edpb
European Data Protection Board

Statement

Statement 2/2019 on the use of personal data in the course of political campaigns

Adopted on 13 March 2019

The European Data Protection Board has adopted the following statement:

Engaging with voters is inherent to the democratic process. It allows the preparation of political programmes, enables citizens to influence politics and the development of campaigns in line with citizens expectations.

Political parties, political coalitions and candidates increasingly rely on personal data and sophisticated profiling techniques to monitor and target voters and opinion leaders. In practice, individuals receive highly personalised messages and information, especially on social media platforms, on the basis of personal interests, lifestyle habits and values.

Predictive tools are used to classify or profile people’s personality traits, characteristics, mood and other points of leverage to a large extent, allowing assumptions to be made about deep personality traits, including political views and other special categories of data. The extension of such data processing techniques to political purposes poses serious risks, not only to the rights to privacy and to data protection, but also to trust in the integrity of the democratic process. The Cambridge Analytica revelations illustrated how a potential infringement of the right to protection of personal data could affect other fundamental rights, such as freedom of expression and freedom to hold opinions and the possibility to think freely without manipulation.

The EDPB observes that, in addition to political parties and candidates, several other actors can be involved in the processing of personal data for political purposes: social media platforms, interest groups, data brokers, analytics companies, ad networks. These actors can play an important role in the election process and their compliance is subject to supervision by independent data protection authorities.

In light of the elections to the European Parliament and other elections in the EU scheduled for 2019, the EDPB wishes to underline a number of key points to be respected when political parties process personal data in the course of electoral activities:

1. Personal data revealing political opinions is a special category of data under the GDPR. As a general principle, the processing of such data is prohibited and is subject to a number of narrowly-interpreted conditions, such as the explicit, specific, fully informed, and freely given consent of the individuals.[1]

2. Personal data which have been made public, or otherwise been shared by individual voters, even if they are not data revealing political opinions, are still subject to, and protected, by EU data protection law. As an example, using personal data collected through social media cannot be undertaken without complying with the obligations concerning transparency, purpose specification and lawfulness.

3. Even where the processing is lawful, organisations need to observe their other duties pursuant to the GDPR, including the duty to be transparent and provide sufficient information to the individuals who are being analysed and whose personal data are being processed, whether data has been obtained directly or indirectly. Political parties and candidates must stand ready to demonstrate how they have complied with data protection principles, especially the principles of lawfulness, fairness and transparency.

4. Solely automated decision-making, including profiling, where the decision legally or similarly significantly affects the individual subject to the decision, is restricted. Profiling connected to targeted campaign messaging may in certain circumstances cause 'similarly significant effects' and shall in principle only be lawful with the valid explicit consent of the data subject.[2]

5. In case of targeting, adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it and how they can exercise their rights as data subjects. In addition, the Board notes that, under the

[1] See article 9 GDPR. One example is that of data manifestly made public by the data subject, which, like other derogations of special data categories, should be interpreted narrowly, as it cannot be used to legitimate inferred data.

[2] The EDPB has previously clarified that a legal effect generated by automated decision-making may include affecting a person's vote in an election.

law of some Member States, there is a transparency requirement as to payments for political advertisement.

The EDPB refers political parties and other stakeholders to the practical guidance and recommendations issued by several data protection authorities regarding the use of data in the course of elections.[3] It also welcomes the set of measures presented by the European Commission in September 2018,[4] and the Conclusions of the Council and of the Member States on securing free and fair European elections.[5]

EDPB members also work together with other relevant competent authorities[6] to ensure consistent interpretation and compliance with applicable laws, including the GDPR, to safeguard trust in the security and integrity of the elections to the European Parliament and other elections in the EU scheduled for 2019 and beyond.

Compliance with data protection rules, including in the context of electoral activities and political campaigns, is essential to protect democracy. It is also a means to preserve the trust and confidence of citizens and the integrity of elections. Ahead of the upcoming electoral deadlines, data protection authorities are committed to monitor and, if necessary, enforce the application of data protection principles in the context of elections and political campaigns, such as transparency, purpose limitation, proportionality and security, as well as the exercise of data subject rights. Data protection authorities will make full use of their powers, as provided by the GDPR, and ensure cooperation and consistency in their actions within the framework of the EDPB.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[3] See Annex I.

[4] And especially the Guidance on the application of EU data protection law and the Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

[5] https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf.

[6] For instance, in the framework of European election networks as further described in the Commission's "electoral package" (see, in particular, the Recommendation on election cooperation networks mentioned in footnote 4 above and the Commission’s proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament).