



# Free and fair European 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.'*

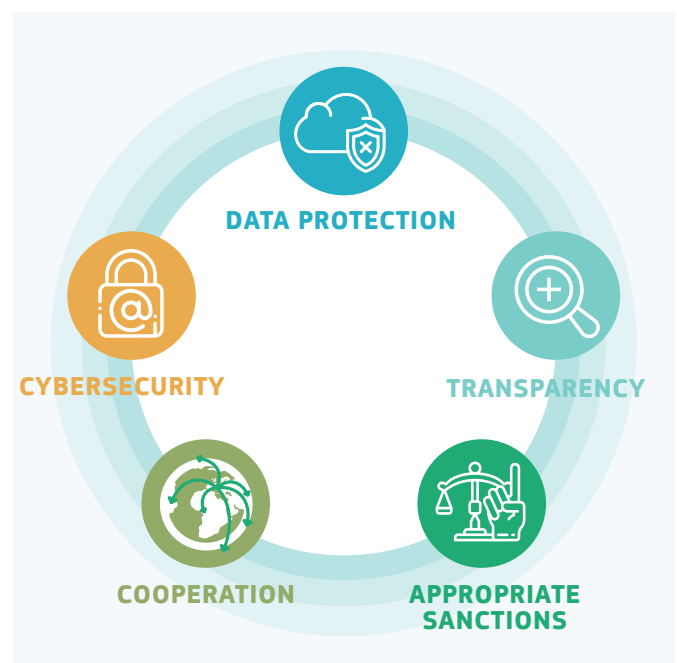
Jean-Claude Juncker, 12 September 2018



Ensuring the resilience of the Union's democratic systems is part of the Security Union. This is why to help making sure that next year's **elections** to the European Parliament are organised in a **free, fair and secure** manner, President Juncker announced in his annual State of the Union Address a set of concrete measures. The Commission is outlining today the potential threats to the elections and proposing solutions for how national governments and authorities, political parties, the media and digital platforms could address them.

#### The proposed measures include:

- a Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns;
- guidance on the application of of the EU's General Data Protection Regulation;
- a legislative amendment tightening the rules on European political party funding.



#### The set of measures to protect European elections focus on:

**DATA PROTECTION:** improving the protection of personal data in the electoral context

**TRANSPARENCY:** guaranteeing the transparency of online political advertising

**CYBERSECURITY:** protecting elections from cyberattacks

**COOPERATION:** improving national and European cooperation on potential threats to European Parliament elections

**APPROPRIATE SANCTIONS:** guaranteeing that electoral rules are respected by all



## DATA PROTECTION

Recent revelations, including the “Facebook/Cambridge Analytica” case, where personal data is believed to have been misused, have highlighted the risks of certain online activities to the electoral processes.

The Commission gives **guidance** to European political parties, foundations, national authorities organising elections, but also social media platforms **on how to apply the new EU’s General Data Protection Regulation that applies since May 2018 in the electoral context.**



## TRANSPARENCY

While safeguards and rules apply off-line for the organisation of elections, such as transparency and limits on electoral spending, silence periods and equal treatment of candidates by the media during election periods, these rules are vulnerable to being bypassed online.

The Commission has already launched work on tackling online disinformation. A Code of Practice should commit online platforms and the advertising industry to ensure transparency and restrict targeting options for political advertising. The Code is expected to be endorsed by the end of September 2018. The Commission will closely follow the process, evaluate the progress made and analyse the first results of the Code of Practice by the end of 2018.

**The Commission gives recommendations** to the authorities and political parties and foundations in EU countries on how **to ensure transparency of political advertising:**



political parties, foundations and campaign organisations should make information available for citizens on how much money they spend on online advertising in a campaign;



they should clearly indicate which party or political support group is behind paid online political advertisements;



they should share with European citizens information on how they are targeted in the dissemination of such advertisements;



where these principles are not followed, Member States should apply relevant electoral sanctions.



## NATIONAL AND EUROPEAN COOPERATION

Cooperation at national and EU level of the different actors involved in the electoral process will help detect potential risks including hybrid threats to elections and solve these issues quickly.

The Commission organised the first exchange between EU countries on electoral best practices in April 2018. As a follow up, the Commission will set up a European cooperation network in view of the 2019 European Parliament elections. Two additional meetings will be organised in January and April 2019.

**The Commission recommends that** the authorities in EU countries improve:

- ▶ **cooperation at national level** - every country should appoint a national election cooperation network to coordinate the efforts of its different authorities (authorities with competence on electoral matters; authorities in charge of monitoring and enforcing rules related to online activities). This will enable them to quickly detect potential threats to the elections to the European Parliament and swiftly enforce existing rules including by applying sanctions.
- ▶ **cooperation at European level** - every country should appoint a single point of contact for the implementation of this recommendation. This will facilitate the sharing of expertise and best practices among EU countries including on threats, gaps and enforcement.



## CYBERSECURITY

Cyberattacks pose a risk to elections, campaigns, political parties, candidates or public authorities' systems and can affect the integrity and fairness of the electoral process.

The Commission has developed together with the national authorities responsible for cybersecurity and the EU Cybersecurity Agency a Compendium which provides specific guidance on cybersecurity-related threats. In parallel to the Recommendation, the Commission proposes to create a Network of Cybersecurity Competence Centres together with a new European Competence Centre to better target and coordinate available funding for cybersecurity cooperation, research and innovation.

**The Commission recommends:**

- ▶ that the authorities in EU countries should adopt technical and organisational measures **to manage the risks posed to the security of network and information systems** used for the organisation of elections to the European Parliament.
- ▶ that Member States' authorities responsible for cybersecurity apply the developed guidance on cybersecurity-related threats.



## APPROPRIATE SANCTIONS

The Commission proposes **to introduce financial penalties of 5% of the annual budget of the European party or political foundation** concerned if they infringe the data protection rules in an attempt to influence the outcome of elections to the European Parliament. In addition, any party or foundation found guilty would not be able to apply for funding from the general budget of the European Union in the year in which it was sanctioned. These rules will be enforced by the Authority for European political parties and European political foundations. As regards political advertising, Member State authorities should apply relevant electoral sanctions where the principles of transparency are not followed.

