COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 10 September 2021 T-PD-BUR(2021)3rev2

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 by and for Political Campaigns

Contents

1. Introduction 2

2. Scope and Purpose 3

3. Definitions for the purposes of the Guidelines 5

4. The Application of Convention 108+ to Political Campaigns and Campaign Organizations 7

4.1. Legitimacy of data processing and quality of data (Article 5) 7

4.2. The processing of the special category of data on political opinions (Article 6) 9

4.3. Data security in political campaigns (Article 7) 11

4.4. The Transparency of processing of personal data in political campaigns (Article 8) 12

4.5. The Rights of Data Subjects (Article 9) 12

4.6. Additional Obligations of Political Campaigns (Article 10) 13

5. Recommendations for Supervisory Authorities (Article 15) 14

1. Introduction

Effective political communication is central to democratic forms of government. Voters need information about candidates and political parties, and about their future plans and policies. And political campaigns can more effectively engage with the electorate and mobilize voters if they have accurate information on voters' beliefs, preferences and intentions. Political campaigns are a core element of the democratic process, and there is an important public interest in processing personal data for political campaigning, governed by high standards of personal data protection.

However, as political campaigns have employed contemporary digital technologies and communications tools, they have been able to target voters with increasing sophistication. A "political influence industry" operates in many countries and now enables campaigns to profile the electorate with increasing accuracy, and to deliver "micro-targeted" messages through various means, to narrow segments of voters based on those profiles. Trust and confidence in the integrity of elections can be undermined by the hidden practices that permit the manipulation of data on the electorate. Political micro-targeting is not only about political engagement, it can also permit voter suppression, and the discouragement of voters from exercising their democratic rights.

As elections in most countries have become increasingly "data-driven," it is therefore critically important that all organizations involved in political campaigns process personal data on voters in compliance with well-established data protection principles.

~~Moreover, recent scandals, including that involving Cambridge Analytica and Facebook, have demonstrated graphically that trust and confidence in the integrity of elections can be undermined by the hidden practices that permit the manipulation of the electorate. Thus~~F~~, f~~amiliar data protection questions are now at the center of a heated international debate about the integrity and resilience of democratic institutions, and about the rights to free elections enshrined in the European Convention on Human Rights.

Thus, i~~I~~nternational instruments for the protection of data, such as the Council of Europe's Convention ETS No 108 for the protection of individuals with regard to the processing of personal data as amended by the Protocol CETS No 223 (Convention 108+)~~108~~,[1] assume an increasing importance in the regulation of data-driven elections, and in the support of broad democratic principles of pluralism and individual autonomy. These Guidelines recognize that the application of sound data protection principles can go a long way to addressing broader issues of election integrity and restoring trust in democratic processes in the digital age.

Convention 108+ is explicitly rooted in a broad aim "to secure the human dignity and protection of the human rights and fundamental freedoms of every individual." It speaks of "personal autonomy based on a person's right to control of his or her personal data and the processing of such data." It recognizes that the "right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression."[2] These Guidelines attempt that reconciliation.

~~These Guidelines recognize that~~ T~~t~~he protection of the right to privacy in political campaigns is crucial to the conduct of free and fair elections, as expressed in Article 3 of Protocol No. 1 of the European Convention on Human Rights (ECHR): "Everyone has the right to elect the government of his/her country by secret vote. Without this right there can be no free and fair elections. It guarantees the citizens' free expression, the proper representativeness of elected representatives and the legitimacy of the legislative and executive bodies, and by the same token enhances the people's confidence in the institutions."

[1] 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-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (hereafter Convention 108+)

[2] Convention 108+, Preamble.

These Guidelines recognize the principles of free expression and robust public debate in both offline and online media, as expressed in Article 10 of the ECHR on freedom of expression: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." The illegitimate processing of personal data revealing political opinions can chill political speech, and adversely affect rights of free political communication protected by the ECHR.

The European Court of Human Rights has repeatedly held that the expression of political opinions has privileged status, as a basis for free expression and free elections. Further, the right to free elections enshrined in Article 3 of the ECHR entails a positive obligation on member states to establish the conditions under which individuals can freely form and express their opinions and choose their representatives without discrimination. Article 14 prohibits discrimination on grounds of "political or other opinions."[3]

Article 4 of Convention 108+ obliges Parties to incorporate its provisions into their law, and to secure their effective implementation in practice. The Convention requires that the law be applied to all data controllers and processors within its jurisdiction, including political parties and other campaigning organizations.

In many countries in Europe and elsewhere, data protection law applies, and has always applied, to the personal data processed by the organizations involved in political campaigning – including the political parties, their candidates, and the various data brokers, voter analytical companies, platforms, advertising and other companies that might process personal data on their behalf. Only relatively recently, however, have supervisory authorities grappled with the tricky questions of how to reconcile the privacy rights of the voter and the democratic obligations of political campaigns to communicate with the electorate.

The aim of these Gguidelines is to provide practical advice to supervisory authorities, regulators and to political organizations about how that reconciliation should occur. They demonstrate how the processing of personal data for the purposes of political campaigning should comply with the Council of Europe's Modernized Convention ~~for the Protection of Personal Data (Convention 108+), as interpreted through the Explanatory Report to Convention~~ 108+.[4] They offer a framework through which individual data protection authorities, and other regulators, may provide more precise guidance tailored to the unique political, institutional and cultural conditions of their own democratic states.[5]

2. Scope and Purpose

2.1. These Guidelines apply the data protection principles of Convention 108+ to the processing of personal data carried out by ~~in~~ political campaign organizations recognizing the increasing use of digital campaigning strategies via social media and the increasing

[3] European Court of Human Rights, Guide on Article 14 of the European Convention of Human Rights and on Article 1 of Protocol No. 12 to the Convention (August 31, 2020), p. 30 at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf

[4] 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. CETS 223 at: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

[5] These Guidelines build upon the background research paper: 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/t-pd-2020-02rev-political-campaigns-en-2-/1680a0bf4b

sophistication of voter analytics.

2.2. Political campaign organizations refer to political parties, as well as more temporary organizations constituted during referendum campaigns.

2.3. Political campaigns not only refer to "election campaigns." Political campaign organizations will be constituted during referendums, for example, and also capture and process personal data on voters and potential voters for the purposes of political influence. The guidelines also recognize the reality of "permanent campaigning" in modern democracies. Rules on the capture and processing of personal data by political campaigns do not just apply to the relatively brief period during which legislatures are dissolved and formal election campaigning occurs.

2.4. Political campaign organizations collect a variety of personal data on voters including: basic contact information from a national or local list of electors provided by the election regulatory body; on donations and financial contributions ~~donors~~; and on voters' attitudes, affiliations and intentions. They also process personal data on campaign employees and volunteers; and on candidates or potential candidates. These guidelines apply solely to the processing of personal data on voters (or potential voters)

2.5. These Guidelines recognize the increasing reliance of political campaign organizations on private companies that provide data brokerage, analytics and marketing services including: personal data brokers; voter analytical companies; campaigning platforms; behavioral and micro-targeted advertising companies; social media and messaging applications. The organizational ecosystem behind political campaigning is complex and opaque.

2.6. These Guidelines recognize that the extent and effect of data-driven practices in campaigning are influenced by a range of legal and constitutional provisions in different states: provisions on freedom of communication, information and association; election law; campaign financing law; telemarketing rules; advertising codes and regulations; rules on unsolicited communications.

2.7. These Guidelines recognize 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 organizations; the existence of "primary elections"; the frequency of referendums; and others.

2.8. These Guidelines recognize that the processing of personal data on voters is influenced by cultural factors and historical legacies: trust in political elites; the level of participation in elections; and the general acceptability of direct candidate to voter communication (on the doorstep, over the phone, via text and email, through social media).

2.9. These Guidelines recognize that a range of different threats to democracy have been raised by the use of digital technologies in elections. The mass profiling of the electorate and the delivery of micro-targeted messages to increasingly narrow categories of voters can create: filter bubbles or echo chambers: voter discrimination and disenfranchisement; a possible chilling of political participation; increased polarization; the erosion of robust democratic debate; and election integrity.

~~2.10.~~ The Guidelines therefore remain high-level. Supervisory authorities -- (data protection authorities (DPAs), election regulatory bodies and other oversight agencies -- may wish to adapt these guidelines to the processing or personal data in their specific national political campaign contexts. Supervisory authorities may also wish to consider developing domestic codes of practice on political campaigning sensitive to their domestic political systems, consistent with their responsibilities under Article 15 of Convention 108+., ~~such~~

~~as those developed by the Information Commissioner in the UK.[6]~~

2.10.

2.11. Other guidelines published by the Council of Europe are also relevant to the processing of personal data in political campaigns. The Guidelines on artificial intelligence and on Big Data, for instance, should be followed to ensure that applications do not undermine the human dignity, the human rights and fundamental freedoms of voters either as individuals, or as communities.[7]

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:

3.1. "Political campaign" refers to any organized effort which seeks to influence the political choices of voters and potential voters, such as voting for candidates in national or local elections or making a choice on a specific issue in a referendum.

3.2. "Political campaign organization" is any organization that runs a political campaign.

3.3. "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[8].'.

3.4. Personal data revealing "p~~P~~olitical opinions" are a special category of ~~information~~ data under Article 6 of the Convention, and may refer to: a political ideology or creed; a political affiliation or membership; an opinion about a policy preference; and/or a predicted or inferred score on political beliefs or attachments.

3.5. "Personal political communication" encompasses different forms of communication including by: post, e-mail, text message, voicemail, phone or automated calls; and via social media platforms

3.6. "Data controllers in political campaigns" include: political parties; official candidates of political parties; campaign organizations established on a temporary basis to support nor oppose a referendum question; and other organizations ~~data processors~~ when they alone or jointly with others have decision-making power with respect to personal data processing, as ~~determine the nature of the processing as~~ defined in Article 2 (d) of Convention 108+.

3.7. "Data processors in political campaigns" process personal data on behalf of the controller under Article 2 (f) and include: public opinion companies; voter analytics companies; political consultants; social media platforms; and providers of campaigning tools and software.

~~[6] Information Commissioner's Office, Guidance on Political Campaigning: Draft Framework Code for Consultation 08-2019) at: https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf~~

[7] Council of Europe, Guidelines on Artificial Intelligence and Data Protection T-PD (2019)01 (Strasbourg, 25 January 2019). Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (Strasbourg, 23, January, 2017)

[8] GUIDELINES **CDL-AD(2010)024** ON POLITICAL PARTY REGULATION BY OSCE/ODIHR AND VENICE COMMISSION

~~3.8.~~ “ Election regulatory bodies” are those national administrators 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 list. ~~These guidelines do not apply to data that might be captured during voting process by these election regulatory bodies, including the data that might be captured during the voting process at the voting station, including those from contemporary electronic voting machines.~~

3.8.

3.9. “Voters list” refers to the national list of registered electors developed for the purposes of the verification and authentication of the legitimate voting eligible population both nationally and in local voting districts.

~~3.10.~~

~~3.11.~~3.10. A “voter profile” refers to a set of characteristics attributed to an individual, characterising a category of individuals. “Profiling” refers to any form of automated processing of personal data including use of machine learning systems consisting of the use of personal or non-personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's political opinions and his/her likelihood to vote for one party or another.

~~Fundamental principles of personal data processing in political campaigns~~

~~5.4. Convention 108+ is explicitly rooted in a broad aim “to secure the human dignity and protection of the human rights and fundamental freedoms of every individual.” It speaks of “personal autonomy based on a person’s right to control of his or her personal data and the processing of such data.” It recognises that the “right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression.”[9] These Guidelines attempt that reconciliation.~~

~~5.1.~~4.1. ~~These Guidelines recognize that the protection of the right to privacy in political campaigns is crucial to the conduct of free and fair elections, as expressed in Article 3 of Protocol No. 1 of the European Convention on Human Rights (ECHR): “Everyone has the right to elect the government of his/her country by secret vote. Without this right there can be no free and fair elections. It guarantees the citizens’ free expression, the proper representativeness of elected representatives and the legitimacy of the legislative and executive bodies, and by the same token enhances the people’s confidence in the institutions.”~~

~~5.1.~~4.1. ~~The European Court of Human Rights has repeatedly held that the expression of political opinions has privileged status, as a basis for free expression and free elections.~~

~~[9] Convention 108+, Preamble.~~

Further, the right to free elections enshrined in Article 3 of the ECHR entails a positive obligation on member states to establish the conditions under which individuals can freely form and express their opinions and choose their representatives without discrimination. Article 14 prohibits discrimination on grounds of "political or other opinions."[10]

4.1. These Guidelines recognize the principles of free expression and robust public debate in debate in both offline and online media, as expressed in Article 10 of the ECHR on freedom of expression: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

5.2.4.1. The illegitimate processing of personal data revealing political opinions can chill political speech, and adversely affect rights of free political communication protected by the ECHR.

5.2. The Guidelines build upon the prior work of the European Commission for Democracy through Law (the "Venice Commission") on the impact of digital technologies on elections and democracy.[11] The Guidelines note the Venice Commission's opinion that "personal data need to be effectively protected, particularly during the crucial period of elections" and its call for a specific "legal instrument to address the risks that the use of digital technologies in elections represents to personal data protection."[12]

5.3.4.1. Article 4 of Convention 108+ obliges Parties to incorporate its provisions into their law, and to secure their effective implementation in practice. The Convention requires that the law be applied to all data controllers and processors within its jurisdiction, including political parties and other campaigning organizations.

6.4. The Application of Convention 108+ to Political Campaigns and Campaign Organizations

45.1. Legitimacy of data processing and quality of data (Article 5)

6.1.1.4.1.1. Data processing of voters' personal data (especially that which reveals sensitive political opinions) should be proportionate in relation to the legitimate purposes of political campaigns. The capture of personal data on the opinions and preferences of voters should be proportionate to those defined purposes, and should not lead to a disproportionate interference with the voter's interests, rights and freedoms.

6.1.2.4.1.2. The legitimate purposes of a political campaigning include: canvassing political opinions; communicating about policies, events and opportunities for engagement; fundraising; conducting surveys and petitions; advertising via social media, email and text; engaging in "get-out-the-vote" operations on election day. These purposes should be

[10] European Court of Human Rights, Guide on Article 14 of the European Convention of Human Rights and on Article 1 of Protocol No. 12 to the Convention (August 31, 2020), p. 30 at: https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf

[11] Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections, adopted by the Council of Democratic Elections at its 65th meeting (Venice, 20 June 2019) and by the Venice Commission at its 119th Plenary Session (Venice, 21-22 June 2019) at: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-e

[12] European Commission for Democracy through Law (Venice Commission), *Principles for a Fundamental Rights-Compliant Use of Digital Technologies in Electoral Processes*, Council of Europe Opinion No 974/2019, p. 17.

stated as precisely and fully as possible in campaign publicity materials. Further processing should be confined to these stated purposes. –

~~6.1.3.~~4.1.3. Personal data on voters should not be used for other purposes, and should not be further used for "undefined, imprecise or vague purposes."[13]

4.1.4. ~~Where the legitimate basis for processing is based on consent, T~~the free, specific, informed and unambiguous consent of the data subject is the preferred legal basis for the processing of personal data in the political campaigning context. ~~on voters should be based on the basis of the free, specific, informed and unambiguous consent of the voter.~~ Consent ~~must~~ should be obtained within every context that political campaigns engage with voters – on the doorstep, over the telephone, via email or text, or via social media. Consent should not be inferred through "silence, inactivity or pre-validated forms or boxes."[14] The voter may withdraw his or her consent to process personal data at any time.[15]

4.1.5. In states where those under the age of 18 may legally vote, political campaigning organizations should take special care to protect the personal data of young people according to Article 15(e).[16]

4.1.6. In circumstances where political campaigns legally acquire the official voters list from the election regulatory body to assist their campaigns, the campaigns must only use those lists for the purposes of communication with the electorate and must obey all requirements laid down in law for the processing, disclosure and retention of those lists. Who is entitled to access these data, and for what purposes should be clearly stipulated in law, limited to what is necessary for engaging the electorate with clear prohibitions (and appropriate sanctions) for using the data for any other purpose.

4.1.7. Unless specifically approved by law, data contact data from the official voters list should not be combined with other sources of personal data to create profiles of voters for micro-targeting purposes.

~~6.1.4.~~4.1.8. No undue influence or pressure ~~(for example, through economic incentives of policy promises)~~ should be exerted on a voter or potential voter to provide personal data by any political campaign organization.[17]

~~6.1.5.4.1.1. The voter may withdraw his or her consent to process personal data at any time.[18]~~

~~6.1.6.~~4.1.9. When organizations campaign in person on the doorstep, campaigners should be transparent about the purposes for which they are capturing personal data. They should not record any information about the household and its occupants beyond that freely and specifically provided by the voter about his/her political views and/or preferences. They should not be inquiring ~~asking~~ about other family members (including children), tenants or ~~or~~ residents. They should not be collecting information on the household or its possessions (such as cars) for purposes of drawing inferences about political preferences or interests.

~~6.1.7.4.1.1. In circumstances where political campaigns legally acquire the official voters list from the election regulatory body to assist their campaigns, the campaigns must only use those lists for the purposes of communication with the electorate and must obey all requirements laid down in law for the processing, disclosure and retention of those lists. Who is entitled to access these data, and for what purposes should be clearly stipulated in~~

[13] Explanatory report, para 48.
[14] Explanatory report, para ~~42.~~
[15] Explanatory report, para. 45.
[16] Explanatory report, para. 125.
[17] Explanatory report, para. 42.
[18] ~~Explanatory report, para. 45.~~

~~law, limited to what is necessary for engaging the electorate with clear prohibitions (and appropriate sanctions) for using the data for any other purpose.~~

~~6.1.9.4.1.1. Unless specifically approved by law, data from the official voters list should not be combined with other sources of personal data to create profiles of voters for micro-targeting purposes.~~

~~6.1.11.~~4.1.10. Political campaigns might be required to collect and report information on donors to the campaign under relevant election financing laws. These data should only be used for purposes stipulated in applicable election financing legislation, and consistent with applicable data protection law.~~.~~

~~6.1.12.~~4.1.11. Political campaigns often obtain personal data, including inferred data, from third party organizations such as data brokers, for election or campaigning purposes to target messages to a particular audience. However, before using the data in this way, campaigns ~~must~~ should carry out full due diligence to ensure the data has been obtained lawfully.

~~6.1.13.~~4.1.12. Political campaigns should ~~must~~ ensure that personal data is accurate, and where necessary kept up-to-date.

~~6.1.14.~~4.1.13. Where the political campaigning organization relies on a "legitimate basis laid down by law" (Article 5(2)), those legitimate grounds should be stated and its legal basis accurately referenced clearly in the privacy policy of the organization. For example, political campaigning organizations may claim that some processing is carried out on the basis of "public interest or of overriding legitimate interests of the controller or the third party."[19] Where the public interest in democratic engagement is claimed as a legitimate basis for processing, those interests should ~~must~~ be clearly stated by law, duly referenced in the privacy policy and in the privacy policy, and should not conflict with the rights and interests of the individual taking into account their reasonable expectations.

~~6.1.15.~~4.1.14. Personal data on voters should not be further processed in a way that the voter might consider "unexpected, inappropriate or otherwise objectionable."[20] For instance, the political organization should not be transferring those data to other organizations, for instance, with presumed similar political goals or ideological perspectives, without the express consent of the voter.

~~6.1.16.~~4.1.15. Political campaigns should not "scrape" data from social media for the purposes of building profiles on the electorate. If a voter is a member of the organization or has affirmatively expressed a wish to follow a candidate or party on a social media platform, then the campaign might reasonably infer that he/she will wish to receive further communications from the candidate or party. But that inference should not be assumed for individuals who maybe within the wider social network of that voter, and who have not affirmatively expressed a preference to be contacted.

~~6.2.~~4.2. The processing of the special category of data on political opinions (Article 6)

~~6.2.1.~~4.2.1. Under 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." It goes on: "Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights

[19] Explanatory report, para 46
[20] Explanatory report, para. 49.

and fundamental freedoms of the data subject, notably a risk of discrimination."[21]

~~6.2.2.~~4.2.2. Article 6(1) of Convention 108+ defines special categories in terms of the "information they reveal relating to …political opinions." Information on political opinions might be revealed or inferred through predictive analytical and profiling tools from a range of other sources of information, for example: magazines and newspapers read; policy beliefs and attitudes derived from polling; membership in interest groups; and professional records and affiliations. ~~(e.g. from LinkedIn)~~

4.2.3. Political parties and other organizations collect large amounts of personal data that reveal actual or inferred political opinions: on their belief systems or ideologies; on their political affiliations and memberships; on their voting histories; and/or on policy preferences. Political organizations often profile or "score" voters on the basis of these data. These are all sensitive categories of data under Convention 108+.

~~6.2.3.~~
~~6.2.4.~~

The processing of personal data revealing political opinions entails severe risks of voter ~~discrimination~~discrimination, leading to ~~. Discrimination can produce~~ voter suppression and intimidation. The knowledge of who has, and has not, supported a governing party can also affect the provision of government services. ~~Those risks are particularly acute in countries with histories of authoritarian rule.~~

~~6.2.6.~~

~~6.2.7.~~4.2.4. The processing of sensitive categories of personal data needs to be accompanied by safeguards appropriate to the risks at stake of voter discrimination~~.~~ ~~at stake~~ and of ~~the~~ interests, rights and freedoms protected~~.~~

~~6.2.8.~~4.2.5. If political parties and other campaign organizations process special category data on political opinions, they should ~~must~~ identify both the lawful basis for processing and the condition for processing. Both should ~~must~~ be documented.

~~6.2.9.~~4.2.6. If political parties and other campaigning organizations are relying on the lawful basis of consent to collect data on political opinions and to send political messaging through electronic communications, they should ~~must~~ ensure that they have the appropriate records of consent from the individual.

~~6.2.10.~~4.2.7. Predictions about groups of voters with shared characteristics based on analysis of large sets of personal data, shall still be considered as processing personal data, even where there is no intention to communicate with an individual. The analysis, sorting and profiling of groups of voters on geographical and/or demographic factors, can have discriminatory impacts.[22]

~~6.2.11.~~4.2.8. Controllers and processors shall not disclose voters' sensitive personal data collected in the course of a political campaign, for others to monetise, or otherwise reprocess for the purposes of selling anonymised or de-identified data (for example to data brokers) without the express consent of the voter.

~~6.2.12.~~4.2.9. Geolocation tracking or geo-fencing in order to identify the location of a voter to target in-app functionality, or for profiling purposes, can reveal sensitive data and present significant risks to individuals. These services should only deployed ~~should be deployed only when necessary and~~ according to an appropriate legal basis. Services should only allow

[21] Convention 108+, Article 6

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

activation with the opt-in of the individual user. Geo-location should not be available by default.

6.2.13.4.2.10. Political campaign organizations share personal data with social media companies for the purposes of digital advertising to groups of like-minded individuals (through instruments such as Facebook's Lookalike or Customized Audiences). No personal data shall be shared with social media companies for the purposes of digital advertising without the express consent of the voter.

6.3.4.3. Data security in political campaigns (Article 7)

6.3.1.4.3.1. Political campaigns often involve the sharing of data on voters with large numbers of campaign volunteers, contractors and employees during the intense period of an election campaign. Political campaign organizations s should take appropriate security measures to ensure against accidental or unauthorized access to, destruction, loss, use, modification or disclosure of personal data. These measures include with due regard to the specificities of the medium (mobile phone, computer, IOT, email, chat, etc.) used: training in privacy and security; access controls; confidentiality agreements; and physical controls on physical access to places and equipment where personal data are stored.

6.3.2.4.3.2. Political campaign organizations should report to supervisory authorities as prescribed by Convention 108+ and to the data subjects themselves in the event of breaches which may seriously interfere with the rights and fundamental freedoms of voters in accordance with Article 7(2) of the Convention. Notification should include adequate and meaningful information about possible measures to mitigate the adverse effects of the breach.[23]

6.3.3.4.3.3. Political campaign organizations can be involved in processing voters' data on a large-scale over several election cycles. Applying appropriate security measures to this 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.[24]

6.3.4.4.3.4. Where data is processed by third party service providers, political organizations must should remain aware of their ongoing responsibilities as data controllers. Controllers should be able to demonstrate, where applicable, that processors comply with their obligations in accordance with Articles 7(1) and 10 of the Convention. Controllers must demonstrate due diligence to establish the third party's ability to protect personal data confidentiality.

6.3.5.4.3.5. Risk assessment prior to processing should must assess whether data is protected against unauthorised access, modification and removal/destruction. Risk assessment should seek to achieve outcomes that embed high standards of security throughout the processing. Such an assessment should must 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.

6.3.6.4.3.6. Political campaign organizations should train all workers on a political campaign, including employees and temporary volunteers, in the importance of privacy and security measures. Each employee or volunteer should sign confidentiality agreements. The databases of political campaigning organizations should be protected by strong access

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

controls for different categories of employees and volunteers.

~~6.4.~~4.4. The Transparency of processing of personal data in political campaigns (Article 8)

~~6.4.1.~~4.4.1. The personal data processed by political organizations shall be processed fairly and in a transparent manner to counter the opacity of contemporary digital advertising and potential for the manipulation of voters.

~~6.4.2.~~4.4.2. At the time of collection (regardless of the method of political communication), representatives of political organizations shall inform voters that they are collecting personal data on behalf of the "x party/organization."

~~6.4.3.~~4.4.3. Political campaign organizations should ~~must~~ inform voters (in a privacy policy or its equivalent) of at least: the legal name and address of the organization; the legal basis for collection of personal data for processing; the categories of personal data processed; any recipients of those data (including the third-party profiling, targeting data broker and advertising companies), and the reasons why they need to be shared; and how the voter might exercise his/her rights.

~~6.4.4.~~4.4.4. Privacy policies should ~~and other published terms and conditions, must~~ be easily accessible, legible, understandable and adapted to the relevant individuals.[25] 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 of a complete but at the same time efficient information.

~~6.4.5.~~4.4.5. In a typical communication from a political campaign, the volunteer or employee ~~will be~~should ~~expected to~~ introduce himself/herself according to a standard script and be prepared to answer questions from the voter about why the information is being collected, how it will be used, with whom it will be shared, and about how the voter might remove his/her name from the campaign's lists. Those scripts should also be publicly available on the campaign website.

4.4.6. In the context of digital advertising, political campaign organizations should provide voters with: adequate information on why they are seeing a particular message, who is responsible for it, and how they can exercise their rights to prevent being targeted; and information on any targeting criteria used in the dissemination of such communications. In the context of the automated delivery of digital political advertising, the voter should have the right to know "why I am seeing this ad."

~~6.4.6.~~4.4.7. Archives of political advertising operated by social media platforms, including the ad imprints, the targeting criteria and the timing and location of ad delivery, support the principle of transparency.

~~6.5.~~4.5. The Rights of Data Subjects (Article 9)

~~6.5.1.~~4.1.1. Data subjects ~~Voters~~ shall have the right not to be subject to decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration. ~~In the context of the automated delivery of digital political advertising, the voter should have the right to know "why I am seeing this ad."~~

[25] Explanatory report, para. 12.

~~6.5.2.~~4.5.1.

~~6.5.3.~~4.5.2. ~~Voter~~ 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, and access to those data in an intelligible form. In the case of political parties, this should include any "score" assigned to the voter which measures his/her ideological orientation.

~~6.5.4.~~4.5.3. ~~Voters~~ Data subjects are entitled to be informed how their personal information was obtained, and from what source.

~~6.5.5.~~4.5.4. Data subjects ~~Voters~~ should be able to object to the processing of data on him or her with a political organization, and to request rectification or erasure, as the case may be, if the data is inaccurate, obsolete or incomplete.[26]

~~6.5.6.~~4.5.5. ~~Voters~~ Data subjects who object to data processing for political marketing purposes are entitled to the unconditional erasure or removal of the personal data covered by that objection.[27]

~~6.5.7.~~4.5.6. ~~Voters~~ Data subjects are entitled to know about the reasoning underlying the processing of their personal data by political campaigns. This may be particularly important where a voter is contacted by a political party with whom they have not had a prior relationship.

~~6.5.8.~~4.5.7. ~~Voters~~ Data subjects are entitled to remedy if their rights under the Convention are violated ~~are not respected~~ by political campaign organizations.

~~6.5.9.~~4.5.8. ~~Voters~~ Data subjects are entitled to benefit from the assistance of a supervisory authority in exercising his or her rights.

~~6.6.~~4.6. Additional Obligations of Political Campaigns (Article 10)

~~6.6.1.~~4.6.1. 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 ~~must~~ be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10(1) of the Convention 108+.

~~6.6.2.~~4.6.2. Political parties and other campaigning organizations ~~must be able~~should ~~to~~ provide a full record of how personal data has been obtained and is being processed, as well as demonstrate compliance of any third-party organization that processes personal data on their behalf.

~~6.6.3.~~4.6.3. Political campaigning organizations ~~must~~ should assess the likely impact of intended data processing on the rights and fundamental freedoms of the voter, prior to 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)).

~~6.6.4.~~4.6.4. Data protection and privacy impact assessments should not only assess the specific impact on an individual voter's rights, but should also consider with the processing is in the best interests of broader democratic values and the integrity of democratic elections.

[26] Explanatory report, para. 72.
[27] Explanatory report, para 79.

~~6.6.5.~~4.6.5. Data controllers should encourage and implement a comprehensive and compliant data governance culture throughout the political organization, both during and between election cycles.

~~6.6.6.~~4.6.6. Political parties and other campaigning organizations should appoint an officer responsible for the verification and demonstration of compliance with the data protection principles enshrined within Convention 108+.[28]

~~7.~~5. Recommendations for Supervisory Authorities (Article 15)

~~7.1.~~ Without prejudice to their powers and tasks in respect of the processing of personal data according to Article 15 of Convention 108+, s~~S~~upervisory authorities should cooperate with other responsible regulators, including elections and telecommunications regulators to: understand the complete campaigning network within their countries; and the diverse array of constitutional, statutory and self-regulatory ~~rules~~ provisions that ~~can~~ affect the processing of personal data in the electoral context in each country.

~~7.2.~~

Elections regulators, in particular, have the long-standing expertise in elections law and the experience in administering the many facets of elections administration, including the distribution of voters lists. ~~However, the regulation of personal data processing in the electoral context cannot be left to elections regulators alone.~~

5.1.

~~7.4.~~5.2. Supervisory authorities should offer their expertise to strengthen the capacity of election and other regulators to identify and address data protection issues in the electoral and political campaign contexts.

~~7.5.~~5.3. Recent proposals in different countries requiring transparency of the sources and financing of political ads, including digital archiving of ad imprints, offer opportunities for regulators better to understand the nature of political micro-targeting in their respective societies, the level of granularity, and the source(s) of payment for the ads. In the world of political campaigning, data protection infractions can also be elections financing infractions, and vice versa. Ad transparency requirements provide an important source of leverage for supervisory authorities in enforcing data protection requirements.

~~7.6.~~5.4. Proactive guidance on best campaigning practices is of critical importance. The risks to fundamental rights from the processing of personal data in election campaigns cannot simply be understood in response to individual complaints to particular candidates and/or political parties at the time of elections.

~~7.7.~~5.5. Supervisory authorities can also assist political parties. 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. Supervisory authorities should therefore work with political parties, and their data processors, to develop tailored guidance in the form of codes of practice.

~~7.8.~~5.6. The implementation of these Guidelines requires the highest level of global collaboration between supervisory authorities. The political "influence industry" knows no geographic boundaries. Its impact nationally and internationally will require the most vigilant and constant cross-national attention from supervisory authorities through their international and regional associations, as well as from the wider network of international privacy advocates and experts (Article 17).

[28] Explanatory report, para. 87.