COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 19 November 2021

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

CONVENTION 108

Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns

Contents

1. Introduction

Effective political communication through political campaigning 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.

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 hidden practices that permit the manipulation of data on the electorate, for the delivery of such focussed messages. Political micro-targeting is not only about political engagement, it can also lead to 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 organisations involved in political campaigns process personal data on voters in compliance with well-established data protection principles. Familiar data protection questions are now at the centre 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, international 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 Automatic Processing of Personal Data as amended by the Protocol CETS No 223 (Convention 108+),[1] assume an increasing importance in the regulation of data-driven elections, and in the support of the broad democratic principles of pluralism and individual autonomy. The application of sound data protection principles contributes to strengthening the integrity of elections and maintaining trust in democracy in the digital age.

Convention 108+, as noted in its Preamble, 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]

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."

The principles of free expression and robust public debate in both offline and online media, are 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 expression protected by the ECHR.

---

[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.

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 organisations.

In many countries in Europe and elsewhere, data protection law applies, and has always applied, to the personal data processed by the organisations 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. As a result of these developments in digital campaigning practices, some supervisory authorities have recently investigated the larger systemic issues and tried to reconcile the privacy rights of the voter and the democratic obligations of political campaigns to communicate with the electorate.

The aim of these Guidelines is to provide practical advice to supervisory authorities, regulators and to political organisations 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 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 political campaign organisations recognizing the increasing use of digital campaigning strategies via social media and the increasing sophistication of voter analytics.

2.2. Political campaign organisations refer to political parties, electoral coalitions as well as more temporary organisations constituted during election or referendum campaigns.

2.3. Political campaigns not only refer to "election campaigns." Political campaign organisations 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 processing of personal data by political campaigns apply to the relatively brief period during which legislatures are dissolved and formal election campaigning occurs, as well as to the periods between elections.

[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 No. 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

2.4. Political campaign organisations collect a variety of personal data on voters that may include: basic contact information from a national or local list of electors provided by the election regulatory body (where authorized by law); on donations and financial contributions; and on voters' attitudes, affiliations and intentions. They also process personal data on campaign employees and volunteers; and on candidates or potential candidates.

2.5. These guidelines 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, all of which have a different relationship with the political campaign organisations and raise very different data protection issues.

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

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

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

2.9. These Guidelines recognise that the processing of personal data on voters is influenced by cultural factors and historical legacies: the overall 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).

2.10. These Guidelines recognise 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 weakening of election integrity.

2.11. 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, alone or in cooperation with national election authorities, sensitive to their domestic political systems, and consistent with their responsibilities under Article 15 of Convention 108+.

2.12. 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, on profiling and on Big Data, for instance, should be followed to ensure that applications do not undermine the human dignity, the human rights and the fundamental freedoms of voters either as individuals, or as communities.[6]

[6] Council of Europe, Guidelines on Artificial Intelligence and Data Protection T-PD (2019)01 (Strasbourg, 25 January

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 an organized set of organisational and communicative activities carried out by campaign organisations 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 organisation" is any organisation 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[7]'.

3.4. Personal data revealing "political opinions" are a special category of data under Article 6 of the Convention and may refer to: personal data revealing adherence to, or rejection of, 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 any form of communication including: 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 organisations established on a temporary basis to support or oppose a referendum question; and other organisations (such as electoral coalitions) when they alone or jointly with others have decision-making power with respect to personal data 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.

3.8. "Election regulatory bodies" are those national authorities responsible for the regulation of the safe and efficient conduct of elections, the implementation of election finance provisions and (where applicable) the development and management of the national voter list.

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. "Profiling" refers to any form of automated processing of personal data, including use of machine learning systems, consisting in the use of data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[8]

2019); Council of Europe, Recommendation CM/Rec(2021)8 of the Committee of Ministers to members states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (November 3, 2021); 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)

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

[8] Council of Europe, Recommendation CM/Rec(2021)8 of the Committee of Ministers to members states on the

3.11. A “profile” refers to a set of data attributed to an individual, characterising a category of individuals or intended to be applied to an individual.[9] A “voter profile” is the result of applying profiling techniques to voters or prospective voters, in particular to analyse or predict that person's political opinions and his/her likelihood to vote for one party or another.

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

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

4.1.1. 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 minimization, accuracy and security. Personal data on political opinions is further protected by Article 6. Processing should be proportionate in relation to the legitimate purposes of political campaigns, reflecting the rights and freedoms at stake. The collection 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.

4.1.2. The legitimate purpose of political campaigning is engagement with the electorate which might be achieved through the following means: canvassing political opinions; communicating about policies, events and opportunities for engagement; fundraising; conducting surveys and petitions; communication on political goals and policies via social media, email and text; engaging in “get-out-the-vote” operations on election day. These purposes and means should be stated as precisely and fully as possible in campaign publicity materials. Further processing should be compatible with this stated purpose, under Article 5(4)b.

4.1.3. In the sensitive context of political campaigning personal data on voters’ political opinions should not be used for other purposes, and should not be further used for “undefined, imprecise or vague purposes.”[10] For instance, these data should not be used to determine governmental appointments, or to reward supporters with policy benefits.

4.1.4. Within every context that political campaigning organisations engage with voters – on the doorstep, over the telephone, via email or text, or via social media – a legal basis for the processing of personal data is required.

4.1.5. Where the legitimate basis for processing is consent (Article 5(2)), the processing of personal data in the political campaigning context 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.”[11] The voter may withdraw his or her consent to process personal data at any time.[12]

protection of individuals with regard to automatic processing of personal data in the context of profiling (November 3, 2021) para 1(c) at: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a46147

[9] Ibid, para 1(d)

[10] Explanatory report, para 48.

[11] Explanatory report, para 42.

[12] Explanatory report, para. 45.

4.1.6. Where the political campaigning organisation relies on a "legitimate basis laid down by law" (Article 5(2)), those legitimate grounds should be stated, and its legal basis accurately referenced in the privacy policy of the organisation. For example, political campaigning organisations 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."[13] Where the public interest in democratic engagement is claimed as a legitimate basis for processing, those interests should be clearly stated by law and duly referenced in the privacy policy. The processing carried out on the basis of an "overriding legitimate interest of the controller or the third party" should not conflict with the rights and interests of the data subjects, taking into account their reasonable expectations.

4.1.7. In states where those under the age of 18 may legally vote, political campaigning organisations should take special care to protect the personal data of young people according to Article 15(e).[14]

4.1.8. Where political campaign organisations legally acquire the official voters list from the election regulatory body to assist their campaigns, the law should stipulate who is entitled to access these data, and for what purposes, limited to what is necessary for engaging with the electorate with clear prohibitions and appropriate sanctions for using the data for any other purposes.

4.1.9. Unless specifically approved by law, 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.

4.1.10. No undue influence or pressure should be exerted on a voter or potential voter to provide personal data by any political campaign organisation.[15]

4.1.11. When campaigning in person on the doorstep, campaigners should ensure that they are collecting and using personal data in compliance with relevant legislation. Campaigners should be transparent about the purposes for which they are collecting personal data, and only collect the data strictly necessary for these purposes. 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 about other family members (especially children), tenants or residents. They should not be collecting information on the household or its possessions (such as cars or other objects) for purposes of drawing inferences about political preferences or interests. There are risks associated with profiling an entire household based on selective observation and information collection.

4.1.12. Political campaign organisations 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.

4.1.13. Political campaign organisations often obtain personal data from third party organisations such as data brokers, for election or campaigning purposes to target messages to a particular audience. Data on political opinions might also be inferred from the analysis of personal data from a variety of sources, and which relate to behaviour and activities that may be unrelated to politics. Before using the data from data brokers, campaigns should carry out full due diligence to ensure the data has been obtained lawfully and inform data subjects in accordance with Article 8, including the legal basis and the purposes of the intended processing.

[13] Explanatory report, para 46

[14] Explanatory report, para. 125.

[15] Explanatory report, para. 42.

4.1.14. Political campaign organisations should ensure that personal data is accurate, and where necessary kept up-to-date.

4.1.15. Personal data on voters should not be further processed in a way that the voter might consider "unexpected, inappropriate or otherwise objectionable."[16] Furthermore, the political organisation should not be transferring those data to other organisations, for instance, with presumed similar political goals or ideological perspectives, without having a legal basis or obtaining the express consent of the voter.

4.1.16. 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 organisation 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 example, for individuals who may be within the wider social network of that voter, and who have not affirmatively expressed a preference to be contacted.

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

4.2.1. 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."[17] Therefore, political organisations may process personal data in each of these special categories, provided that appropriate safeguards have been put in place.

4.2.2. In the context of political campaigning "information they reveal relating to (…) political opinions" is especially relevant. 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.

4.2.3. Political parties and other organisations 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 organisations often profile or "score" voters on the basis of these data. These are all personal data falling within the special categories of data under Convention 108+.

4.2.4. The processing of personal data revealing political opinions entails severe risks of voter discrimination, leading to voter suppression and intimidation. The knowledge of who has, and has not, supported a governing party can also affect the provision of government services. The processing of special categories of personal data needs to be accompanied by safeguards appropriate to the risks at stake of voter discrimination and of the interests, rights and freedoms protected

[16] Explanatory report, para. 49.
[17] Convention 108+, Article 6

4.2.5. If political parties and other campaigning organisations are relying on the lawful basis of consent to collect data on political opinions and to send political messaging through electronic or paper communications, they should ensure that they have the appropriate records of consent from the individual. Procedures for recording the withdrawal of consent should also be established.

4.2.6. The analysis, sorting and profiling of groups of voters on geographical and/or demographic factors, can have discriminatory effects[18] 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.

4.2.7. Controllers and processors shall not disclose voters' sensitive personal data collected in the course of a political campaign, for others (such as data brokers) to monetize, or otherwise reprocess for the purposes of selling anonymized or de-identified data.

4.2.8. 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 be deployed according to an appropriate legal basis. Services should only allow activation with the opt-in of the individual user. Geo-location, as well as other mechanisms for the tracking of location, should not be available by default.

4.2.9. If political campaign organisations 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), then both entities assume joint controllership of the personal data. No personal data shall be shared with social media companies for the purposes of digital advertising without appropriate notification to the data subjects. Data subjects should be informed about their right to object to data processing for marketing purposes which should lead to unconditional erasure or removal of the personal data covered by the objection.

4.3. Data security in political campaigns (Article 7)

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 organisations should take appropriate security measures to ensure against accidental or unauthorized access to, destruction, loss, use, modification or disclosure of personal data. These measures should be introduced with due regard to the specificities of the medium (mobile phone, computer, IOT, email, chat, etc.) used, and include: training in privacy and security; access controls; confidentiality agreements; and controls on physical access to places and equipment where personal data are stored.

4.3.2. Political campaign organisations should report to supervisory authorities as prescribed by Convention 108+ and to the data subjects themselves in the event of data breaches which may seriously interfere with the rights and fundamental freedoms of voters in accordance with Article 7(2) of the Convention. Notification should include adequate and meaningful information about possible measures to mitigate the adverse effects of the breach.[19]

[18] 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)
[19] Explanatory report, para 66.

4.3.3. Political campaign organisations 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.[20]

4.3.4. Where data is processed by third party service providers, political organisations 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 10 of the Convention.

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

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

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

4.4.1. The personal data processed by political organisations shall be processed fairly and in a transparent manner, especially taking into account the potential for the manipulation of voters.

4.4.2. At the time of collection, political campaign organisations should inform voters (in a privacy policy or its equivalent) of at least: the legal name and address of the organisation; the legal basis for collection of personal data for 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. Regardless of the method of communication, representatives of political campaign organisations shall inform voters that they are collecting data "on behalf of X party/organisation."

4.4.3. Privacy policies should be easily accessible, legible, understandable and adapted to the relevant individuals.[21] 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.

4.4.4. In any communication from a political campaign, the volunteer or employee should 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.

[20] Explanatory report, para 63.

[21] Explanatory report, para. 12.

4.4.5. In the context of digital advertising, political campaign organisations 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."

4.4.6. Publicly available 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 expressed in Article 8.

4.5. The Rights of Data Subjects (Article 9)

4.5.1. 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.

4.5.2. 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 campaign organisations, this should include any "score" assigned to the voter which measures his/her ideological orientation.

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

4.5.4. Data subjects should be able to object to the processing of data on him or her with a political organisation, and to request rectification or erasure as the case may be, if the data is inaccurate, obsolete or incomplete.[22]

4.5.5. 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.[23]

4.5.6. Data subjects are, upon request under Article 9(1)(b and c), entitled to be informed 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.

4.5.7. Data subjects are entitled to remedy if their rights under the Convention are violated by political campaign organisations.

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

[22] Explanatory report, para. 72.
[23] Explanatory report, para 79.

4.6. Additional Obligations of Political Campaigns (Article 10)

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 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+.

4.6.2. Political parties and other campaigning organisations 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.

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

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 whether the processing is in the best interests of broader democratic values and the integrity of democratic elections.

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

4.6.6. Political parties and other campaigning organisations should appoint an officer responsible for the verification and demonstration of compliance with the data protection principles enshrined within Convention 108+.[24]

[24] Explanatory report, para. 87.

5. Recommendations for Supervisory Authorities (Article 15)

5.1. Without prejudice to their powers and tasks in respect of the processing of personal data according to Article 15 of Convention 108+, supervisory authorities should cooperate with each other and 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 provisions that affect the processing of personal data in the electoral context in each country. Election's 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.

5.2. Legislative Assemblies may wish to set out regulatory frameworks for the processing of personal data by political campaign organisations in their specific national contexts.

5.3. 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.

5.4. Recent proposals in different countries requiring transparency of the sources and financing of political ads, including digital archiving of ad imprints, offer opportunities for supervisory authorities 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. Ad transparency requirements provide an important source of leverage for supervisory authorities in enforcing data protection requirements.

5.5. 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.

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

5.7. While the implementation of these Guidelines will be shaped by local political contexts, it may also require collaboration between supervisory authorities. The global industry that supports digital campaigning knows no geographic boundaries. Then impact of this industry 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).