COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 27 ~~November~~February 202~~3~~4 T-PD(2023)2rev~~2~~3

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

CONVENTION 108

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

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 ~~voter~~ the authentication of a voter's identity at the time of voting, whether in person or remotely. 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.

In recent years, however, various states have introduced new methods of voter registration and authentication, often based on biometric data. There are various trends at work: the pervasive problem of "techno-solutionism"; narratives (often false) in some countries about voter fraud and impersonation; and the power of a global biometrics industry that aggressively promotes new forms of voter registration and authentication as necessary to promote the principle of "one voter, one vote", a condition for the exercise of free, and transparent elections. Underlying these pressures are broader efforts to promote universal rights to a "digital identity" promoted by various international organisations and the subject of prior guidelines from the Council of Europe.[1]

These trends are particularly notable in countries where new technologies are being introduced for voter registration, and particularly in Africa. However, digital identity rights, and secure online access to the range of government services are issues globally. As new digital forms of citizen authentication are introduced to certify a citizen's legal identity to access the range of government services, there is, and will continue to be, pressures to use those same techniques for the registration and authentication of voters.

Biometric data is just one category of special categories of data given additional ~~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[2] ("Convention 108[~~+~~]", "Convention") whose processing may entail particular risks for data subjects[3] 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 data breaches from voter registers, ~~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.~~ population registers[/database].

Formatted: Not Highlight

The analysis of the introduction of new techniques for electoral registration and authentication purposes should be viewed in the context of wider concerns about the processing of special categories of personal data for electoral and campaign purposes, the subject of earlier analysis and guidance from the Council of Europe [4].

[1] Council of Europe, Consultative Committee on the Convention for the protection of individuals with regard to the automatic processing of personal data, *Guidelines on National Digital Identity.* Strasbourg: Council of Europe (February 2023)

[2] 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+).

[3] 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. Para 57.

[4] Council of Europe, Consultative Committee of the Convention for the protection of individuals with

regard to automatic processing of personal data, *Guidelines on the Protection of Individuals with regard to the processing of personal data by and for electoral campaigns*. Strasbourg: Council of Europe (adopted November 19, 2021); Colin J. Bennett, *Personal Data Processing by and for Political Campaigns: The Application of the Council of Europe's Modernised Convention 108*. Directorate General of Human Rights and Rule of Law, Strasbourg October 26, 2020 at: https://rm.coe.int/political-campaigns-en.

This guidance addresses questions about the data collected, processed and managed by official electoral management bodies (EMBs) and other authorities or organisations for the purpose of voter registration and authentication. ~~For the purpose of~~For these guidelines, t~~T~~he data controllers and 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.

The aim of these guidelines is to provide practical advice to ~~EMBs and other~~ data controllers ~~supervisory authorities~~ about how systems of voter registration and authentication should comply with Convention 108~~+~~ [5] 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.

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;[6] on political campaigning;[7] on artificial intelligence;[8] and on facial recognition.[9]

Different jurisdictions ~~Relevant oversight authorities (could include 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 the responsibilities of Data Protection Authorities (DPAs) under Article 15 of Convention 108~~+~~ and in complementing other existing national supervisory and/or oversight mechanisms, regimes.

2. Relevant national contexts

These guidelines

Recognise that some 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 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

[5] 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.

[6] Council of Europe (2023). Consultative Committee on the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on National Digital Identity.* Council of Europe (adopted February 2023)

[7] Council of Europe (2021). Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns.* Strasbourg: Council of Europe (adopted 19 November 2021)

[8] 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)

[9] 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)

108.[10]

Recognise that the procurement of technologies necessary to adopt biometric forms of identification requires robust 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.

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 further processing should be restricted by law to the 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 mandatory requirements for voting; 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. Such safeguards should be considered before introducing biometric forms of identification, even where the introduction of biometrics is not being actively considered or implemented.

~~2.~~3. 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 to data controllers responsible for the management of voter registers and lists in a given jurisdiction, and to the data processors employed by those controllers. Data controllers include: national and regional ~~mainly to~~ Electoral Management Bodies (EMBs); ~~-~~and local, regional and municipal authorities responsible for the management of voter registers and lists. ~~and/or to other regulatory and/or supervisory authorities responsible for the protection of personal data as data controllers, thereby contributing to the protection 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.

[10] Council of Europe (2023). Consultative Committee on the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on National Digital Identity*. Council of Europe (adopted February 2023)

~~These guidelines a~~Apply to all voting methods, whether in person, by mail or online (e-voting).

~~Recognise that some~~ 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. ~~These guidelines apply to all voting methods, whether in person, by mail or online (e-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.~~[11]

~~Recognise that the procurement of technologies necessary to adopt biometric forms of identification requires robust 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.~~

~~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 further processing use should be restricted by law to the 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 mandatory requirements for voting; 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. Such safeguards should be considered before introducing biometric forms of identification, even where the introduction of biometrics is not being actively considered or implemented.~~

~~3.~~4. 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:

"~~Relevant~~ Competent ~~oversight~~ supervisory authorities" refer to those independent regulatory agencies that ~~might~~ have oversight responsibility for the processing of personal data for electoral purposes, and perform the functions specified in Article 15. These might include other official regulators in addition to ~~and includes~~ data protection authorities (DPAs) [such as EMBs]. ~~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.

Voter registers are the consolidated, official lists of all persons eligible to vote and the underlying personal data processed ~~for this purpose~~in these registers (being stand alone or combined, centralised or federated, etc).

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.~~

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. Voter authentication ~~Authentication~~ is the process of verifying that proof, as well as verifying that the individual is eligible to vote in a particular district in a particular election. ~~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.

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.[12]

Personal data for the information they reveal relating to ~~revealing~~ "political opinions" are a special category of data under Article 6 (1) of the Convention and may include data on voting activity. Data on whether or not a voter has voted, in combination with information on the context, place and method of voting, might reveal political opinions. ~~ty, 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.~~

Biometric data means personal data resulting from specific technical processing of data concerning the relating to the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual, is also considered sensitive when it is precisely used to uniquely identify the data subject.[13] ~~s refers to data resulting from the specific technical processing of data concerning 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.~~

A biometric template is the mathematical representation of features or characteristics from the source biometric data.

Formatted: Font: 11 pt, Not Bold

~~[11] Council of Europe (2023). Consultative Committee on the Convention for the protection of individuals with regard to automatic processing of personal data. *Guidelines on National Digital Identity.* Council of Europe (adopted February 2023)~~

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

[13] Explanatory report, para 58.

4. Application of Convention 108+ to the use of ~~Special Categories of~~ Personal 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 [eligible/~~-~~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. Further processing should be compatible with this stated purpose, under Article 5(4)(b).

Consistent with the principle of data minimi~~s~~zation, data processed in voter registers and voters lists should be limited to that necessary for the registration and authentication of voters (Article 5(4)(c))

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, that ~~ose~~ interest~~s~~ should be clearly stated by law and duly referenced in the privacy polici~~es~~ of EMBs and other data controllers.

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."[14]

Unless prohibited by law, the voter may withdraw his or her consent to be included in the voter register at any time.[15]

[14] Explanatory report, para 42. In most societies, voter registers are derived from mandatory national and/or local population registers. Individual consent is, therefore, overridden by the legitimate basis laid down by law of the voter register. Some jurisdictions do, however, permit voters to remove their names and addresses from voter registers for legitimate reasons.

[15] Explanatory report, para. 45.

The principle of purpose limitation (Article 5(4)(b) stipulates that personal data should be collected for explicit, specified and legitimate purposes and not disclosed in a way incompatible with those purposes. Personal data on voters' registration should not be used for other purposes unless there is a legitimate basis laid down in law, and should especially not be further used for "undefined, imprecise or vague purposes"[16]. When considering "compatible uses" a~~A~~ reliance on the concept ~~of "compatible uses"~~ should not hamper the transparency, legal certainty, predictability or fairness of the processing. [17]

Personal data on voters should not be further processed in a way that the voter might consider "unexpected, inappropriate or otherwise objectionable."[18]

~~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 in election campaigns with clear prohibitions and appropriate sanctions for using the data for any other purposes.

Personal data contained in official voter~~s~~ registers and list~~s~~ are not to be further processed or shared with third parties without express authorisation in law and an ~~/~~appropriate legal basis. ~~Unless specifically approved by law,~~ Nname 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, including 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 safeguards exist to ensure the protection of personal data, particularly through the anonymisation or pseudonymisation of the data [19] 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 influence or pressure should be exerted on a voter or potential voter to provide personal data for the purpose of voter registration, beyond that necessary to encourage participation in the democratic process.[20]

~~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.~~

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.

In states where those under the age of 18 may legally vote, EMBs should take special care to

[16] Explanatory report, para 48.
[17] Explanatory report, para 49.
[18] Explanatory report, para. 49.
[19] Explanatory report, para 50.
[20] Explanatory report, para. 42.

protect the personal data of young people according to Article 15(e).[21]

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

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

These paragraphs ~~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~~.

~~[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.]~~

[21] Explanatory report, para. 125.

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 in the context of voter registration and authentication, should be considered as a special category of data.

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."[22]

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. 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 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~~appropriate 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 lead to discrimination 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[23] 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.

[22] Convention 108+, Article 6
[23] 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)

~~[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 for each processing of ~~to~~ voter registration data, and its processing environments both at rest, in use 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 the high potential adverse consequences for the individuals, the sensitive nature of the personal information, 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, and requirements for long term storage. ~~.~~ Risk assessment should seek to embed these 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.

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 and equipment where personal data in the voter register or the voter lists are stored; ~~,~~ the possible ~~possibility of~~ checking of the resilience of security measures under a false name; the storage of biometric data separately from other personal data; and the maintenance of secure logs of all actions relevant to data security. ~~and equipment where personal data in the voter register or the voter lists are stored.~~

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 be bound by ~~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

EMBs should at least report to the competent 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 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.

~~Risk assessment prior to processing should assess whether data is protected against~~

[24] Explanatory report, para 63.
[25] Explanatory report, para 66.

~~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)

The 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.

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 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.

Where 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 has to be initiated by the individual (~~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 by volunteers and/or employees at the household level~~s~~, 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.

The processing of data on voter registration should also comply with domestic publicity laws and legislation on access to official documents.

4.5. Rights of data subjects (Article 9)

Data subjects should be able to obtain on request at reasonable intervals~~iews~~ and without excessive delay or expense, confirmation of the processing of personal data relating to him or

[26] Convention 108, Article 8(3)
[27] Explanatory report, para. [12.]

her in a voter register or voter list, all available information on their source and on the preservation period, and to access to those data in an intelligible form (Article 9(1)(b). Data subjects are entitled to be informed, upon request, how their personal data was obtained for the voter register, and from what source.

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 subjects shall have the right to be provided, on request, and without excessive delay or expense, 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 have been denied registration, or have been ~~are~~ deregistered from a voting register (for reasons of ~~[~~age~~]~~, mental capacity, or criminal record), they have the right to be informed of the reasons for the decision in a manner that is sensitive to the rights and interests of the individual. ~~.~~

Data subjects shall have the right ~~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 (Article 9(1)(d). The purpose of ensuring accurate voter registration and authentication would be such a 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.~~

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 data controllers ~~authorities~~ (Article 10)

[28] Explanatory report, para. 72.

The accountability principle requires that the data controller and, where applicable, the processor, should ensure compliance with data protection principles, and should be able to demonstrate that the ~~obligation rests with the data controller to ensure adequate data protection and to be able to demonstrate that~~ data processing is in conformity with data protection law and other ~~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+.~~

EMBs and any ~~the~~ processors employed 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 responsibilities of data controllers and data processors should be clearly set out in any contractual arrangements, defined by the nature of the processing (Article 10(1)).

Other measures can include setting up internal procedures to enable the verification and demonstration of compliance and employee training. EMBs should appoint an officer responsible for the verification and demonstration of compliance with the data protection principles enshrined within Convention 108~~+~~.[29]

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)).

Data protection assessments should examine ~~assess~~ the specific impact of the intended processing on data subjects' rights but also consider whether specific ~~the~~ processing operations are ~~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 organis~~z~~ation ~~the [political organisation]~~, both during and between election cycles.

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

[29] Explanatory report, para. 87.

~~compliance with the data protection principles enshrined within Convention 108+.~~[30]

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 the global biometrics ~~is~~ 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, resulting from specific technical processing concerning the physical, biological or physiological characteristics of an individual, which allows the unique identification or authentication of the individual is protected as a sensitive category of data under Article 6 of Convention 108, when it is used uniquely to identify the data subject.

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 under Article 6.

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.[31]

The integration of automated forms of biometric ~~forms of~~ identification into existing voter registration databases poses serious risks to the privacy of individuals and to the democratic rights of eligible voters~~, when the application of these technologies does not always require the awareness or cooperation of individuals~~.[32]

Automated b~~B~~iometric 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 automated 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 and algorithm used (such as the false positive and false negative error rates); the retention period of the biometric template used; the requirement for prior consultation ~~auditing~~ by a supervisory authority; the traceability of the use and sharing of the biometric template;

and the safeguards used.[33]

The automated 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.[34]

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 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.

Developers and manufacturers of biometric technologies ~~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. They ~~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.

All documentation relating to the procurement process engaging a third party for the provision of biometric technology required to process personal data should be made publicly available. Private companies providing such election technology should waive commercial confidentiality and make their technologies fully ~~auditible~~auditable to enable wide understanding of the functions and capabilities of the system. 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 ~~management of~~management of the data.

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

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

Formatted: Font: 10 pt