Council of the
European Union

Brussels, 13 September 2018
(OR. en)

12130/18

DATAPROTECT 179
FREMP 141
JAI 880
DIGIT 172

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	12 September 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2018) 638 final
Subject:	GUIDANCE DOCUMENT Commission guidance on the application of Union data protection law in the electoral context *A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018*

Delegations will find attached document COM(2018) 638 final.

Encl.: COM(2018) 638 final

EUROPEAN
COMMISSION

Brussels, 12.9.2018
COM(2018) 638 final

Free and Fair elections

GUIDANCE DOCUMENT

Commission guidance on the application of Union data protection law in the electoral context

A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018

COMMISSION GUIDANCE ON THE APPLICATION OF UNION DATA PROTECTION LAW IN THE ELECTORAL CONTEXT

Engagement with the electorate is the basis of the democratic process. It is a constant practice for political parties to tailor electoral communication to audiences, taking into account their specific interests. It is therefore natural for actors involved in elections to explore the possibilities to use data in order to win votes. The rise of the digital tools and online platforms have created many new opportunities to engage with people in political debate.

However, the development of micro-targeting of voters based on the unlawful processing of personal data as witnessed in the case of the Cambridge Analytica revelations is of a different nature. It illustrates the challenges posed by modern technologies, but also it demonstrates the particular importance of data protection in the electoral context. It has become a key issue not only for individuals but also for the functioning of our democracies because it constitutes a serious threat to a fair, democratic electoral process and has the potential to undermine open debate, fairness and transparency which are essential in a democracy. The Commission considers that it is of utmost importance to address this issue to restore public trust in the fairness of the electoral process.

The first reports from the UK data protection authority (Information Commissioner's Office – ICO) on the use of data analytics in political campaigns[1] and the Opinion of the European Data Protection Supervisor on online manipulation and personal data[2] have confirmed the growing impact of micro-targeting, initially developed for commercial purposes, in the electoral context.

More generally, several data protection authorities have addressed the issue of data protection in the electoral context[3].

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)[4], which became directly applicable across the Union on 25 May 2018, provides the Union with the tools necessary to address instances of unlawful use of personal data in the electoral context. However, only a firm and consistent application of the rules will

[1] Reports from the UK data protection authorities (Information Commissioner's Office – ICO) of 10 July 2018: "Investigation into the use of data analytics in political campaigns – Investigation update" and "Democracy Disrupted? Personal information and political influence".

[2] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[3] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267 "Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" published in the Official Gazette of the Italian Data Protection Authority number 71 on 26.03.2014 [doc. web n. 3013267]; https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux "Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?" published by the Commission Nationale de l'informatique et des libertés (French National Commission of Informatics and Liberty) 08.11.2016 ; https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office 'Guidance on political campaigning' [20170426].

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

help to protect the integrity of democratic politics. Since it is the first time they will be applied in the European electoral context on the occasion of the forthcoming elections to the European Parliament, it is important to provide clarity to the actors involved in election processes – such as national electoral authorities, political parties, data brokers and analysts, social media platforms and online ad networks. The objective of this guidance is therefore to highlight the data protection obligations of relevance for elections. The national data protection authorities, as enforcers of the General Data Protection Regulation, have to make full use of their strengthened powers to address possible infringements, in particular those relating to the micro-targeting of voters.

1. The Union data protection framework

The protection of personal data is a fundamental right enshrined in the Charter of Fundamental Rights of the European Union (Article 8) and in the Treaties (Article 16 TFEU). The General Data Protection Regulation strengthens the data protection framework, making the Union better equipped to deal with cases of personal data abuse in the future and all actors more accountable and more responsible in how they deal with personal data.

It gives individuals in the Union additional and stronger rights which are particularly relevant in the electoral context. The data protection regime that was in place in the Union for the previous 20 years suffered in particular from the fragmented application of the rules between Member States, the absence of any formalised mechanisms for cooperation between national data protection authorities and the limited enforcement powers of those authorities. The General Data Protection Regulation addresses those shortcomings: building on the proven principles of data protection, it harmonises key notions such as consent, strengthens individuals' rights to receive information about the processing of their data, clarifies the conditions under which personal data can be further shared, introduces rules on personal data breaches, establishes a cooperation mechanism between data protection authorities in cross-border cases and strengthens their enforcement powers. In case of infringement of EU data protection rules, data protection authorities have the powers to investigate (by, for instance, ordering to provide information, carrying out inspections at the premises of controllers and processors) and to correct behaviour (by, for instance, issuing warnings and reprimands, or impose a temporary or definitive suspension of the processing). They also have the power to impose fines up to EUR 20 million or, in the case of a company, up to 4% of its worldwide turnover[5]. When deciding on imposing fines and their level, the data protection authorities will consider the circumstances of the individual case and factors such as the nature, scope or purpose of the processing, the number of persons affected and the level of damage suffered by them[6]. In the electoral context, it is probable that the gravity of the infringement and the number of persons affected will be high. This might lead to the imposition of high level fines, in particular considering the importance of the issue of citizens' trust for the democratic process.

[5] Commission guidance on the General Data Protection Regulation at: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
[6] Article 83 General Data Protection Regulation.

The newly established European Data Protection Board, which groups all national data protection authorities, as well as the European Data Protection Supervisor, plays a key role in the application of the General Data Protection Regulation by issuing guidelines, recommendations and best practices[7]. As enforcers of the General Data Protection Regulation and direct contacts for stakeholders, national data protection authorities are well placed to provide additional legal certainty regarding its interpretation. The Commission actively supports that work.

The Directive on privacy and electronic communications, or 'e-Privacy Directive' (Directive 2002/58/EC of the European Parliament and of the Council[8]), completes the Union data protection framework, and is relevant in the electoral context as its scope includes rules on the electronic sending of unsolicited communications, including for the purposes of direct marketing. The e-Privacy directive also lays down rules on the storing of information and gaining access to information already stored, such as cookies that may be used to track a user's online behaviour, in terminal equipment, such as a smartphone or computer. The Commission's proposal for a Regulation on Privacy and Electronic Communications, ('e-Privacy Regulation')[9], currently under negotiation, is based on the same principles as the e-Privacy Directive. The new Regulation will widen its scope beyond traditional telecom operators to include internet-based electronic communication services.

2. Key obligations of the various actors

The General Data Protection Regulation applies to all actors active in the electoral context such as European and national political parties (hereinafter: "political parties"), European and national political foundations (hereinafter: "foundations"), platforms, data analytics companies and public authorities responsible for the electoral process. They must process personal data (for example names and addresses) lawfully, fairly and in a transparent manner, for specified purposes only. They cannot further use it in a manner incompatible with the purposes for which the data were initially collected. Processing for journalistic purposes also falls within the scope of the General Data Protection Regulation, in principle, but may benefit from exemptions and derogations as provided for in national law, given the importance of the right to freedom of expression and information in a democratic society[10].

The notion of personal data is a comprehensive one. Personal data is all data relating to an identified or identifiable natural person. Data processed in the electoral context will often include special categories of personal data ("sensitive data") such as political opinions, trade union membership, ethnic origin, sex life, etc. which benefit from a more protective regime[11].

[7] The European Data Protection supervisor also issues Opinions.
[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).
[9] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017)10 final.
[10] Article 85(2) General Data Protection Regulation.
[11] Article 9(1) General Data Protection Regulation.

Moreover, data analytics can infer "sensitive data" (such as political opinions but also religious beliefs or sexual orientations) from sets of non-sensitive data. The processing of those inferred data also fall within the scope of the General Data Protection Regulation and should therefore comply with all data protection rules.

In conclusion, virtually all data processing operations in the electoral context are subject to the General Data Protection Regulation.

Taking into account the need to provide clarity to the actors involved in the electoral process and the first findings in the Cambridge Analytica case, the following sections highlight the data protection obligations which appear of particular relevance in the electoral context. They are summarised in the annex.

2.1 Data controllers and processors

The notion of accountability of data controllers and joint controllers is a central feature of the General Data Protection Regulation. The data controller is the organisation deciding, alone or in cooperation with others, why and how the personal data is processed; the data processor processes personal data only on behalf and under the instructions of the controller (with their relationship determined in a contract or another legal binding act). Controllers must put in place measures appropriate to the risks and implement data protection by design from the outset and be able to demonstrate compliance with the General Data Protection Regulation (accountability principle).

The role as data controller or data processor has to be assessed in each individual case. In the electoral context, a number of actors can be data controllers: political parties, individual candidates and foundations are, in most instances, data controllers; platforms and data analytics companies can be (joint) controllers or processors for a given processing depending on the degree of control they have over the processing concerned[12]; national electoral authorities are controllers for the electoral registers.

When their processing activities relate to the offering of goods and services to individuals in the Union or the monitoring of their behaviour in the Union, companies based outside the Union also have to comply with the General Data Protection Regulation. This is the case of a number of platforms and data analytics companies.

2.2 Principles, lawfulness of processing and special conditions for "sensitive data"

Actors involved in elections can only process personal data, including those obtained from public sources, in accordance with the principles related to the processing of personal data and based on the limited number of grounds clearly identified by the General Data Protection Regulation[13]. The most relevant grounds for lawful processing in the electoral context appear

[12] The recent case law of the Court of Justice of the European Union (Jehovah Witnesses case C-25/17, judgement of 10 July 2018) clarified that an organisation 'exercising influence' over the activity of collecting and processing personal data can, under certain circumstances, be considered a controller.
[13] Articles 5 and 6 General Data Protection Regulation.

to be the consent of an individual, the compliance with a legal obligation under Union or national legislation, the performance of a task carried out in the public interest and the legitimate interest of one of the actors. However, actors in the electoral context can rely on the ground of legitimate interest only if their interests are not overridden by the interests or the fundamental rights and freedoms of the individuals concerned.

In addition storing of information, or gaining access to information already stored, in the terminal equipment (computer, smartphone, etc.), must be in compliance with the e-Privacy Directive's requirements on the protection of terminal equipment, which means that the individual concerned would need to give his/her consent.

When consent is used as a legal ground, the General Data Protection Regulation requires that this is given through a clear and affirmative action and is free and informed[14].

Public authorities involved in the electoral context process personal data in order to comply with a legal obligation or for the exercise of a public task. Other actors in the electoral context can process data on the grounds of consent or legitimate interest[15]. Political parties and foundations can also process data on the grounds of public interest if so provided by national law[16].

Public authorities may disclose certain information on individuals included in electoral lists or in registers of residents to political parties only when specifically authorised by Member State law and only for the purpose of advertising in the electoral context and as far as necessary for that purpose, such as name and address.

Processing in the electoral context will often involve "sensitive data". The processing of such data, including inferred "sensitive data", is generally prohibited unless one of the specific justifications provided for by the General Data Protection Regulation[17] applies. Processing of "sensitive data" requires specific, stricter conditions to be fulfilled: the person must have given explicit consent[18] or have made the data concerned public[19]. Political parties and foundations can also process "sensitive data" if there is substantial public interest on the basis of Union or Member State law and appropriate safeguards are in place[20]. The General Data Protection Regulation provides that they can also process "sensitive data" to the extent it relates solely to their members or former members, or to persons who have regular contact with them – but only for disclosure within their political party or foundation[21]. This specific

[14] Article 7 and Article 4(11) General Data Protection Regulation.
[15] Provided that the rights and freedoms of the concerned individuals are not seriously impacted.
[16] See Recital 56 of the General Data Protection Regulation "where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established".
[17] Article 9 General Data Protection Regulation.
[18] Article 9(2)(a) General Data Protection Regulation.
[19] Article 9(2)(e) General Data Protection Regulation.
[20] Article 9(2)(g) General Data Protection Regulation.
[21] Article 9(2)(d) General Data Protection Regulation. Political party or foundation cannot share the data relating to their members or former members, or to persons who have regular contact with them, with a third party without the consent of the individual concerned.

provision however cannot be used by a political party to process data of prospective members or voters.

The purpose of the data processing should be specified at the time of collection ("purpose limitation" principle)[22]. Data collected for one purpose can only be further processed for a compatible purpose; otherwise a new legal ground, provided for by the General Data Protection Regulation, such as consent, has to be found for the processing for the new purpose. In particular, when lifestyle data brokers or platforms collect data for commercial purposes, that data cannot be further processed in the electoral context.

Unless political parties and foundations apply due diligence and check that the data has been obtained lawfully, they cannot use any such data received from a third party.

2.3 Transparency requirements

The Cambridge Analytica case has shown the importance of fighting opacity and properly informing the individuals concerned. Individuals often do not know who processes their personal data and for which purposes. The principles of fair and transparent processing require that individuals be informed of the existence of the processing operation and its purposes[23]. The General Data Protection Regulation clarifies the obligations of data controllers in this respect. They have to inform individuals about key aspects related to the processing of their personal data such as:

- the identity of the controller,
- the purposes of processing,
- the recipients of personal data,
- the source of the data when not collected directly from the person,
- the existence of automated decision-making and
- any further information necessary to ensure fair and transparent processing[24].

Moreover, the General Data Protection Regulation requires that information to be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language[25]. For instance, a short, opaque notice on data protection printed only in small print in electoral materials would not meet the transparency requirements.

According to the preliminary findings, incomplete information on the purpose for which the data were collected was a key shortcoming in the Cambridge Analytica case, which also put into question the validity of the consent of the persons concerned. All organisations processing personal data in the electoral context have to make sure that individuals fully understand how and for what purpose their personal data will be used, before they give their consent or before processing by the controller commences based on any other ground for processing.

[22] Article 5(1) (b) General Data Protection Regulation.
[23] Article 5(1) (a) General Data Protection Regulation.
[24] Articles 13 and 14 General Data Protection Regulation.
[25] Guidelines of the European Data Protection Board on transparency.

Information has to be provided to individuals at each stage of the processing, not only when data is collected.

In particular, when political parties process data obtained from third party sources (such as from electoral registers, data brokers, data analysts and other sources) they typically need to inform and explain to the individuals concerned how they combine and use this data to ensure fair processing[26].

2.4 Profiling, automated decision-making and micro-targeting

Profiling is a form of automated data processing used to analyse or predict aspects concerning for instance personal preferences, interests, economic situation, etc[27]. Profiling can be used to micro-target individuals, namely to analyse personal data (such as a search history on internet) to identify the particular interests of a specific audience or individual in order to influence their actions. Micro-targeting may be used to offer a personalised message to an individual or audience using an online service e.g. social media.

The Cambridge Analytica case has shown the particular challenges raised by micro-targeting methods on social media. Organisations can be mining the data collected through social media users to create voters' profiles. This might allow such organisations to identify voters who can be more easily influenced and therefore allow such organisations to exert an impact on the outcome of elections.

All the general principles and rules of the General Data Protection Regulation apply to such data processing, such as the principles of lawfulness, fairness and transparency and purpose limitation. Individuals very often are not aware that they are subject to profiling: they do not understand why they receive some advertisement so clearly linked to the last searches they made, or why they receive personalised messages from different organisations. The General Data Protection Regulation obliges all data controllers, for instance political parties or data analysts, to inform the individuals when they use such techniques and on their consequences[28].

The General Data Protection Regulation recognises that automated decision-making, including profiling, can have serious consequences. The General Data Protection Regulation provides that an individual has the right not to be subject to a decision based solely on automated processing and producing legal effects concerning him or her or similarly significantly affects him or her, unless such processing is carried out under strict conditions, namely when individuals provide their explicit consent, or when Union or Member State law which lays down appropriate safeguards allows for it[29].

Micro-targeting practices in the electoral context fall into this category when they produce sufficiently significant effect on individuals. The European Data Protection Board stated that

[26] Article 14 General Data Protection Regulation.
[27] As defined in Article 4(4) General Data Protection Regulation.
[28] Article 13(2) General Data Protection Regulation.
[29] Article 22 General Data Protection Regulation.

this is the case when the decision has the potential to significantly affect the circumstances, behaviour or choices of the individuals or have a prolonged or permanent impact on the individual[30]. The Board considered that online targeted advertisement could have in some circumstances the capability to sufficiently significantly affect the individuals when, for instance, it is intrusive or uses knowledge of vulnerabilities of the individuals. Given the significance of the exercise of the democratic right to vote, personalised messages which have for instance the possible effect to stop individuals from voting or to make them vote in a specific way could have the potential of meeting the criterion of significant effect.

In the electoral context therefore controllers need to ensure that any processing using such techniques is lawful in accordance with the above mentioned principles and strict conditions of the General Data Protection Regulation.

2.5 Security and accuracy of personal data

Security is of particular importance in the electoral context given the size of the data sets involved, and the fact that such sets often contain "sensitive data". The General Data Protection Regulation requires operators processing personal data (both controllers and processors) to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks posed by the processing to the rights and freedoms of individuals[31].

The General Data Protection Regulation requires controllers to notify personal data breaches to the competent supervisory authority without undue delay and at the latest within 72 hours. When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must also inform the individuals affected by that data breach without undue delay[32].

Political parties and other actors involved in the electoral process have to pay particular attention to ensure the accuracy of personal data when big data sets are concerned and when data are compiled from different, heterogeneous sources. Inaccurate data must be immediately erased or rectified and, where necessary, updated.

2.6 Data protection impact assessment

The General Data Protection Regulation introduces a new tool for assessing the risk before processing starts: the data protection impact assessment. It is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals[33]. This is the case in the electoral context when a data controller evaluates, systematically and extensively, personal aspects of an individual (including profiling), significantly affecting the individual, and when

[30] Guidelines of the European Data Protection Board on automated decision making, WP251rev.01 as last revised and adopted on 06.02.2018.
[31] Article 32 General Data Protection Regulation.
[32] Articles 33 and 34 General Data Protection Regulation; and Guidelines of the European Data Protection Board on personal data breach notification.
[33] Articles 35 and 36 General Data Protection Regulation; and Guidelines of the European Data Protection Board on data protection impact assessment.

the controller processes "sensitive data" on a large scale. National electoral authorities acting in the performance of their public tasks might not have to conduct a data protection impact assessment if a data protection impact assessment has already been carried out in the context of the adoption of the legislation.

The impact assessments to be carried out by the various actors in the context of elections should include the elements necessary to address the risks involved in such processing, notably the lawfulness of processing also for data sets obtained from third parties and the transparency requirements.

3. Rights of individuals

The General Data Protection Regulation gives individuals additional and stronger rights which are particularly relevant in the electoral context:

- the right to access to their personal data;
- the right to request the deletion of their personal data if the processing is based on consent and that consent is withdrawn, if the data is no longer needed or if the processing is unlawful; and
- the right to have incorrect, inaccurate or incomplete personal data corrected.

Individuals also have the right to object to processing (for example of data included in electoral lists transmitted to political parties) if the processing of their data is based on the "legitimate interest" or the "public interest" grounds.

Individuals have the right not to be subject to decisions based solely on the automated processing of their personal data. In such cases the individual may request intervention by a natural person and have the right to express their point of view and to contest the decision.

In order for individuals to be able to exercise those rights, all actors involved have to provide the necessary tools and settings. The General Data Protection Regulation provides for the possibility to develop a code of conduct approved by a data protection authority specifying the application of the Regulation in specific areas, including in the electoral context.

The General Data Protection Regulation grants individuals the right to lodge a complaint to a supervisory authority and the right to a judicial remedy. It also gives individuals the right to mandate a non-governmental organisation to lodge a complaint on their behalf[34]. In certain Member States, national legislation allows a non-governmental organisation to lodge a complaint without being mandated by an individual. This is particularly relevant in the electoral context given the large number of persons potentially concerned.

[34] Article 80(1) General Data Protection Regulation.

Key data protection issues relevant in the electoral process[35]

<table>
<tr><td rowspan="2">Political parties and foundations</td><td colspan="2">Political parties and foundations are data controllers</td></tr>
<tr><td colspan="2">• Comply with purpose limitation, further processing only for compatible purpose (for example, when sharing data with platforms)
• Choose the appropriate legal basis for processing (also for inferred data): consent, legitimate interest, task in the public interest (if provided by law), specific conditions for “sensitive data” (for instance: political opinion)
• Conduct a data protection impact assessment
• Inform individuals on each processing purpose (transparency requirements), either when collecting data directly or when obtaining it from third parties
• Ensure data accuracy, in particular for data coming from different sources and for inferred data
• Check if data received from third parties have been obtained lawfully and for which purposes (for instance: whether concerned individuals gave their informed consent for a given purpose)
• Take into account the specific risks of profiling and adopt appropriate safeguards
• Comply with specific conditions when using automated decision making (for example, obtain explicit consent and implement suitable safeguards)
• Clearly identify who has access to the data
• Ensure security of processing through technical and organisational measures; report data breaches
• Clarify obligations in contracts or other legal binding acts with data processors, such as data analytics companies
• Delete the data when it is no longer necessary for the initial purpose for which it was collected</td></tr>
<tr><td rowspan="3">Data brokers and data analytics companies</td><td colspan="2">Data brokers and data analytics companies are either (joint) controllers or processors depending on the degree of control they have over the processing</td></tr>
<tr><td>As data controller</td><td>As data processor</td></tr>
<tr><td>• Comply with purpose limitation, further processing only for compatible purpose (especially when sharing the data with third parties)
• Choose the appropriate legal basis for processing: consent, legitimate interest.</td><td>• Comply with obligations from the contract or other binding legal act with the controller
• Ensure security of processing through technical and organisational measures</td></tr>
</table>

[35] The information above is in no way exhaustive. It aims at highlighting a number of key obligations linked to data under the General Data Protection Regulation which are relevant in the electoral process. They correspond to a scenario where political parties are collecting data themselves (from public sources, from their presence on social media, directly from voters, etc.) and use the service from data brokers or data analytics companies with the objective to target voters through social media platforms. Platforms can also be a source of data for the actors mentioned above. Other legislation may be relevant as well, such as the rules on the sending of unsolicited communications and the protection of terminal equipment in the ePrivacy Directive.

	If "sensitive data", processing only possible if explicit consent or data manifestly made public • Conduct a data protection impact assessment • Inform individuals on each processing purpose (transparency requirements) – in particular when consent is sought since usually the data will be sold to a third party • Comply with specific conditions when using automated decision making (e.g. obtain explicit consent and implement suitable safeguards) • Pay particular attention to lawfulness of processing and to accuracy when combining different data sets • Ensure security of processing through technical and organisational measures; report data breaches	• Support for the controller in data protection impact assessment or in the exercise of data subjects rights or in communicating to the controller a data breach without delay if they become aware of one
	Platforms are usually data controllers for processing taking place on their platforms and possibly co-controller with other organisations	
Social media platforms / online ad networks	• Choose the appropriate legal basis for processing: contract with individuals, consent, legitimate interest. If "sensitive data", processing only possible if explicit consent or data manifestly made public • Use only data that is necessary for the identified purpose • Conduct a data protection impact assessment • Ensure lawfulness when sharing members data with third parties • Comply with transparency requirements, in particular as regards the Terms and Conditions, if data are subsequently shared with a third party, etc. • Comply with specific conditions when using automated decision making (e.g. obtain explicit consent and implement suitable safeguards) • Ensure security of processing through technical and organisational measures; report data breaches • Provide controls and settings for individuals to effectively exercise their rights, including the right not to be subject to a decision based solely on automated processing including profiling	
	National electoral authorities are data controllers	
National electoral authorities	• Legal basis for processing: legal obligation or task of public interest based on law • Conduct a data protection impact assessment if impact not already assessed in the law	