy or its equivalent)~~ of at least: ~~the~~ its legal name and address~~ of the organisation~~; the legal basis for the processing of personal data and the purposes of the intended processing; the categories of personal data processed; any recipients or categories of recipients of those data (including third-party processors), and the reasons why they need to be shared; and how the voter might exercise his/her data subject's rights in accordance with Article 9 (Article 8 (1)). The data controller may use any available, reasonable and affordable means to inform the data subjects collectively (through a website or public notice) or individually.

Commented [A68]: See addition below

Commented [A69]: See Article 8 (1)

Commented [A70]: This is actually not directly foreseen by Article 8 (1)

Commented [A71]: See ER 70

Where the personal data are not directly collected from the data subject, e. g. where the registers are constructed from existing state registers (e.g., population databases, tax records, census records) the data controller is not required to inform individuals provided the processing is expressly provided by law, or if it would require disproportionate effort.[26]

In countries in which registration is self-directed, the individual should be clearly informed at the time of registration how his/her personal data will be used, the purposes for which it is processed, and any third-party processors to whom it might be communicated.

In countries that pursue voter registration drives at household levels, individuals should be clearly told the purpose of the data collection, and the legal basis for the registration.

The privacy policies of EMBs should be easily accessible, legible, understandable and adapted to the relevant individuals.[27] Communication methods should not dilute the explanations that are necessary for fair processing but should not be excessive. Layered privacy notices could help to combine the need for complete, but at the same time accurate information.

Commented [A72]: Not exactly sure what is meant here: The information must be provided "when" collecting the data.

4.5. Rights of data subjects (Article 9)

Commented [A73]: We suggest a slight restructuring and rewording with a view to the wording of the Convention in Article 9

Data subjects should be able to obtain on request at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her in a voter register, all available information on their origin and on the preservation period and to access to those data in an intelligible form (Article 9(1)(b)). That means that data subjects are entitled to be informed, upon request, how their personal data was obtained for the voter register, and from what source.

Commented [A74]: See Article 9(1)(b)

Data subjects have to be given the possibility to request rectification or erasure, if applicable and/or concerning the inaccurate data, as the case may be, if the data is inaccurate, obsolete or incomplete (Article 9(1)(e)).[28]

Data subjects shall have the right not to be subject to decisions significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration (Article 9(1)(a)) unless the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests (Article (9)(2)).~~.~~

Data subject shall have the right to be provided, on request, with knowledge of the reasoning underlying data processing where the results of such processing are applied to them (Article 9(1)(c)). For example, where data subjects are deregistered from a voting register (for reasons of [age], mental capacity, criminal record), they have the right to be informed of the reasons

[26] Convention 108, Article 8(3)

[27] Cf. Explanatory report, para. [12.]

[28] Cf. Explanatory report, para. 72.

for the decision. This might also be particularly important where a voter has been denied registration.

Data subjects ~~should~~ shall have the right ~~be able~~ to object to the processing of data on him or her with an EMB or the competent authority on grounds relating to his or her situation at any time to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms (Article 9(1)(d))~~.~~ The purpose of ensuring voter registration and authentication would be such an legitimate ground.

~~Data subjects are entitled to be informed how their personal data was obtained for the voter register, and from what source~~.

~~Data subjects are, upon request under Article 9(1)(b &c), entitled to be informed without excessive delay and expense, about the reasoning underlying the processing of their personal data by EMBs, of the data processed and its origin, and of the preservation period. This might be particularly important where a voter has been denied registration~~.

Commented [A75]: See rewording abov

Data subjects are entitled to remedy under applicable law if their rights under the Convention are violated (Article 9(1)(f)).

Data subjects are entitled to benefit from the assistance of a supervisory authority in exercising his or her rights (Article 9(1)(g)).

4.6. Additional obligations and recommendations for Election Management Bodies and other authorities (Article 10)

The accountability principle obliges data controllers, and where applicable processors, ~~The obligation rests with the data controller~~ to take appropriate measures to ensure adequate data protection and to be able to demonstrate that their data processing follows applicable laws.

~~The accountability of data controllers and data processors should be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10(1) of Convention 108+.~~

Commented [A76]: Moved below

Appropriate measures might include that EMBs as data controllers and the processors should provide a full record of how personal data has been obtained and is being processed, as well as demonstrate compliance of any third-party organisation that processes personal data on their behalf. The accountability of data controllers and data processors should be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10(1) of Convention 108+.

Other measures can include setting up internal procedures to enable the verification and demonstration of compliance or training employees. The designation of a “data protection officer” entrusted with the means necessary to fulfil his or her mandate could facilitate this process. With a view of the sensitivity of the data processed an the importance of election in a democratic country such an designation should be strongly considered.

Commented [A77]: See ER 85 and 87

EMBs should assess the likely impact of intended data processing on the rights and fundamental freedoms of the voter, prior to collection and the commencement of data processing and should design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms (Article 10(2)).

Data protection assessments should assess the specific impact on data subjects’ rights but also consider whether the processing is in the best interests of broader democratic values and the integrity of democratic elections.

EMBs should encourage and implement a comprehensive and compliant data governance culture ~~throughout the [political organisation],~~ both during and between election cycles.

Commented [A78]: Maybe this could be also deleted

~~EMBs should appoint an officer responsible for the verification and demonstration of~~

Commented [A79]: See wording proposal above. Within the logic of the Convention it remains the responsibility of the controller to verify and demonstrate the compliance

Proactive guidance on best practices in the conduct of elections is of critical importance. The risks to human rights from the processing of voting data cannot simply be understood in response to individual complaints to particular EMBs at the time of elections.

Supervisory (data protection) authorities can also assist EMBs within the scope of their competencies. They have valuable experience in the detailed and practical work of data protection implementation and privacy management and can assist in the tailoring of rules to the electoral context.

While the implementation of these guidelines will be shaped by local political contexts, it may also require collaboration between supervisory authorities.~~ []~~ The impact of this industry nationally and internationally will require the most vigilant and constant cross-national attention from EMBs and supervisory authorities through their international and regional associations.

4.7. Additional Obligations for processing of biometric data for voter registration and authentication

Biometric data, using technical means to uniquely identify an individual, is ~~classified~~ protected as a special category of data under Article 6 of Convention 108+.

The context of processing of biometric forms of identification for purposes of voter registration and authentication also establishes heightened levels of sensitivity given that personal data revealing political opinions is also defined as a special category.

The processing of special categories of data shall only be allowed where appropriate safeguards are enshrined in law complementing those in Convention 108+, guarding against the risks that the processing of sensitive data poses for the interests, rights and fundamental freedoms for the data subject, and notably the risk of discrimination.[30]

The integration of biometric forms of identification resulting from automated recognition into existing voter registration databases poses serious risks to the privacy of individuals, when the application of these technologies does not always require the awareness or cooperation of individuals.[31]

Commented [A80]: What is meant here?

Commented [A81]: The procession of personal data (especially biometric data) for voter registration and authentication may include serious risks (not only for privacy but also) for the democratic rights of eligible voters, e.g. the risk to be excluded from voting unlawfully.

Biometric forms of identification resulting from automated recognition for voter registration and authentication purposes should be assessed in light of the proportionality and necessity of the processing, and should only be introduced if existing (legacy) forms of identification and authentication have been demonstrably shown to be inadequate, inaccurate and/or contrary to the rights of the individual.

Commented [A82]: To differentiate from "just" using a photo ID when the EMB authenticates the voter

Commented [A83]: On the other hand, registration and automated recognition of registered voters by technical means may not always be reliable. Even with a very high level of reliability errors can occur. Precautions should be taken to deal with such errors, e. g. measures to ensure that voters can prove their identity in an alternative way.

The application of biometrics resulting from automated recognition for the purposes of voter registration and authentication should only be grounded in a legal framework which should specify: the specific purpose of the biometric; standards on the minimum reliability and accuracy of the algorithm used (such as the false positive and false negative error rates); the retention period of the biometric used; the requirement for auditing by a supervisory authority; the traceability of the use and sharing of the biometric; and the safeguards.[32]

The application of biometric forms of identification resulting from automated recognition (and especially facial recognition) should only be for purposes of voter registration and authentication and should not be processed to infer race, ethnic origin, age, health or other social conditions.

Where facial recognition is used, no digital images should be used that were uploaded to the internet or social media sites, or captured by video surveillance.[33]

No biometric data should ever be shared with political parties, political candidates or campaign organisations,~~ unless explicitly authorised by law~~.

Commented [A84]: What circumstances could justify to share biometric data, that has been collected for the purpose of voter identification, with third parties?

(...)

ITALY

1. Introduction

(…)

~~[29] Cf. Explanatory report, para. 87.~~
[30] Convention 10, Art 6. 2.
[31] Guidelines on facial recognition, p. 5.
[32] Guidelines on facial recognition, p. 7.
[33] Guidelines on facial recognition, p. 9.

This guidance addresses questions about the data ~~captured~~ collected, processed and official electoral management bodies (EMBs) and other authorities for the purpose of voter registration and authentication. The data controllers are therefore not political parties or other campaigning organisations, but the organisations (including EMBs) responsible for processing personal data on eligible voters for the purposes of voter registration, and voter authentication at the time and place that a ballot is cast in an election.

(…)

~~Supervisory~~ Relevant oversight authorities (could include~~ing~~ EMBs, data protection authorities (DPAs), and other oversight agencies) may wish to adapt these guidelines to their particular electoral systems. They may also wish to consider developing domestic codes of practice on voter registration and authentication, alone or in cooperation, sensitive to their domestic political systems, and consistent with ~~their~~ the responsibilities of DPAs under Article 15 of Convention 108+.

2. Scope and Purpose

These guidelines:

Apply the data protection principles of Convention 108+ to the processing of personal data for purposes of voter registration and authentication.

Apply mainly to Electoral Management Bodies (EMBs) and/or to other regulatory and/or supervisory authorities responsible for the protection of personal data as data controllers, thereby contributing ~~for the purposes of~~ to the protection ~~ng of~~ of the right to vote in a free and equitable manner.

Apply solely to the processing of personal data on voters (or potential voters). They do not apply to the processing of personal data on candidates, potential candidates, or employees and volunteers.

[Recognise that most countries are experimenting with new forms of remote voting methods. These methods require new, and sometimes, different forms of authentication from those used for in-person voting.

Recognise and support the broader global development on rights to a digital identity and complement the Guidelines on National Digital Identity adopted by the Consultative Committee of Convention 108.

Recognise that voter registers and voter lists may be assembled and maintained in a variety of ways and locations using both digital and non-digital media by a range of national and local authorities.

Recognise that the names and addresses of voters in the voters lists (based on the voter register) are legally shared in some jurisdictions with registered political parties and candidates for campaigning purposes, and that their use should be restricted by law to legitimate purposes of campaigning activities.

Recognise that different administrative and institutional factors shape the conduct of elections and the personal data processing practices in elections: the electoral system; the party system; the relationship between central and local party organisations; the existence of "primary elections"; the frequency of referendums; and others.

Commented [A85]: I still find this sentence ambiguous for a number of reasons:

- Putting together different authorities including DPAs may be misleading because they have different roles. DPAs oversees the compliance of the electoral procedure with data protection rules; EMBs, sometimes as controllers, have to respect DP rules.
- -Not sure it is a question for authorities to "wish to adapt these guidelines to their electoral system" as it is said here. Rather, the legal framework regulating the electoral system can impact on the processing of personal data, for example in terms of legal basis
- -Not sure what we mean in the very last words "and consistent with the responsibilities of DPAs under Article 15 of Convention 108+".

I would suggest to delete the sentence. We may want to keep the reference to codes of practice in a separated sentence not necessarily in this introductory part

Commented [A86]: I am not sure I can think about cases where DPAs would act as controllers in the electoral field. Again, I have the feeling we are mixing up the addressees of the 108+ principles (EMB and other regulatory bodies in the electoral field as controllers) with DPAs, which on the contrary are called upon to ensure the compliance of the processing carried out by those bodies with DP rules. Can't we simply say something as: "Apply to the processing of personal data carried out by Electoral Management Bodies (EMBs) and/or other competent regulatory authorities in the electoral field"

Recognise that many countries have introduced, or will introduce, biometric forms of identification to register and authenticate voters, and that safeguards are necessary (even where the introduction of biometrics is not being actively considered).]

Commented [A87]: Toute cette partie que je mets entre [ ] ne devrait-elle pas être déplacée dans un préambule (comme dans les recommandations).

3. Definitions for the purposes of the Guidelines

In addition to the definitions stipulated in Article 2 of Convention 108+, the guidelines use the following terms to ensure a uniformity of definition:

"~~Supervisory~~ Relevant oversight authorities" refer to those independent regulatory agencies that might have oversight responsibility for the processing of personal data for electoral purposes, and includes data protection authorities (DPAs) and election management bodies (EMBs)

Commented [A88]: same concerns as above: I am not sure we need to create a category/notion to include both electoral and data protection bodies. Moreover, it is a notion which, unless I am mistaken, is not used again in the text of the guidelines

(…)

Personal data revealing "political opinions" are a special category of data under Article 6 of the Convention and may include data on voting activity, including: whether the voter has voted; taking into account the underlying context and/or together with other personal data the place of voting; and the method of voting.

Commented [A89]: not sure the method of voting can reveal political opinions.

(…)

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

(…)

4.5. Rights of data subjects (Article 9)

(…)

Data subjects shall have the right not to be subject to decisions significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration. For example, where data subjects are deregistered from a voting register (for reasons of [age], mental capacity, criminal record), they have the right to be informed of the reasons for the decision.

Commented [A90]: This is not totally consequential as the first sentence of the paragraph speaks about the possibility to contest the decision whereas the second refers to the right to know the reasoning of the decision

(…)

SWITZERLAND

1. Introduction

(…)

The aim of these guidelines is to provide practical advice to EMBs and other supervisory authorities about how systems of voter registration and authentication should comply with Convention 108+ [34] especially when new biometric techniques are being introduced. They offer a framework through which individual regulators may provide more precise guidance tailored to the unique political, institutional, and cultural conditions of their own states.

Commented [A91]: CH: can EMBs really be compared with independent supervisory authorities? In some countries, such as in CH, they are part of the federal administration. Therefore, the word "other" is misleading.

Other recent guidelines on the application of Convention 108 may also relate to the processing of personal data for purposes of voter registration and authentication: on digital identity; on political campaigning; on artificial intelligence;[35] and on facial recognition.[36]

~~Supervisory~~ Relevant oversight authorities (could include~~ing~~ EMBs, data protection authorities (DPAs), and other oversight agencies) may wish to adapt these guidelines to their particular electoral systems. They may also wish to consider developing domestic codes of practice on voter registration and authentication, alone or in cooperation, sensitive to their domestic political systems, and consistent with ~~their~~ the responsibilities of DPAs under Article 15 of Convention 108+.

Commented [A92]: CH: see remark above.

2. Scope and Purpose

These guidelines:

Apply the data protection principles of Convention 108+ to the processing of personal data for purposes of voter registration and authentication.

Apply mainly to Electoral Management Bodies (EMBs) and/or to other regulatory and/or supervisory authorities responsible for the protection of personal data as data controllers, thereby contributing ~~for the purposes of~~to the protection ~~ng~~ of the right to vote in a free and equitable manner.

Commented [A93]: CH: «supervisory authorities *responsible* for the protection of personal data as data *controllers*» is probably not correct.

Apply solely to the processing of personal data on voters (or potential voters). They do not apply to the processing of personal data on candidates, potential candidates, or employees and volunteers.

Recognise that most countries are experimenting with new forms of remote voting methods. These methods require new, and sometimes, different forms of authentication from those used for in-person voting.

Commented [A94]: CH: quite an abstract formulation. It would be useful to explain better what is meant with it (E-voting, postal voting? Eventually, a reference to CM/Rec(2017)5 could be added?

[34] Council of Europe (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, at: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

[35] Council of Europe (2019). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on artificial intelligence* and data protection. Strasbourg: Council of Europe (adopted 25 January 2019)

[36] Council of Europe (2021). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on Facial Recognition.* Strasbourg: Council of Europe (adopted 2021)

Recognise and support the broader global development on rights to a digital identity and complement the Guidelines on National Digital Identity adopted by the Consultative Committee of Convention 108.

Recognise that voter registers and voter lists may be assembled and maintained in a variety of ways and locations using both digital and non-digital media by a range of national and local authorities.

Recognise that the names and addresses of voters in the voters lists (based on the voter register) are legally shared in some jurisdictions with registered political parties and candidates for campaigning purposes, and that their use should be restricted by law to legitimate purposes of campaigning activities.

Commented [A95]: CH: Eventually, the necessity of deleting the data after use for a specific election should be pointed out here. In general, the deletion of data is not addressed enough in these guidelines.

Recognise that different administrative and institutional factors shape the conduct of elections and the personal data processing practices in elections: the electoral system; the party system; the relationship between central and local party organisations; the existence of “primary elections”; the frequency of referendums; and others.

Recognise that many countries have introduced, or will introduce, biometric forms of identification to register and authenticate voters, and that safeguards are necessary (even where the introduction of biometrics is not being actively considered).

3. Definitions for the purposes of the Guidelines

In addition to the definitions stipulated in Article 2 of Convention 108+, the guidelines use the following terms to ensure a uniformity of definition:

“~~Supervisory~~ Relevant oversight authorities” refer to those independent regulatory agencies that might have oversight responsibility for the processing of personal data for electoral purposes, and includes data protection authorities (DPAs) and election management bodies (EMBs)

Commented [A96]: CH: As we understand it, oversight seems to be less intrusive that supervision.

These guidelines often refer to supervisory authorities (cf. p. 3, 8, 11 and 12) as the Convention 108+ only mentions supervisory authorities in its articles (art. 15, 16, 17, etc.).
So what is the definition of supervisory authorities ? How does it differ from "oversight authorities"? According to us, this should be defined.

Commented [A97]: CH: Since EMBs are included here, "independent" probably does not fit in many countries (e.g. in Switzerland) or would have to be explained (see also definition of EMB).

Commented [A98]: CH : should be replaced by « electoral management bodies » in order to be coherent with the definition.

“Electoral Management Bodies” (EMBs) refers to those national authorities responsible for the regulation of the safe and efficient conduct of elections, the implementation of election finance provisions and (where applicable) the development and management of the national voter register as a data controller.

Voter registration refers to the process for collecting, assembling, and maintaining relevant information on individuals included in the voter register.

Commented [A99]: CH: The definition should already state that "voter registration" only concerns the data processing of EMBs.

Voter registers are the consolidated, official lists of all persons eligible to vote and the underlying personal data processed for this purpose ~~[.]~~

Voter lists refer to the list of all persons registered to vote in a particular electoral district or constituency for a particular election.

Depending on the jurisdiction, different data controllers might be responsible for the management and processing of voter registers and voter lists including: national and regional EMBs; local government authorities responsible for population registration and the conduct of elections; and statistical agencies.

Commented [A100]: CH : This is not really a definition.

Electoral district refers to the defined region in which a voter is registered to vote.

~~Voter authentication refers to the process for verifying the eligibility of individuals to vote in a particular electoral district in a particular election.~~ Authentication is the ability to prove that an individual is genuinely who that person claims to be. Voter authentication is the process of verifying that proof as well as verifying that the person is eligible to vote in a particular district in a particular election. Authentication may, or may not, require the positive and unique identification of the individual in question.

Commented [A101]: CH: The definition is probably flawed: The definition makes it seem that merely looking up an individual in the voter register would be considered to be "voter authentication". This shouldn't be the case.
In addition, it should, as mentioned above, already be stated in the definition that "voter authentication" only concerns the data processing of EMBs.

A "political party" is 'a free association of persons, one of the aims of which is to participate in the management of public affairs, including through the presentation of candidates to free and democratic elections.[37]

Personal data revealing "political opinions" are a special category of data under Article 6 of the Convention and may include data on voting activity, including: whether the voter has voted; taking into account the underlying context and/or together with other personal data the place of voting; and the method of voting.

Biometrics refers to data resulting ~~to~~ from the automated recognition that is a specific technical processing of data concerning ~~of~~ individuals based on their distinguishing and repeatable biological (physiological), biological and/or behavioural characteristics which allows the unique identification or authentication of the individual, when it is precisely used to uniquely identify the data subject.

Commented [A102]: CH: the formulation is not really clear. Are Biometrics the data resulting from the identification / authentication process ("resulting from"), or do biometrics also include the data that forms the basis for identification / authentication? (Presumably the second reading would make sense).

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

(…)

The legitimate purpose of voter registration and authentication is to enable the right to vote for all legitimate voters in a given electoral district. These purposes and means should be stated as precisely and fully as possible in publicly available documents, according to the transparency principle (Article 8). Further processing should be compatible with this stated purpose, under Article 5(4)b.

Commented [A103]: CH: It seems questionable whether data that is used for "voter authentication" should be available for other purposes at all (especially biometric data). These guidelines would be a good place to prohibit this.

(…)

The following paragraphs are to be interpreted in line with the generally recognised principle of the secrecy of elections and are without prejudice to domestic rules on access to public information. Where political campaign organisations and their candidates legally acquire the official voters list from the EMB to assist their campaigns, the law should stipulate who is entitled to access these data, for what purposes, and for how long. The sharing of voters' lists should be limited to what is necessary for engaging with the electorate with clear prohibitions and appropriate sanctions for using the data for any other purposes than the assistance with their electoral campaign.

Commented [A104]: CH: it makes sense to repeat the purpose.

Personal data contained in official voters list are not to be further processed or shared with third parties without express authorisation in law/appropriate legal basis. Unless specifically approved by law and subject to the principle of proportionality, name and addresses from the official voters list should not be combined with other sources of personal data processed by political parties or other campaign organisations to create profiles of voters for micro-targeting purposes.

Commented [A105]: CH: and in voter registers?

Commented [A106]: SECRETARIAT : This change was made by the Secretariat.

Commented [A107]: CH: The addition seems useful to emphasize that even a legal basis cannot legitimize any further processing or disclosure of data in electoral lists (because proportionality must also be observed).

[37] Guidelines CDL-AD (2010))24 On Political Party Regulation by OSCE/ODIHR and Venice Commission.

The statistical processing of personal data on voting trends by demographic or geographic variables would normally be considered a "compatible purpose" provided other safeguards exist to ensure the anonymisation or pseudonymisation of the data [38] Such processing should respect the secrecy of the ballot, and should not lead to a disproportionate interference with the voters' interests, rights, and freedoms.

No ~~undue~~ influence or pressure should be exerted on a voter or potential voter to provide personal data for the purpose of voter registration.[39]

(…)

4.2. Processing of special categories of data (including biometric data) that uniquely identifies an individual for voter registration and authentication (Article 6)

In the context of voter registration, the recording of information on whether or not the individual voted in a particular election is information that may reveal political opinions. The recording over time of voting histories is also information that may reveal political opinions. These are all personal data falling within the special categories of data under Convention 108+. The processing of those information might also fall under the domestic legislation on access to official documents.

In some countries, various individuals might be legitimately prohibited from voting on the grounds of criminal record, mental capacity, [] . These data are special categories data which can lead to unlawful discrimination and are therefore subject to the highest safeguards.

The processing of personal data revealing political opinions entails severe risks of voter discrimination and can lead to voter suppression and intimidation. The knowledge of who has, and has not, voted can (in some societies) also affect the provision of government services. The processing of special categories of personal data needs to be accompanied by safeguards appropriate to the risks at stake of voter discrimination and of the interests, rights and freedoms protected and has to take into account the domestic legislation on access to official documents as well.

The analysis, sorting and profiling of groups of voters on geographical and/or demographic factors, can have discriminatory effects[40] when predictions about groups of voters based on shared characteristics, and based on large data sets, are used to target or otherwise single-out specific voters.

EMBs should not disclose personal data to third parties unless permitted by domestic law that provide for appropriate safeguards for the protection of personal data and private life of individuals. EMBs should not disclose data from voter registration to third parties (such as data brokers) to monetise, or otherwise reprocess for the purposes of selling anonymised or de-identified data.

[EMBs should not use data in the voter register for purposes of promoting democratic participation and encouraging voter turnout ~~without the express consent of the voter, or~~ unless permitted by law. If consent can be an appropriate legal basis for such processing the consent shall be free, informed, and unambiguous]

Commented [A108]: CH: Unclear use of the word "other" here. If it is only about the following safeguards of anonymization or pseudonymization, then the word is not needed.

Commented [A109]: CH: This should probably not be deleted. The right to vote is at least partly a civic duty.

Commented [A110]: CH: According to the title, this point should deal in particular with data that uniquely identifies an individual. However, the point below deals primarily with sensitive data on voting behavior and practically no uniquely identifying data, which is somewhat strange given the guidelines' focus on voter registration and authentication. More content is needed on uniquely identifying data in this point and, if necessary, a structural subdivision so that the existing points on sensitive data on voting behavior are treated separately. Accordingly, it makes sense to integrate point 4.7 here.

Commented [A111]: CH: Is this really in the context of voter registration?

Commented [A112]: CH: Publicity laws often contain an obligation to anonymize and/or weigh up the interests of the data subjects when disclosing personal data. At best, it would have to be added here that information on voting behavior may only be disclosed in anonymized form and that the interests of the data subjects in non-disclosure normally prevail.

Commented [A113]: CH: It is not clear what is meant by "subject to the highest standards". Article 6 C108+ requires for special categories of data that additional appropriate safeguards to those in the Convention are laid down in law and that these safeguards must in particular protect against discrimination. It could make sense to require that TOMs be taken to specifically protect this data.

Commented [A114]: CH: It is not clear to what extent this addition makes sense. The sentence states that measures for protection must be taken when special categories of data are processed (cf. Art. 6(1) C108+). The processing itself does not have to take into account the publicity legislation. The publicity legislation may apply retrospectively, but this does not affect the measures taken prior to processing. A clarifying reformulation would be necessary here.

Commented [A115]: CH: How is this compatible with the public nature of the voting registers enshrined in Swiss law?

[38] Explanatory report, para 50.

[39] Explanatory report, para. 42.

[40] Council of Europe, The Protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/REC (2010) 13 (November 23, 2010)

4.3. Data security and confidentiality (Article 7)

Applying appropriate security measures to voter registration data, and its processing environments both in use at rest and in transit, is vital to ensure voters' data are protected to the highest standards. Security measures should take into account the current state of the art data-security methods and techniques in the field of data processing. [Their [cost] should be commensurate with the seriousness and probability of the potential risks.][41]

Commented [A116]: CH: Suggestion to add: «in use».

The authentication of voters during an election often involves the sharing of data on voters with large numbers of volunteers, contractors and employees during the intense period of elections. EMBs should take appropriate security measures to ensure against accidental or unauthorised access to, destruction, loss, use, modification, or disclosure of personal data. With regard to information security CIA triad shall apply, i.e. EMBs shall safeguard confidentiality, integrity and availability

Commented [A117]: CH: Suggestion to add this sentence.

Security measures should include: training in privacy and security; access controls; confidentiality agreements; ~~and~~ controls on physical access to places, safeguard secure transfer of data, possibility of checking the resilience of security measures under a false name and equipment where personal data in the voter register or the voter lists are stored. Where EMB process data electronically, all actions relevant with regard to data security have to be logged, whereas the logs need to be protected in integrity and security.

Commented [A118]: CH: The practical benefit of these guidelines is enhanced by the quality of the explanations of the security measures. Currently, the security measures are only dealt with briefly and not as a focal point. This could be changed by describing the individual measures in more detail and including additional measures.

Commented [A119]: CH: Consolidation of required – technical and organizational – security measures of the different paragraphs in this chapter.

Commented [A120]: CH: suggestion to add this part.

Commented [A121]: CH: suggestion to add this part.

EMBs should report to supervisory authorities as prescribed by Convention 108+ and to the data subjects themselves in the event of data breaches which may seriously interfere with the rights and fundamental freedoms of voters in accordance with Article 7(2) of the Convention 108+. Notification should include adequate and meaningful information about possible measures to mitigate the adverse effects of the breach.[42]

Commented [A122]: CH: according to art. 7(2) C108+ it should be «notify» resp. «notification».

Commented [A123]: CH: Art. 7(2) C108+ does not provide for notification of data subjects in the event of a data protection incident. The wording "at least" implies that the legislation can/should also provide for notification of the data subjects. Accordingly, it is not correct to use "as prescribed" here. If the guidelines require notification of the data subjects, then it should be pointed out that the legislation should stipulate this accordingly.

Where voter registration data is processed by third party service providers, EMBs should remain aware of their ongoing responsibilities as data controllers. Controllers should be able to demonstrate, that processors comply with their obligations in accordance with Articles 7(1) and where applicable 10 of the Convention 108+.

Commented [A124]: SECRETARIAT : This changes was made by the Secretariat.

Risk assessment prior to processing should assess whether data is protected against unauthorised access, modification and removal/destruction. Risk assessment should seek to embed high standards of security throughout the processing. Such an assessment should be informed by considerations of necessity and proportionality, and the fundamental data protection principles across the range of risks including physical accessibility, networked access to devices and data, and the backup and archiving of data.

EMBs should train all workers and volunteers in the importance of privacy and data security measures with regard to the voter register and the voters lists. Each employee or volunteer should have to be under confidentiality obligations. The voter register and voter lists should be protected by strong access controls for different categories of employees and volunteers.

Commented [A125]: CH: see above.

(…)

4.5. Rights of data subjects (Article 9)

Data subjects should be able to obtain on request and without excessive delay or expense, confirmation of the processing of personal data relating to him or her in a voter register, and to access to those data in an intelligible form.

Commented [A126]: CH: and in a voter list?

[41] Explanatory report, para 63.

[42] Explanatory report, para 66.

Data subjects have to be given the possibility to request rectification or erasure, if applicable and/or concerning the inaccurate data, as the case may be, if the data is inaccurate, obsolete or incomplete.[43]

Data subjects shall have the right not to be subject to decisions significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration. For example, where data subjects are deregistered from a voting register (for reasons of [age], mental capacity, criminal record), they have the right to be informed of the reasons for the decision.

Data subjects should be able to object to the processing of data on him or her with an EMB or the competent authority at any time to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms.

Commented [A127]: CH: This seems to be an important clarification. Otherwise, the proper conduct of ballots would be jeopardized.

[43] Explanatory report, para. 72.

~~and to request rectification or erasure, as the case may be, if the data is inaccurate, obsolete or incomplete.[44]~~

~~Data subjects should be able to obtain on request and without excessive delay or expense, confirmation of the processing of personal data relating to him or her in a voter register, and to access to those data in an intelligible form.~~

Data subjects are entitled to be informed how their personal data was obtained for the voter register, and from what source.

(…)

4.6. Additional obligations and recommendations for Election Management Bodies and other authorities (Article 10)

The obligation rests with the data controller to ensure adequate data protection and to be able to demonstrate that data processing follows applicable laws. The accountability of data controllers and data processors should be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10(1) of Convention 108+.

(…)

While the implementation of these guidelines will be shaped by local political contexts, it may also require collaboration between supervisory authorities. [~~The global industry that supports biometric registration knows no geographic boundaries.~~] The impact of this industry nationally and internationally will require the most vigilant and constant cross-national attention from EMBs and supervisory authorities through their international and regional associations.

4.7. Additional Obligations for processing of biometric data for voter registration and authentication

(…)

The integration of biometric forms of identification into existing voter registration databases poses serious risks to the privacy of individuals, when the application of these technologies does not always require the awareness or cooperation of individuals.[45]

Biometric forms of identification for voter registration and authentication purposes should be assessed in light of the proportionality and necessity of the processing, and should only be introduced if existing (legacy) forms of identification and authentication have been demonstrably shown to be inadequate, inaccurate and/or contrary to the rights of the individual.

(…)

The application of biometric forms of identification (and especially facial recognition) should only be for purposes of voter registration and authentication and should not be processed to infer race, ethnic origin, age, health or other social conditions.

Where facial recognition is used, no digital images should be used that were uploaded to the internet or social media sites, or captured by video surveillance.[46]

No biometric data should ever be shared with political parties, political candidates or campaign organisations, unless explicitly authorised by law.

Developers and manufacturers of biometric technologies shall take steps to ensure that the biometric data are accurate under Article 5. This involves continual testing their systems to

Commented [A128]: CH: and for the voter list?

Commented [A129]: CH: If possible, do not use qualifying words about the type of data protection. Data controllers must ensure compliance with data protection principles. It is not clear enough what is meant by adequate data protection. Art. 10 C108+ also does not refer to adequate data protection.

Commented [A130]: CH: Which one ? Does it refer to the "industry that supports biometric registration"? With the deletion of the previous sentence, this sentence needs to be clarified to be understood.

Commented [A131]: CH: If the previous sentence is deleted, it is not clear what this refers to.

Commented [A132]: CH: The content of this point belongs to section 4.2 (see comment above).

Commented [A133]: CH: This restriction is probably not necessary - The risk exists regardless of the awareness of the individual.

Commented [A134]: CH: Not clear what is meant. To what extent does a lack of cooperation on the part of the data subject constitute an increased risk to privacy when using biometrics? A lack of knowledge about the use of biometrics is certainly not good, but the increased risk of using biometrics does not result from a lack of knowledge or cooperation, but from the type of data, the type of processing, the potential for discrimination, the possibility of further use of this data, etc.

Commented [A135]: CH: Isn't this too weak? Even if non-biometric processes have failed in the past, then other non-biometric processes should be explored.

"…if non-biometric forms of identification or authentication have been explored and shown to be inadequate,…"

Commented [A136]: CH: Could it be included somewhere that the principle of data minimization should be implemented and, if possible, biometric data should be deleted/destroyed after matching or identification?

Commented [A137]: CH: Are there cases where the law would authorise sharing biometric data in this context?

eliminate disparities, particularly according to ethnicity, age and gender. They should integrate data protection by design principles into the manufacture of biometric products and services. They should also examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of the data processing and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms. The moreover should implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

(…)

Commented [A138]: CH: “They”.

~~[44] Explanatory report, para. 72.~~
[45] Guidelines on facial recognition, p. 5.
[46] Guidelines on facial recognition, p. 9.

TÜRKIYE

1. Introduction

(…)

Biometric data is just one category of ~~sensitive~~ special categories of data given special protection by international instruments such as the Council of Europe's Convention for the protection of individuals with regard to the automatic processing of personal data (ETS No. 108) as amended by Protocol CETS No. 223[47] ("Convention 108+", "Convention") whose processing can lead to a variety of individual and social risks to privacy, and to other human rights. (…)

(…)

This guidance addresses questions about the data ~~captured~~ collected and managed by official electoral management bodies (EMBs) and other authorities for the purpose of voter registration and authentication. (…)

(…)

~~Supervisory~~ Relevant oversight authorities (could include~~ing~~ EMBs, data protection authorities (DPAs), and other oversight agencies) may wish to adapt these guidelines to their particular electoral systems. They may also wish to consider developing domestic codes of practice on voter registration and authentication, alone or in cooperation, sensitive to their domestic political systems, and consistent with ~~their~~ the responsibilities of DPAs under Article 15 of Convention 108+.

2. Scope and Purpose

(…)

Apply mainly to Electoral Management Bodies (EMBs) and/or to other regulatory and/or supervisory authorities responsible for the protection of personal data as data controllers, thereby contributing ~~for the purposes of~~to the protection ~~ng~~ of the right to vote in a free and equitable manner.

(…)

3. Definitions for the purposes of the Guidelines

In addition to the definitions stipulated in Article 2 of Convention 108+, the guidelines use the following terms to ensure a uniformity of definition:

"~~Supervisory~~ Relevant oversight authorities" refer to those independent regulatory agencies that might have oversight responsibility for the processing of personal data for electoral purposes, and includes data protection authorities (DPAs) and election management bodies (EMBs)

"Electoral Management Bodies" (EMBs) refers to those national authorities responsible for the regulation of the safe and efficient conduct of elections, the implementation of election finance provisions and (where applicable) the development and management of the national voter register as a data controller.

[47] Council of Europe (2018), *Convention for the protection of individuals with regard to the processing of personal data* (2018) at: https://rm.coe.int/convention-108-for-the-protection-of-individuals (hereafter Convention 108+).

Voter registration refers to the process for collecting, assembling, and maintaining relevant information on individuals included in the voter register.

Voter registers are the consolidated, official lists of all persons eligible to vote and the underlying personal data processed for this purpose ~~[.]~~

(…)

Personal data revealing “political opinions” are a special category of data under Article 6 of the Convention and may include data on voting activity, including: whether the voter has voted; taking into account the underlying context and/or together with other personal data the place of voting; and the method of voting.

Biometrics refers to data resulting ~~to~~ from the automated recognition that is a specific technical processing of data concerning ~~of~~ individuals based on their distinguishing and repeatable biological (physiological), biological and/or behavioural characteristics which allows the unique identification or authentication of the individual, when it is precisely used to uniquely identify the data subject.

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

~~All personal data on voters processed for the purposes of voter registration and authentication should be considered a special category of data and should be processed lawfully and in accordance with the principles set out in Article 5 of Convention 108+~~Personal data on voters should be processed lawfully and in accordance with the principles set out in Article 5 of Convention 108+: proportionality, lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, and security. Processing should be proportionate in relation to the legitimate purposes of the data processing, reflecting the rights and freedoms at stake.

(…)

A “legitimate basis laid down by law” (Article 5(2)), for the collection of personal data, should ~~normally~~ be included in an applicable electoral legislation. Where the public interest in democratic engagement is the legitimate basis for processing, those interests should be clearly stated by law and duly referenced in the privacy policy of EMBs.

(….)

The following paragraphs are to be interpreted in line with the generally recognised principle of the secrecy of elections and are without prejudice to domestic rules on access to public information. Where political campaign organisations and their candidates legally acquire the official voters list from the EMB to assist their campaigns, the law should stipulate who is entitled to access these data, for what purposes, and for how long. The sharing of voters’ lists should be limited to what is necessary for engaging with the electorate with clear prohibitions and appropriate sanctions for using the data for any other purposes.

Personal data contained in official voters list are not to be further processed or shared with third parties without express authorisation in law/appropriate legal basis. Unless specifically approved by law, name and addresses from the official voters list should not be combined with other sources of personal data processed by political parties or other campaign organisations to create profiles of voters for micro-targeting purposes.

(….)

No ~~undue~~ influence or pressure should be exerted on a voter or potential voter to provide personal data for the purpose of voter registration.[48]

(….)

The EMB should not be transferring those data to other organisations for processing even in aggregate form outside of the controller-processor relationship without having a legal basis or obtaining the express consent of the voter.

4.2 Processing of special categories of data (including biometric data) that uniquely identifies an individual for voter registration and authentication (Article 6)

(….)

In the context of voter registration, the recording of information on whether or not the individual voted in a particular election is information that may reveal political opinions. The recording over time of voting histories is also information that may reveal political opinions. These are all personal data falling within the special categories of data under Convention 108+. The processing of those information might also fall under the domestic legislation on access to official documents.

(….)

The processing of personal data revealing political opinions entails severe risks of voter discrimination and can lead to voter suppression and intimidation. The knowledge of who has, and has not, voted can (in some societies) also affect the provision of government services. The processing of special categories of personal data needs to be accompanied by safeguards appropriate to the risks at stake of voter discrimination and of the interests, rights and freedoms protected and has to take into account the domestic legislation on access to official documents as well.

(…)

EMBs should not disclose personal data to third parties unless permitted by domestic law that provide for appropriate safeguards for the protection of personal data and private life of individuals. EMBs should not disclose data from voter registration to third parties (such as data brokers) to monetise, or otherwise reprocess for the purposes of selling anonymised or de-identified data.

[EMBs should not use data in the voter register for purposes of promoting democratic participation and encouraging voter turnout ~~without the express consent of the voter, or~~ unless permitted by law. If consent can be an appropriate legal basis for such processing the consent shall be free, informed, and unambiguous]

4.3. Data security and confidentiality (Article 7)

(…)

Security measures should include: training in privacy and security; access controls; confidentiality agreements; ~~and~~ controls on physical access to places, possibility of checking the resilience of security measures under a false name and equipment where personal data in the voter register or the voter lists are stored.

[48] Explanatory report, para. 42.

EMBs should report to supervisory authorities as prescribed by Convention 108+ and to the data subjects themselves in the event of data breaches which may seriously interfere with the rights and fundamental freedoms of voters in accordance with Article 7(2) of the Convention 108+. Notification should include adequate and meaningful information about possible measures to mitigate the adverse effects of the breach.[49]

Where voter registration data is processed by third party service providers, EMBs should remain aware of their ongoing responsibilities as data controllers. Controllers should be able to demonstrate, that processors comply with their obligations in accordance with Articles 7(1) and where applicable 10 of the Convention 108+.

4.4 Transparency of processing of personal data for voter registration and authentication (Article 8)

(…)

Depending on the source of the voter register, EMBs should inform voters (in a privacy policy or its equivalent) of at least: the legal name and address of the organisation; the legal basis ~~for collection of personal data~~ for the processing of personal data; the categories of personal data processed; any recipients of those data (including third-party processors), and the reasons why they need to be shared; and how the voter might exercise his/her rights.

4.5 Rights of data subjects (Article 9)

Data subjects should be able to obtain on request and without excessive delay or expense, confirmation of the processing of personal data relating to him or her in a voter register, and to access to those data in an intelligible form.

Data subjects have to be given the possibility ~~-~~to request rectification or erasure, if applicable and/or concerning the inaccurate data, as the case may be, if the data is inaccurate, obsolete or incomplete.[50]

(…)

Data subjects should be able to object to the processing of data on him or her with an EMB or the competent authority at any time to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms.

[49] Explanatory report, para 66.

[50] Explanatory report, para. 72.

~~and to request rectification or erasure, as the case may be, if the data is inaccurate, obsolete or incomplete.[51]~~

~~Data subjects should be able to obtain on request and without excessive delay or expense, confirmation of the processing of personal data relating to him or her in a voter register, and to access to those data in an intelligible form.~~

Data subjects are entitled to be informed how their personal data was obtained for the voter register, and from what source. Data subjects are entitled to learn the purpose of processing their personal data regarding the voter register and whether they are used in accordance with their purpose, and the right to object to the emergence of a result against them by analyzing the processed data exclusively through automated systems.

4.6. Additional obligations and recommendations for Election Management Bodies and other authorities (Article 10)

(…)

While the implementation of these guidelines will be shaped by local political contexts, it may also require collaboration between supervisory authorities. [~~The global industry that supports biometric registration knows no geographic boundaries.~~] The impact of this industry nationally and internationally will require the most vigilant and constant cross-national attention from EMBs and supervisory authorities through their international and regional associations.

4.7 Additional Obligations for processing of biometric data for voter registration and authentication

Biometric data, using technical means to uniquely identify an individual, is classified as a special category of data under Article 6 of Convention 108+.

The context of processing of biometric forms of identification for purposes of voter registration and authentication also establishes heightened levels of sensitivity given that personal data revealing political opinions is also defined as a special category.

The processing of special categories of data shall only be allowed where appropriate safeguards are enshrined in law complementing those in Convention 108+, guarding against the risks that the processing of sensitive data poses for the interests, rights and fundamental freedoms for the data subject, and notably the risk of discrimination.[52]

(…)

No biometric data should ever be shared with political parties, political candidates or campaign organisations, and third parties unless explicitly authorised by law.

Developers and manufacturers of biometric technologies shall take steps to ensure that the biometric data are accurate under Article 5. This involves continual testing their systems to eliminate disparities, particularly according to ethnicity, age and gender. They should integrate data protection by design principles into the manufacture of biometric products and services. They should also examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of the data processing and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms. The moreover should implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

URUGUAY

1. Introduction

(…)

This guidance addresses questions about the data ~~captured~~ collected, processed and managed by official electoral management bodies (EMBs) and other authorities for the purpose of voter registration and authentication. The data controllers are therefore not political parties or other campaigning organisations, but the organisations (including EMBs) responsible for processing personal data on eligible voters for the purposes of voter registration, and voter authentication at the time and place that a ballot is cast in an election.

Commented [A139]: Suggestion to suppress the word managed; "collected and further processed" as an option

Commented [A140]: Suggestion to start the phrase by "Therefore, for the purpose of these guidelines…"

The aim of these guidelines is to provide practical advice to EMBs and other supervisory authorities about how systems of voter registration and authentication should comply with Convention 108+ [53] especially when new biometric techniques are being introduced. They offer a framework through which individual regulators may provide more precise guidance tailored to the unique political, institutional, and cultural conditions of their own states.

Commented [A141]: I share Alessandra´s concern on the scope of the term "authority" throughout the document. In the first paragraph of this page we have already defined what is "controller" as EMB and other organizations that collect and process data for purposes of voter registration and authentication when a ballot is cast. I propose to keep the reference to "controllers" without any distinctions and define Supervisory authorities as DPAs in the terms of article 15. I would also suppress the references to "authorities" and "relevant oversight authorities".

Other recent guidelines on the application of Convention 108 may also relate to the processing of personal data for purposes of voter registration and authentication: on digital identity; on political campaigning; on artificial intelligence;[54] and on facial recognition.[55]

Commented [A142]: 108+

~~Supervisory~~ Relevant oversight authorities (could include~~ing~~ EMBs, data protection authorities (DPAs), and other oversight agencies) may wish to adapt these guidelines to their particular electoral systems. They may also wish to consider developing domestic codes of practice on voter registration and authentication, alone or in cooperation, sensitive to their domestic political systems, and consistent with ~~their~~ the responsibilities of DPAs under Article 15 of Convention 108+.

Commented [A143]: I still find this sentence ambiguous for a number of reasons:

- Putting together different authorities including DPAs may be misleading because they have different roles. DPAs oversees the compliance of the electoral procedure with data protection rules; EMBs, sometimes as controllers, have to respect DP rules.
-Not sure it is a question for authorities to "wish to adapt these guidelines to their electoral system" as it is said here. Rather, the legal framework regulating the electoral system can impact on the processing of personal data, for example in terms of legal basis
-Not sure what we mean in the very last words "and consistent with the responsibilities of DPAs under Article 15 of Convention 108+".

I would suggest to delete the sentence. We may want to keep the reference to codes of practice in a separated sentence not necessarily in this introductory part

(…)

2. Scope and Purpose

These guidelines:

[53] Council of Europe (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, at: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

[54] Council of Europe (2019). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on artificial intelligence* and data protection. Strasbourg: Council of Europe (adopted 25 January 2019)

[55] Council of Europe (2021). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on Facial Recognition.* Strasbourg: Council of Europe (adopted 2021)

Apply the data protection principles of Convention 108+ to the processing of personal data for purposes of voter registration and authentication.

Apply mainly to Electoral Management Bodies (EMBs) and/or to other regulatory and/or supervisory authorities responsible for the protection of personal data as data controllers, thereby contributing ~~for the purposes of~~to the protection~~ng~~ of the right to vote in a free and equitable manner.

Commented [A144]: I am not sure I can think about cases where DPAs would act as controllers in the electoral field. Again, I have the feeling we are mixing up the addressees of the 108+ principles (EMB and other regulatory bodies in the electoral field as controllers) with DPAs, which on the contrary are called upon to ensure the compliance of the processing carried out by those bodies with DP rules. Can't we simply say something as: "Apply to the processing of personal data carried out by Electoral Management Bodies (EMBs) and/or other competent regulatory authorities in the electoral field"

Commented [A145R144]: I agree with Alessandra, with the addition of "(controllers for the purpose of these guidelines)" or something of the sorts.

(…)

[Recognise that most countries are experimenting with new forms of remote voting methods. These methods require new, and sometimes, different forms of authentication from those used for in-person voting.

Recognise and support the broader global development on rights to a digital identity and complement the Guidelines on National Digital Identity adopted by the Consultative Committee of Convention 108.

Recognise that voter registers and voter lists may be assembled and maintained in a variety of ways and locations using both digital and non-digital media by a range of national and local authorities.

Recognise that the names and addresses of voters in the voters lists (based on the voter register) are legally shared in some jurisdictions with registered political parties and candidates for campaigning purposes, and that their use should be restricted by law to legitimate purposes of campaigning activities.

Recognise that different administrative and institutional factors shape the conduct of elections and the personal data processing practices in elections: the electoral system; the party system; the relationship between central and local party organisations; the existence of "primary elections"; the frequency of referendums; and others.

Recognise that many countries have introduced, or will introduce, biometric forms of identification to register and authenticate voters, and that safeguards are necessary (even where the introduction of biometrics is not being actively considered).]

Commented [A146]: Toute cette partie que je mets entre [ ] ne devrait-elle pas être déplacée dans un préambule (comme dans les recommandations).

3. Definitions for the purposes of the Guidelines

In addition to the definitions stipulated in Article 2 of Convention 108+, the guidelines use the following terms to ensure a uniformity of definition:

"~~Supervisory~~ Relevant oversight authorities" refer to those independent regulatory agencies that might have oversight responsibility for the processing of personal data for electoral purposes, and includes data protection authorities (DPAs) and election management bodies (EMBs)

Commented [A147]: same concerns as above: I am not sure we need to create a category/notion to include both electoral and data protection bodies. Moreover, it is a notion which, unless I am mistaken, is not used again in the text of the guidelines

(…)

"Voter authentication" refers to the process for verifying the eligibility of individuals to vote in a particular electoral district in a particular election. Authentication is the ability to prove that an individual is genuinely who that person claims to be. Authentication may, or may not, require the positive and unique identification of the individual in question.

Commented [A148]: Perhaps we can follow the definition included in the NDIS guidelines that defines Authentication as "the process of verifying the identity of an individual and that they are who they claim to be", and in the last sentence I believe that it would be better to state that "Authentication may, or may not, require the use of biometrics to positively and uniquely identify the individual in question".

A “political party” is ‘a free association of persons, one of the aims of which is to participate in the management of public affairs, including through the presentation of candidates to free and democratic elections.[56]

“Personal data revealing ~~“~~political opinions” are a special category of data under Article 6 of the Convention and may include data on voting activity, including: whether the voter has voted; taking into account the underlying context and/or together with other personal data the place of voting; and the method of voting.

Commented [A149]: not sure the method of voting can reveal political opinions.

“Biometrics” refers to data resulting ~~to~~ from the automated recognition that is a specific technical processing of data concerning ~~of~~ individuals based on their distinguishing and repeatable biological (physiological), biological and/or behavioural characteristics which allows the unique identification or authentication of the individual, when it is precisely used to uniquely identify the data subject.

Commented [A150]: Same as above, though both are inspired in the ER, perhaps we should adopt one definition and keep it in all further guidelines.

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

(…)

A “legitimate basis laid down by law” (Article 5(2)), for the collection of personal data, should ~~normally~~ be included in an applicable electoral legislation. Where the public interest in democratic engagement is the legitimate basis for processing, those interests should be clearly stated by law and duly referenced in the privacy policy of EMBs.

Commented [A151]: “controllers”?

(…)

Personal data contained in official voters list are not to be further processed or shared with third parties without express authorisation in law/appropriate legal basis. Unless specifically approved by law, name and addresses from the official voters list should not be combined with other sources of personal data processed by political parties or other campaign organisations to create profiles of voters for micro-targeting purposes.

Commented [A152]: I agree with these paragraphs, but are outside of the scope of the guidelines, that aim at embs and other authorites for the purposes of voter registration or authentication at the time of the election.

(…)

No ~~undue~~ influence or pressure should be exerted on a voter or potential voter to provide personal data for the purpose of voter registration.[57]

Commented [A153]: In cases where voting is mandatory, personal data for voting registration must be provided or there might be sanctions, could this be interpreted as “pressure”?. In that case perhaps we should keep the term “undue”.

EMBs might be required to collect and report information on donors to the campaign under relevant election financing laws. Personal data collected under this legal authority should only be used for purposes stipulated in applicable election or party financing legislation, and consistent with applicable data protection law.

Commented [A154]: Is this within the scope of this document?

Where EMBs obtain personal data from other authorities (such as tax authorities, or population registries) those data should only continue to be used based on a legitimate base, for the defined and specified purpose and should only be retained for as long as necessary to register the voter.

[56] Guidelines CDL-AD (2010))24 On Political Party Regulation by OSCE/ODIHR and Venice Commission.

[57] Explanatory report, para. 42.

In states where those under the age of 18 may legally vote, EMBs should take special care to protect the personal data of young people according to Article 15(e) Convention 108+.[58]

Commented [A155]: "or be allowed to register before that age"

(…)

4.6, Additional obligations and recommendations for Election Management Bodies and other authorities (Article 10)

Commented [A156]: See how we will solve the references to authorities throughout the document

(…)

EMBs and the processors should provide a full record of how personal data has been obtained and is being processed, as well as demonstrate compliance of any third-party organisation that processes personal data on their behalf.

Commented [A157]: The scope of the chapter is broader

(…)

[58] Explanatory report, para. 125.

DATA PROTECTION COMMISSIONER

1. Introduction

(…)

This guidance addresses questions about the data ~~captured~~ collected, processed and managed by official electoral management bodies (EMBs) and other authorities for the purpose of voter registration and authentication. The data controllers are therefore not political parties or other campaigning organisations, but the organisations (including EMBs) responsible for processing personal data on eligible voters for the purposes of voter registration, and voter authentication at the time and place that a ballot is cast in an election.

(…)

2. Scope and Purpose

(…)

[Recognise that most countries are experimenting with new forms of remote voting methods. These methods require new, and sometimes, different forms of authentication from those used for in-person voting.

Recognise and support the broader global development on rights to a digital identity and complement the Guidelines on National Digital Identity adopted by the Consultative Committee of Convention 108.

Recognise that voter registers and voter lists may be assembled and maintained in a variety of ways and locations using both digital and non-digital media by a range of national and local authorities.

Recognise that the names and addresses of voters in the voters lists (based on the voter register) are legally shared in some jurisdictions with registered political parties and candidates for campaigning purposes, and that their use should be restricted by law to legitimate purposes of campaigning activities.

Recognise that different administrative and institutional factors shape the conduct of elections and the personal data processing practices in elections: the electoral system; the party system; the relationship between central and local party organisations; the existence of "primary elections"; the frequency of referendums; and others.

Recognise that many countries have introduced, or will introduce, biometric forms of identification to register and authenticate voters, and that safeguards are necessary (even where the introduction of biometrics is not being actively considered).]

Commented [A158]: Toute cette partie que je mets entre [ ] ne devrait-elle pas être déplacée dans un préambule (comme dans les recommandations).

(…)

4. Application of Convention 108+ to the use ~~of Special Categories~~ of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

(…)

In states where those under the age of 18 may legally vote, EMBs should take special care to protect the personal data of young people according to Article 15(e) Convention 108+.[59]

(…)

4.2. Processing of special categories of data (including biometric data~~)~~ that uniquely identifies an individual) for voter registration and authentication (Article 6)

(…)

The processing of personal data revealing political opinions entails severe risks of voter discrimination and can lead to voter suppression and intimidation. The knowledge of who has, and has not, voted can (in some societies) also affect the provision of government services. The processing of special categories of personal data needs to be accompanied by safeguards appropriate to the risks at stake of voter discrimination and of the interests, rights and freedoms protected and has to take into account the domestic legislation on access to official documents as well.

The processing of personal data revealing political opinions entails severe risks of voter discrimination and can lead to voter suppression and intimidation. The knowledge of who has, and has not, voted can (in some societies) also affect the provision of government services. The processing of special categories of personal data needs to be accompanied by safeguards appropriate to the risks at stake of voter discrimination and of the interests, rights and freedoms protected and has to take into account the domestic legislation on access to official documents as well.

The analysis, sorting and profiling of groups of voters on geographical and/or demographic factors, can have discriminatory effects[60] when predictions about groups of voters based on shared characteristics, and based on large data sets, are used to target or otherwise single-out specific voters.

EMBs should not disclose personal data to third parties unless ~~permitted~~provided by domestic law ~~that provide for~~with appropriate safeguards for the protection of personal data and private life of individuals. EMBs should not disclose data from voter registration to third parties (such as data brokers) to monetise, or otherwise reprocess for the purposes of selling anonymised or de-identified data.

[EMBs should not use data in the voter register for purposes of promoting democratic participation and encouraging voter turnout ~~without the express consent of the voter, or~~ unless ~~permitted~~ provided by law. If consent can be an appropriate legal basis for such processing the consent shall be free, informed, and unambiguous~~.~~]

(…)

[59] Explanatory report, para. 125.

[60] Council of Europe, The Protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/REC (2010) 13 (November 23, 2010)

Commented [A159]: La Convention 108+ s'applique à toutes données personnelles

Commented [A160]: N'y-a-t-il pas une contradiction à demander des garanties contre les risques de discrimination et à réserver les lois sur l'accès aux documents officiels ? Si ces lois peuvent entrer en ligne de compte, elles ne peuvent le faire qu'en préservant les droits de personnes contre des risques mentionnés à l'article 6. Peut-être serait-il plus sage à ne pas faire une référence expresse à ces lois ici ! Celles-ci sans être expressément sont également visées dans le § ci-dessous sur la communication des données "EMBs should not disclose personal data …"

Commented [A161]: N'y-a-t-il pas une contradiction à demander des garanties contre les risques de discrimination et à réserver les lois sur l'accès aux documents officiels ? Si ces lois peuvent entrer en ligne de compte, elles ne peuvent le faire qu'en préservant les droits de personnes contre des risques mentionnés à l'article 6. Peut-être serait-il plus sage à ne pas faire une référence expresse à ces lois ici ! Celles-ci sans être expressément sont également visées dans le § ci-dessous sur la communication des données "EMBs should not disclose personal data …"

4.6. Additional obligations and recommendations for Election Management Bodies and other authorities (Article 10)

The obligation rests with the data controller to ensure adequate data protection and to be able to demonstrate that data processing follows applicable laws. The accountability of data controllers and data processors should be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10(1) of Convention 108+.

Commented [A162]: Il faudrait adopter le même style de citation pour l'ensemble du texte; parfois on mentionne après l'article, parfois pas !

EMBs and the processors should provide a full record of how personal data has been obtained and is being processed, as well as demonstrate compliance of any third-party organisation that processes personal data on their behalf.

EMBs should ~~assess~~ examine the likely impact of intended data processing on the rights and fundamental freedoms of the voter, prior to collection and the commencement of data processing and should design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms (Article 10(2)).

Commented [A163]: C'est le terme utilisé dans la Convention

Data protection assessments should ~~assess~~ examine the specific impact on data subjects' rights but also consider whether the processing is in the best interests of broader democratic values and the integrity of democratic elections.

(…)

Supervisory ~~(~~data protection~~)~~ authorities can also assist EMBs within the scope of their competencies. They have valuable experience in the detailed and practical work of data protection implementation and privacy management and can assist in the tailoring of rules to the electoral context.

(…)

4.7. Additional Obligations for processing of biometric data for voter registration and authentication

(…)

Developers and manufacturers of biometric technologies shall take steps to ensure that the biometric data are accurate under Article 5 of Convention 108+. This involves continual testing their systems to eliminate disparities, particularly according to ethnicity, age and gender. They should integrate data protection by design principles into the manufacture of biometric products and services. They should also examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of the data processing and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms. The moreover should implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

In compliance with Article 15(3) of Convention 108+, supervisory authorities shall be consulted on proposals for the introduction of biometric forms of identification for voter registration and authentication. These authorities shall be consulted systematically and in advance of the deployment of biometric voter registration schemes.

EDPS

1. Introduction

(…)

~~Supervisory Relevant oversight authorities~~ ~~(could includ~~e~~ing~~ EMBs, data protection authorities (DPAs), and other oversight agencies~~)~~ may wish to adapt these guidelines to their particular electoral systems. They may also wish to consider developing domestic codes of practice on voter registration and authentication, alone or in cooperation, sensitive to their domestic political systems, and consistent with ~~their~~ the responsibilities of DPAs under Article 15 of Convention 108+.

Commented [A164]: As explained further below, we recommend to clearly differentiate between DPAs (supervisory authorities when it comes to the processing of personal data) and EMBs or other public organisations acting as controllers when it comes to the processing of personal data.

We made an editorial suggestion to implement this comment.

2. Scope and Purpose

These guidelines:

Apply the data protection principles of Convention 108+ to the processing of personal data for purposes of voter registration and authentication.

Apply mainly to Electoral Management Bodies (EMBs) as data controllers and may be relevant to ~~/or to~~ other regulatory and/or supervisory authorities responsible for the protection of personal data~~ as data controllers,~~ thereby contributing ~~for the purposes of~~to the protection ~~ng~~ of the right to vote in a free and equitable manner.

Commented [A165]: We are not sure to understand the impact of latest changes here: are we suggesting that DPAs will act as data controllers for the purposes of voters registration and authentication?

See proposed editorial changes to reflect that EMB will be data controllers.

(…)

3. Definitions for the purposes of the Guidelines

In addition to the definitions stipulated in Article 2 of Convention 108+, the guidelines use the following terms to ensure a uniformity of definition:

"~~Supervisory~~ Relevant oversight authorities" refer to those independent regulatory agencies that might have oversight responsibility for the processing of personal data for electoral purposes, and includes data protection authorities (DPAs) and election management bodies (EMBs)

Commented [A166]: We would recommend to clearly differentiate between DPAs and EMBs and not have them under the same definition. EMBs are already defined below. If we want to have a definition of supervisory or relevant oversight authority, this definition should then clarify that it is the authority competent for supervising the processing of personal data, ie the DPA pursuant to Art 15 of C108+

(…)

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

(…)

Where EMBs obtain personal data from other authorities (such as tax authorities, or population registries) those data should only continue to be used based on a legitimate base, for the defined and specified purpose and should only be retained for as long as necessary to register the voter.

Commented [A167]: Given the nature of EMBs (public bodies), we would rather recommend to specify that they may only obtain personal data from other authorities if laid down under local law that provides adequate safeguards, as stated in Article 6 of Convention 108+.

4.2. Processing of special categories of data (including biometric data) that uniquely identifies an individual for voter registration and authentication (Article 6)

(…)

In the context of voter registration, the recording of information on whether or not the individual voted in a particular election is information that may reveal political opinions. The recording over time of voting histories is also information that may reveal political opinions. These are all personal data falling within the special categories of data under Convention 108+. The processing of those information might also fall under the domestic legislation on access to official documents.

Commented [A168]: in this case, the rights to privacy and data protection of persons concerned shall however be duly taken into account.

suggestion to add something along these lines.

In some countries, various individuals might be legitimately prohibited from voting on the grounds of criminal record, mental capacity, [] . These data are special categories data which can lead to unlawful discrimination and are therefore subject to the highest safeguards.

The processing of personal data revealing political opinions entails severe risks of voter discrimination and can lead to voter suppression and intimidation. The knowledge of who has, and has not, voted can (in some societies) also affect the provision of government services. The processing of special categories of personal data needs to be accompanied by safeguards appropriate to the risks at stake of voter discrimination and of the interests, rights and freedoms protected and has to take into account the domestic legislation on access to official documents as well.

Commented [A169]: Same comment as above

The analysis, sorting and profiling of groups of voters on geographical and/or demographic factors, can have discriminatory effects[61] when predictions about groups of voters based on shared characteristics, and based on large data sets, are used to target or otherwise single-out specific voters.

EMBs should not disclose personal data to third parties unless permitted by domestic law that provide for appropriate safeguards for the protection of personal data and private life of individuals. EMBs should not disclose data from voter registration to third parties (such as data brokers) to monetise, or otherwise reprocess for the purposes of selling anonymised or de-identified data.

Commented [A170]: We would say not disclose to third parties **nor repurpose**

(…)

4.7. Additional Obligations for processing of biometric data for voter registration and authentication

(…)

The application of biometric forms of identification (and especially facial recognition) should only be for purposes of voter registration and in any case authentication and should not be processed to infer race, ethnic origin, age, health or other social conditions.

Commented [A171]: added 'in any case'

The application of biometric forms of identification (and especially facial recognition) should only be for purposes of voter registration and in any case authentication and should not be processed to infer race, ethnic origin, age, health or other social conditions.

Commented [A172]: added 'in any case'

Where facial recognition is used, no digital images should be used that were uploaded to the internet or social media sites, or captured by video surveillance.[62]

No biometric data should ever be shared with political parties, political candidates or campaign organisations, unless explicitly authorised by law.

Commented [A173]: Before ‚having this last part of the sentence, it would be interesting to understand better what are the use cases we have in mind here and that would justify such sharing authorised by law?

(…)

[61] Council of Europe, The Protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/REC (2010) 13 (November 23, 2010)

[62] Guidelines on facial recognition, p. 9.

PRIVACY INTERNATIONAL

1. Introduction

(…)

Biometric data is just one category of ~~sensitive~~ special categories of data given special protection by international instruments such as the Council of Europe's Convention for the protection of individuals with regard to the automatic processing of personal data (ETS No. 108) as amended by Protocol CETS No. 223[63] ("Convention 108+", "Convention") whose processing can lead to a variety of individual and social risks to privacy, and to other human rights. There are risks to the secrecy of the ballot, of voter intimidation and discrimination, of disenfranchisement of eligible voters, of security and data breaches, of the uses of official registration data for campaigning activities, and of the integration of voter registration databases with other national identifications systems as well as privately controlled datasets.

(…)

~~Supervisory~~ Relevant oversight authorities (which could include~~ing~~ EMBs, data protection authorities (DPAs), and other oversight agencies) may wish to adapt these guidelines to their particular electoral systems. They may also wish to consider developing domestic codes of practice on voter registration and authentication, alone or in cooperation, sensitive to their domestic political systems, and consistent with ~~their~~ the responsibilities of DPAs under Article 15 of Convention 108+.

2. Scope and Purpose

(…)

Recognise ~~and support~~ the broader global development on rights to a digital identity and complement the Guidelines on National Digital Identity adopted by the Consultative Committee of Convention 108.

Commented [A174]: Concerns about the human rights implication of the introduction of digital identity abound (see Privacy International, https://privacyinternational.org/campaigns/identity-crisis) For this reason, we recommend these guidelines avoid expressing support for such developments.

(…)

Recognise that the procurement of technologies necessary to adopt biometrics forms of identification requires robust human rights due diligence, transparency and accountability to mitigate the risks to human rights posed by the introduction of these technologies and by the public private partnerships they often entail.

Commented [A175]: For some details on the issues and safeguards, please see Privacy International, https://privacyinternational.org/sites/default/files/2023-11/Data%20and%20elections%20checklist_Update_Final_21Nov_Reduced.pdf Section 1.5

3. Definitions for the purposes of the Guidelines

(…)

Biometrics refers to data resulting ~~to~~ from the automated recognition that is a specific technical processing of data concerning ~~of~~ individuals based on their distinguishing and repeatable biological (physiological), biological and/or behavioural characteristics which allows the unique identification or authentication of the individual, when it is precisely used to uniquely identify the data subject.

Commented [A176]: Any reason for using a different definition than the one included in the Explanatory report? "Data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics
of an individual which allows the unique identification or authentication of the individual"

[63] Council of Europe (2018), *Convention for the protection of individuals with regard to the processing of personal data* (2018) at: https://rm.coe.int/convention-108-for-the-protection-of-individuals (hereafter Convention 108+).

4. Application of Convention 108+ to the use of Special Categories of Personal data for Voter Registration and Authentication

4.1. Legitimacy of data processing and quality of data in light of the legitimate purposes of voter registration and authentication (Article 5)

(…)

The legitimate purpose of voter registration and authentication is to enable the right to vote for all legitimate voters in a given electoral district. The voters' register should not include personal data other than that which is required to establish eligibility to vote. These purposes and means should be stated as precisely and fully as possible in publicly available documents, according to the transparency principle (Article 8). Further processing should be compatible with this stated purpose, under Article 5(4)b.

Commented [A177]: We suggest including this general principle here to clarify the scope of personal data to be included in the voter registry and to encourage states to apply the relevant data protection principles (notable data minimisation).

(…)

Personal data contained in official voters list are not to be further processed or shared with third parties without express authorisation in law/appropriate legal basis. Unless specifically approved by law, name and addresses from the official voters list should not be combined with other sources of personal data processed by political parties or other campaign organisations, including to create profiles of voters for micro-targeting purposes.

Commented [A178]: Micro-targeting is one of many techniques that exploit personal data of voters. We suggest adding 'including' to broaden the scope of this guideline and help making it future proof.

(…)

4.2. Processing of special categories of data (including biometric data) that uniquely identifies an individual for voter registration and authentication (Article 6)

(…)

EMBs should not disclose personal data to third parties unless permitted by domestic law that provide for appropriate safeguards for the protection of personal data and private life of individuals. EMBs should not disclose data from voter registration to third parties (such as data brokers) to monetise, or otherwise reprocess for the purposes of selling anonymised or de-identified data.

In particular, no third party other than the EMB should have access to the biometric data processed for voter registration. Biometric data (including photographs) must not be used for anything other than deduplication and/or voter identity authentication.

Commented [A179]: Given the concerns surrounding the potential abuses of biometric data, we suggest to make clear in this guidelines that only the EMB should have access to such data and limit its use only for the purpose of voter's authentication. For some references and rationale, please see Privacy International, https://privacyinternational.org/sites/default/files/2023-11/Data%20and%20elections%20checklist_Update_Final_21Nov_Reduced.pdf Section 1.2

[EMBs should not use data in the voter register for purposes of promoting democratic participation and encouraging voter turnout ~~without the express consent of the voter, or~~ unless permitted by law. If consent can be an appropriate legal basis for such processing the consent shall be free, informed, and unambiguous]

(…)

4.3. Data security and confidentiality (Article 7)

Applying appropriate security measures to voter registration data, and its processing environments both at rest and in transit, is vital to ensure voters' data are protected to the highest standards. Security measures should take into account the current state of the art data-security methods and techniques in the field of data processing. [Their [cost] should be commensurate with the seriousness and probability of the potential risks.][64]

[64] Explanatory report, para 63.

Additional protection for biometric data against unauthorised access or other data breaches should be developed and deployed, including storing biometric data separately from other data.

Commented [A180]: Here or in the section below, we recommend to flag the additional security consideration necessary for the processing of biometric data. For more details, see see Privacy International, https://privacyinternational.org/sites/default/files/2023-11/Data%20and%20elections%20checklist_Update_Final_21Nov_Reduced.pdf Section 1.2

(…)

4.4. Transparency of processing of personal data for voter registration and authentication (Article 8)

~~The p~~Personal data []shall be processed fairly and in a transparent manner at all stages of the electoral process, especially considering the potential for the manipulation of voters.

(…)

4.5. Rights of data subjects (Article 9)

Data subjects should be able to obtain on request, free of charge and without excessive delay ~~or expense~~, confirmation of the processing of personal data relating to him or her in a voter register, and to access to those data in an intelligible form.

Commented [A181]: We suggest to clarify that the exercise of the right to access should be free of charge.

(…)

Data subjects are, upon request under Article 9(1)(b &c), entitled to be informed free of charge and without excessive delay ~~and expense~~, about the reasoning underlying the processing of their personal data by EMBs, of the data processed and its origin, and of the preservation period. This might be particularly important where a voter has been denied registration.

(…)

4.6. Additional obligations and recommendations for Election Management Bodies and other authorities (Article 10)

The obligation rests with the data controller to ensure adequate data protection and to be able to demonstrate that data processing follows applicable laws. The accountability of data controllers and data processors should be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10(1) of Convention 108+.

All documentation relating to the procurement process engaging a third party for the provision of technology required to process personal data should be made publicly available. Private companies purporting to provide such election technology should waive commercial confidentiality and make their technologies fully auditable to enable understanding of its functioning. Contracts for the provisioning of electoral technology should give explicit details of the company's access to data including ownership, and provide for corresponding safeguards to ensure security and proper handling of the data.

Commented [A182]: Given the increase reliance on private companies in the processing of data for electoral purposes, we recommend the inclusion of this language to guide EMB when they enter public/private partnerships.

(…)

While the implementation of these guidelines will be shaped by local political contexts, it may also require collaboration between supervisory authorities. [~~The global industry that supports biometric registration knows no geographic boundaries.~~] The impact of ~~this~~ the biometric industry nationally and internationally will require the most vigilant and constant cross-national attention from EMBs and supervisory authorities through their international and regional associations.

Commented [A183]: Assuming, from the previous struck out sentence

4.7. Additional Obligations for processing of biometric data for voter registration and authentication

(…)

The integration of biometric forms of identification into existing voter registration databases poses serious risks to the privacy of individuals, particularly when the application of these technologies does not always require the awareness or cooperation of individuals.[65]

(…)

[65] Guidelines on facial recognition, p. 5.