European Commission

STATE OF THE UNION 2018

Protecting Europeans' personal data in elections

#SOTEU

12 September 2018

'I want Europeans to be able to make their political choices next May in fair, secure and transparent European elections. In our online world, the risk of interference and manipulation has never been so high. It is time to bring our election rules up to speed with the digital age to protect European democracy.'

Jean-Claude Juncker, 12 September 2018

Political parties are increasingly using personal data to target citizens on social media during election periods. The Cambridge Analytica revelations demonstrate the risk modern technologies can pose to the electoral process. The Commission has set out guidance today on how existing EU rules should be used to tackle this issue and guarantee the fairness of the electoral process, especially ahead of the 2019 European Parliament elections.

The EU's General Data Protection Regulation that entered into application in May 2018 provides clear rules on how all actors involved in elections need to play their part and abide by the new data protection rules.

Obligations for political parties and foundations

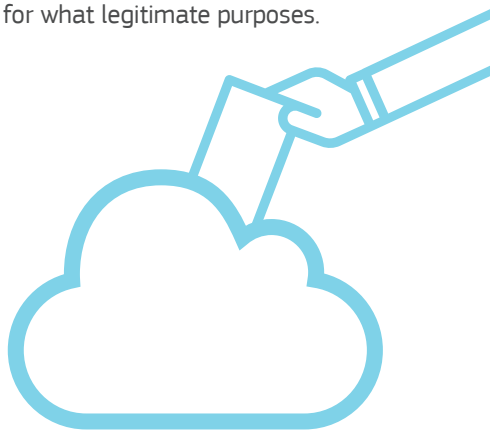
Political parties and foundations are data controllers, as they decide why and how personal data is processed.

DOs:

- Choose the **appropriate legal basis** for processing people's data and pay attention to the specific conditions for processing sensitive data;
- Make sure the systems you are using are **secure** and, if there is a data breach, inform people about it without delay;
- Inform individuals when you start processing their data, and also when you collect it from third parties;
- Make sure that the data you process is accurate, especially when compiling data from various sources;
- If you are using services of a **third party** — for example a data analytics company — check if data received from it has been obtained legally.

DON'Ts:

- Don't process people's data if it was provided by them for another **purpose** unrelated to the specific election context;
- Don't give wide **access** rights to people's data that you have. You should check who in your organisation has access to the data and for what legitimate purposes.



Data analytics companies / Data brokers

Data analytics companies/data brokers are either controllers or processors depending on the degree of control they have over the processing. For example, if a data analytics company processes people's data under the instruction of a political party, it is a data processor.

DOs:

- Choose the **appropriate legal basis** for processing people's data;

The text below is only valid if the data analytics company/ data broker is a data controller

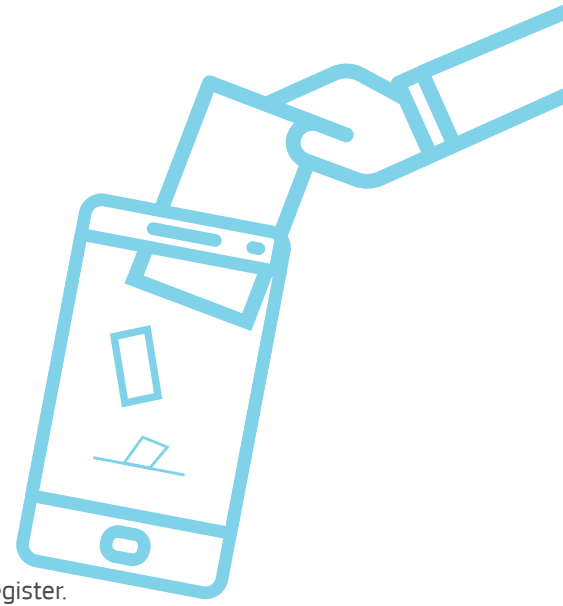
- If you process **sensitive data** (e.g. ethnic origin), you need to have an explicit consent from that person; or apply other exceptions foreseen by the General Data Protection Regulation;
- Make sure the systems you are using are **secure** and, if there is a data breach, inform people about it without delay;
- If you combine different **data sets** about people, make sure it is done accurately and legally;

The last point is only valid if the data analytics company/ data broker is a data processor

- Help **third parties** you are working with — such as political parties — if they need your assistance, for example when preparing a data protection impact assessment.

DON'Ts:

- Don't process people's data if it was given by them for another **purpose** unrelated to the specific election context;
- You should inform people on each processing purpose, especially when you sell it to a third party — for example a political party.



National electoral authorities

National electoral authorities are **data controllers**, as they control the electoral register.

DOs:

- Conduct a data protection **impact assessment** to assess risk before you start processing people's data;
- The **legal basis** for processing people's data will usually be to meet a legal obligation or carry out a task of public interest based on law.

Social Media Platforms

Social media platforms are data controllers, because the processing of people's data takes place on their platforms.

DOs:

- Choose the **appropriate legal basis** for processing people's data;
- If you process **sensitive data** (e.g. ethnic origin), you need to have an explicit consent from that person; or apply other exceptions foreseen by the General Data Protection Regulation;
- Give people **controls and settings** to effectively exercise their rights, for example when they request correction or deletion of their data;
- Make sure the systems you are using are **secure** and, if there is a data breach, inform people about it without delay.

DON'Ts:

- Don't share data with **third parties**, for example with a data analytics' company, unless the users have given their explicit consent;
- If you share your users' data with third parties, specify this clearly in the Terms and Conditions of your platform.