



Strasbourg 15 November / novembre 2021

T-PD(2021)3rev3Mos

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

**COMITÉ CONSULTATIF DE LA CONVENTION
POUR LA PROTECTION DES PERSONNES
À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL**

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

**Compilation des commentaires sur le Projet des Lignes directrices relatives à la protection des
personnes à l'égard du traitement des données à caractère personnel dans le cadre des campagnes
politiques**

TABLE OF CONTENT / TABLE DES MATIERES

BULGARIA / BULGARIE	3
EUROPEAN UNION – EUROPEAN COMMISSION / UNION EUROPEENNE – COMMISSION EUROPEENNE	5
GERMANY / ALLEMAGNE	9
ITALY / ITALIE	16
MEXICO.....	18
URUGUAY	20

BULGARIA / BULGARIE

2. Scope and Purpose

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

Commented [A1]: National laws in some Eastern European countries stipulate formal opportunity for election coalitions both for election and referendum campaigns.

~~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 of 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 including joint opinions with relevant election authorities, consistent with their responsibilities under Article 15 of Convention 108+. ~~such as those developed by the Information Commissioner in the UK.~~⁴

Formatted: Font: (Default) Arial, Highlight

3. Definitions for the purposes of the Guidelines

3.6. “Data controllers in political campaigns” include: political parties; official candidates of political parties; campaign organizations established on a temporary basis to support or oppose a referendum question; and other organizations (such as election coalitions) 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+.

Formatted: Font: (Default) Arial, Highlight

~~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.~~

Commented [A2]: In order to achieve clarity we would suggest to exchange “administrators” with “institutions” or “authorities”

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.

~~3.10.~~ 3.11. “Mass media” process personal data lawfully for the purpose of implementing freedom of expression and the right to information while simultaneously respecting privacy.

Formatted: Font: (Default) Arial, Highlight

⁴ Information Commissioner's Office, Guidance on Political Campaigning: Draft Framework Code for Consultation 06-2019) at: <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>

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

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

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.

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 or other belongings) for purposes of drawing inferences about political preferences or interests.

Commented [A3]: We would suggest to exchange "including" with "especially"

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

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. Furthermore, mechanisms for taking into account of the withdrawal of the consent should be established.

Formatted: Font: (Default) Arial, Highlight

Formatted: Font: (Default) Arial, 11 pt, Highlight

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 activation with the opt-in of the individual user. Geo-location as well as other methods of automated means should not be available by default.

Formatted: Font: (Default) Arial, Highlight

EUROPEAN UNION – EUROPEAN COMMISSION / UNION EUROPEENNE – COMMISSION EUROPEENNE

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.

(...)

Commented [A4]: Suggest rephrasing to avoid confusion with public interest grounds for processing – later on, in section 4.1.4 you mention consent as preferred ground for lawfulness.

3. Definitions for the purposes of the Guidelines

(...)

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.

Commented [A5]: By this definition, “Profiling” refers to any form of automated processing of personal data [...] to evaluate certain personal aspects relating to an individual” - this is a very broad definition (it would catch any computerized processing that applies simple rules such as “if older than 65 years, we assume they're interested in our policy on pensions, so lead with messaging on pension, if under 25, [...] lead with messaging on education”. Is that really the intention?

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

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

~~4.1.4. Where the legitimate basis for processing is based on consent, 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.”² The voter may withdraw his or her consent to process personal data at any time.³

Commented [A6]: When a legal basis can be validly used, there is no hierarchy between them – yes, many things will require consent, but where there are other grounds available (such as in the case of 4.1.6 below), it is not clear why consent should be privileged.

Commented [A7]: How does this fit with section 4.1.6 below, which is not consent-based?

² Explanatory report, para 42.

³ Explanatory report, para. 45.

(...)

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 obain line with they 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.~~

Commented [A8]: It is fair to assume that "only use for communication with the electorate" is a condition under that law, but the permissible purposes are for those laws to lay down.

~~4.1.6-4.1.7. 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.~~

Commented [A9]: Assume this would also cover consent (as one of the legal bases), not just laws explicitly allowing campaigns to do this (with certain safeguards), correct?

(...)

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 ~~other~~ information on the household or its possessions ~~(such as cars)~~ for purposes of drawing inferences about political preferences or interests.

(...)

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."⁴ 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.~~

Commented [A10]: This paragraph seems to conflate the "non-consent" bases referred to in 5(2) CoE 108+ in general with the specific legal bases of "necessary for task in the public interest assigned by law" and "legitimate interest of controller" legal 6(1)(e) and (f) GDPR (... or similar provisions in non EU/EEA jurisdictions).

In the 6(1)(f) GDPR case, the interest is not "stated by law" in the sense of "Law X assigns task Y to entity Z, which requires the processing of personal data categories A, B, C for purpose D" (but it is for the controller to explain its legitimate interests). The "stated by law" element is only there for 6(1)(e).

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

(...)

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.

Commented [A11]: Why this scope limitation here? Would this not apply to consent-based paper communications as well?

⁴ Explanatory report, para 46

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.⁵

Commented [A12]: What do you intend to cover here?
The information "Dentists are more likely to vote for party X compared to the general population" on its own is not personal data (but the underlying processing that lead to this may very well have been).

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.

However, "This dentist is likely to vote for party X" is personal data about that natural person, also if that information is not used for communicating with that person, yes.

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 be deployed when necessary and according to an appropriate legal basis. Services should only allow activation with the opt-in of the individual user. Geo-location should not be available by default.

This is the same issue as in the profiling GLs – the abstract profile ("people with characteristics X often do Y") is not personal data, while attaching this label to a specific person ("this person has characteristics X, so we assume they're likely to do Y") is.

Commented [A13]: If properly anonymized, the data is out of the scope of data protection rules

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.

Commented [A14]: Not clear who the addressee of this statement is; would suggest dropping (where local laws require opt-in, the sentence before already makes that point).

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

(...)

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.

Commented [A15]: As phrased, this statement is about all targeting, not just for political ads. Do you intend to make this such a general statement?

Commented [A16]: Is this transparency in the data protection sense of "how am I targeted?" or rather about "how are people in general targeted and with what"?

⁵ Council of Europe, The Protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/REC (2010) 13 (November 23, 2010)

4.5. The Rights of Data Subjects (Article 9)

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.~~

(...)

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.

Commented [A17]: 1) Why is this only targeted to political parties (see 4.2.3 above, where you discuss scoring in relation to "political organisations")?
2) Linked to the paragraph above: do you consider that any such score "significantly affects" the DS?

Commented [A18]: This wording is often used in connection with profiling, but here, this is addressed for all processing of personal data – What does this add here to the general information obligations of the controller?

4.6. Additional Obligations of Political Campaigns (Article 10)

(...)

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.

Commented [A19]: Is a DPIA the right place to address these questions beyond "is what we intend to do legal?"

5. Recommendations for Supervisory Authorities (Article 15)

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.~~

Commented [A20]: What do you mean here? Disclosing sources of funding is not a data protection requirement.

Commented [A21]: Not clear how financing transparency would contribute here, please be more specific in case you refer to ad archives here.

GERMANY / ALLEMAGNE

1. Introduction

(...)

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 lead to permit voter suppression, and the discouragement of voters from exercising their democratic rights.

Commented [A22]: Isn't that a different/separate issue? Isn't micro-targeting more about targeting than manipulating the data on voters?

(...)

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 the processing of personal data as amended by the Protocol CETS No 223 (Convention 108+),⁶ 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. ~~These Guidelines recognize that the~~ The application of sound data protection principles contribute to the strengthening the integrity of elections can go a long way to addressing broader issues of election integrity and restoring maintain trust in democratic processes in the digital age.

Commented [A23]: We still suggest “maintain” and object to “restoring” as it applies that all trust has been lost.

(...)

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. As a result of these developments in digital campaigning practices, some supervisory authorities have recently investigated the larger systemic issues. Only relatively recently, however, have supervisory authorities grappled with the tricky questions of how and tried to to reconcile the privacy rights of the voter and the democratic obligations of political campaigns to communicate with the electorate.

Commented [A24]: Reference?

⁶ 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. Scope and Purpose

(...)

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, as well as to the periods between elections.

Commented [A25]: This would broaden the scope a lot.

(...)

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

Commented [A26]: In Germany for example, the relevant law is the party financing law

2.8.

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 organizational and communicative activities carried out by political campaign organizations ~~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.

Commented [A27]: The new definitions is a tautology – defining political campaigns with activities by an political campaign organization. We suggest returning to the old definition.

(...)

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 the support or rejection to a ~~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.

Commented [A28]: We still suggest that wording as someone might reject a political ideology without adhering to another and this could still be considered data protected by Article 6

(...)

3.6. “Data controllers in political campaigns” include: political parties; official candidates of political parties; campaign organizations established on a temporary basis to support ~~or~~

oppose a referendum question; and other organizations (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.

(...)

- 3.10. "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.⁷ Profiling means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.⁸ A "voter profile" is the result of applying these same techniques to voters or prospective voters, 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.

Commented [A29]: We still maintain that this should be in another section. Art. 2 (d) Conv. 108+ defines who is a controller. When applying the Convention in the context political campaigns some guidance on who is the controller in what particular context might be useful.

Commented [A30]: See comment above

Commented [A31]: The new Recommendation has been adopted on 3 November 2021.

4. The Application of Convention 108+ to Political Campaigns

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

- 4.1.2. The legitimate purposes of a political campaigning ~~is engagement with the electorate which might be achieved through the following means~~ include: canvassing political opinions; communicating about policies, events and opportunities for engagement; fundraising; conducting surveys and petitions; ~~advertising communication on the political goals~~ 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 these~~ ~~fixed to these~~ stated purposes, ~~under Article 5(4)b.~~

(...)

- 4.1.4. ~~Unless~~ not otherwise authorized by law, ~~The free, specific, informed and unambiguous~~

Commented [A32]: Germany welcomes that part of our comment has been taken into account here. However, this seems to be a very broad purpose

Commented [A33]: The current wording would allow for advertising that has no direct context to the political engagement with the voters and might only have commercial/financial reasons

⁷ Council of Europe, Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling

⁸ 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 – Section 1(e), p. 9

~~consent of the data subject is the preferred legal basis for the processing of personal data in the political campaigning context should shall be based on the free, informed and unambiguous consent of the data subject. Consent should be obtained W~~within every context that political campaigns engage with voters – on the doorstep, over the telephone, via email or text, or via social media a legal basis for the data processing is needed. Consent should not be inferred through “silence, inactivity or pre-validated forms or boxes.”⁹ The voter may withdraw his or her consent to process personal data at any time.¹⁰

Commented [A34]: If it is not authorized by a law, the only other legal basis is consent.

4.1.6. 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).¹¹

~~4.1.6.~~
~~4.1.7.~~

~~In circumstancesWhere where~~ political campaign organizations ~~e~~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. the campaigns must only use these 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.

Commented [A35]:

4.1.10. ~~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 capturingcollecting 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.~~

⁹ Explanatory report, para

¹⁰ Explanatory report, para. 45.

¹¹ Explanatory report, para. 125.

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

4.2.1. ~~Under~~ According to Article 6 (1) 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:~~ According to Article 6 (2) “Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.”¹² Therefore, Ppolitical organizations may process personal data in each of these special categories, provided that appropriate safeguards have been put in place. This is without prejudice to general data protection requirements such as the existence of a legal basis.

Formatted: Font: (Default) Arial, Highlight

Formatted: Font: (Default) Arial, Highlight

Commented [A36]: We propose the slight rewording to clarify the structure of Article 6 and its consequences, as well as the addition.

4.2.2. ~~In particular, Article 6(1) of Convention 108+ defines special categories in terms of the~~ In the context of political campaigning “information they reveal relating to ...political opinions-” ~~is particularly 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 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 personal data falling within the special sensitive categories of data under Convention 108+.

Commented [A37]: as an alternative it might read: “..are all special category data...”?

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 ~~sensitive 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

Commented [A38]: Wording of the Convention

Commented [A39]: This remains unclear: The conditions for legitimate processing are already set out in *the Convention*: Personal data should be processed lawfully, fairly and in a transparent manner. Personal data must also have been collected for explicit, specified and legitimate purposes, and the processing of that particular data must serve those purposes, or at least not be incompatible with them. (see also ER 48)

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

Commented [A40]: The still propose the deletion: Further processing is prohibited when it is not compatible but not in general by the Convention. Instead of this paragraph, examples could be given to illustrate what should be deemed compatible or incompatible.

(...)

~~4.2.11. 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, (for example to data brokers) without the express consent of the voter.~~

The Convention does not know the prohibition of “selling” data unlike e.g. the California Consumer Privacy Act. So this seems a bit problematic.

Furthermore, it should be taken into account that once the data has been anonymized, data protection law does not apply anymore.

¹² Convention 108+, Article 6

(...)

4.2.10. ~~If p~~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), 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 legal basis and a notification to the data subjects~~the express consent of the voter.~~ In particular, data subjects shall be informed about their right to object to data processing for marketing purposes which should lead to unconditional erasing or removing of the personal data covered by the objection.

Commented [A41]: We propose to add the last sentence.

Indeed, according to Convention 108+ personal data can be transferred for marketing purposes without the consent of the data subject.

However, there should be at least a reference made to Recital 79 of the explanatory report of Convention 108+.

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

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.


Commented [A42]: We still propose "publicly available" as only those would add significantly to the transparency principle.

4.5. The Rights of Data Subjects (Article 9)

~~4.5.6.~~ Data subjects are ~~- upon request (Art. 9 (1) lit. b and c. -~~ entitled to be informed about 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.

Commented [A43]: Art. 8 does not cover these categories, however, Article 9 does, but only upon request of the data subject.

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. 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 voter  lists.

5.5. Supervisory authorities can also assist political parties within the scope of their respective 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.

Commented [A44]: Political parties have no competency regarding the DPAs competencies

5.6. ~~While t~~The implementation of these Guidelines will be shaped by local political contexts, it also may require ~~the highest level of global~~ collaboration between supervisory authorities.

Formatted: Font: (Default) Arial, Not Highlight

The ~~global industry that supports digital campaigning political~~ “influence industry” knows no geographic boundaries. ~~The impact of this industry 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).

ITALY / ITALIE

1. Scope and Purpose

- 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; 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).

Commented [A45]: Who are we trying to exclude?

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

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

4.1.10. Political campaigns organisations 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.

4.1.11. Political campaigns organisations 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.

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."¹³ 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.

Commented [A46]: Accurately and clearly is maybe repetitive

¹³ Explanatory report, para 46

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

- 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.

Commented [A47]: Legitimately this section refers to one specific category of sensitive data, namely those revealing political opinions, but there may be other data, for example related to health or ethnic origin that may be processed to better target political marketing. Should we consider these categories as well?

Commented [A48]: Are we sure that we want to say that with the express consent data could be sold?

MEXICO

1. Introduction

(...)

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, but it can also permit voter suppression, and the discouragement of voters from exercising their democratic rights.](#)

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

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.¹⁴

4.3. Data security in political campaigns (Article 7)

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 [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.¹⁵

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+, sSupervisory authorities should cooperate with](#)

¹⁴ Council of Europe, The Protection of individuals with regard to automatic processing of personal data in the context of [profiling](#) profiling. Recommendation CM/REC (2010) 13 (November 23, 2010)

¹⁵ Explanatory report, para 66.

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 ~~rules~~ provisions that can affect the processing of personal data in the electoral context in each country.

- 5.5. Supervisory authorities can also assist political parties within the scope of their respective 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.

URUGUAY

4. L'application de la Convention 108+ aux campagnes politiques et aux organisations de campagne

4.1. Légitimité du traitement des données et qualité des données (article 5)

4.1.1. Le traitement des données à caractère personnel des électeurs (en particulier celles qui révèlent des opinions politiques sensibles) devrait être proportionné au regard des finalités légitimes des campagnes politiques. La collecte de données à caractère personnel sur les opinions et les préférences des électeurs devrait être proportionnée au regard de ces finalités et ne devrait pas entraîner d'ingérence indue dans les intérêts, les droits et les libertés des électeurs.

4.1.9. Quand les membres d'une organisation de campagne font du porte à porte, ils doivent faire preuve de transparence sur le but dans lequel ils collectent des données personnelles. Ils ne devraient pas enregistrer d'informations sur le foyer et ses occupants autres que celles que les électeurs communiquent librement et spécifiquement sur leurs opinions et/ou préférences politiques. Ils ne devraient pas poser de questions sur les autres membres de la famille (y compris sur les enfants), des locataires ou d'autres résidents, ni recueillir d'informations sur le ménage ou ses biens (comme des voitures) dans le but d'en tirer des déductions sur les préférences ou les intérêts politiques.

4.1.15. Les organisations de campagne politique ne ~~devraient~~ doivent pas « récupérer » des données sur les médias sociaux aux fins d'établir des profils de l'électorat. Si un électeur est adhérent d'une organisation ou a positivement exprimé le souhait de suivre tel candidat ou tel parti sur une plateforme de média social, alors l'organisation peut raisonnablement en déduire que cette personne est disposée à recevoir d'autres communications du candidat ou du parti en question. Mais elle ne doit pas partir du principe qu'il en va de même pour les personnes qui peuvent faire partie du réseau social élargi de cet électeur et qui n'ont pas manifesté positivement leur souhait d'être contactés.

4.2. Traitement de la catégorie particulière de données relative aux opinions politiques (article 6)

4.2.10. Les organisations de campagne politique communiquent des données personnelles à des entreprises de médias sociaux en vue d'adresser des publicités numériques à des groupes de personnes dont les idées sont proches (à l'aide d'outils comme ~~les audiences similaires ou personnalisées de Facebook~~ Lookalike Customized Audience). Aucune donnée à

Commented [A49]: Dans quelques pays le vote est secret, plus la considération d'être une donnée sensible, alors c'est très important d'avoir le consentement de l'électeur pour le traitement. Le point 4.1.4 devrait être en premier lieu.

Commented [A50]: Si le consentement libre, spécifique, éclairé et non-équivoque de la personne concernée est la base légale privilégiée pour le traitement de données personnelles dans le contexte des campagnes politiques, les médias sociaux ne peuvent pas être une source pour cette information.

caractère personnel ne doit être communiquée ~~aux~~ des entreprises de médias sociaux dans un but de publicité numérique sans le consentement express des électeurs.

Commented [A51]: En tout cas, si c'est le résultat d'une enquête, les données personnelles devraient être anonymes ou que les législations établissent un secret de l'information statistique.