**Follow up to the European Parliament non-legislative resolution on** **the use of Facebook users’ data by Cambridge Analytica and the impact on data protection**

1. **Resolution tabled pursuant to Rule 123(2) of the European Parliament's Rules of procedure by the Committee on Civil Liberties, Justice and Home Affairs**
2. **Reference numbers:** 2018/2855 (RSP) /B8-0480/2018 / P8\_TA-PROV(2018)0433
3. **Date of adoption of the resolution:** 25 October 2018
4. **Subject:** The use of Facebook users’ data by Cambridge Analytica and the impact on data protection
5. **Competent Parliamentary Committee:** Committee on Civil Liberties, Justice and Home Affairs (LIBE)
6. **Brief analysis/ assessment of the resolution and requests made in it:**

The resolution covers the fallout of the Facebook/ Cambridge Analytica scandal within the context of two main subject areas – the misuse of personal data for political advertising and election interference.

The resolution summarises the conclusions reached following last May’s meeting between leading members of the European Parliament (MEPs) and Facebook CEO Mark Zuckerberg, and the three subsequent hearings. It also references the data breach suffered by Facebook on 28 September. It references a number of Commission’s actions, in particular the Election package of 12 September.

Misuse of personal data for political advertising

MEPs note that the data obtained by Cambridge Analytica may have been used for political purposes, by both sides in the United Kingdom's referendum on the membership of the European Union and to target voters during the 2016 American presidential election.

The resolution notes that the misuse of personal data affects the fundamental rights of billions of people around the globe and considers that the General Data Protection Regulation (GDPR) and the e-Privacy Directive provide the highest standards of protection that must be upheld by all stakeholders.

The MEPs find that Facebook not only breached the trust of the citizens of the European Union, but also the law of the European Union.

The resolution calls for the following actions:

* Facebook to make changes to its platform to comply with the data protection law of the European Union and to allow for a full audit to be done by the European Union Agency for Network and Information Security (ENISA) and the European Data Protection Board (EDPB);
* National and European Union data protection authorities to conduct a thorough investigation of Facebook and its current practices to ensure compliance with GDPR;
* That third-party audits be carried out after referendum campaigns to ensure that personal data held by the campaign is deleted;
* Member States to provide data protection authorities with adequate funding to meet new challenges and the Commission to scrutinise the Member States closely on this obligation;
* The Commission to suspend the Privacy Shield until the American authorities comply with its terms. It further calls on the competent European Union data protection authorities to investigate the revelations in the Facebook/ Cambridge Analytica case and, if appropriate, suspend or prohibit data transfers under the Privacy Shield;
* The Commission to upgrade competition rules to reflect the possible monopoly situation of social media platforms and to propose amendments to the European Electronic Communications Code to overcome the lock-in effect for their users;
* All European Union bodies to evaluate their current communication policies on the social media to ensure they do not put the personal data of citizens at risk;
* The next Commission to task one of its members specifically with the privacy and data protection portfolio;
* The Commission to audit the activities of the advertising industry on social media and propose legislation in the event that the sector and concerned parties are unable to reach agreement on voluntary Codes of Conduct with dissuasive measures.

Election interference

The resolution considers election interference to be a huge risk for democracy, the tackling of which requires a joint effort involving service providers, regulators and political actors and parties. It highlights the urgency of countering any attempt to manipulate European Union elections and of reinforcing rules applicable to online platforms.

The resolution welcomes the package presented by the Commission on 12 September 2018 regarding preparations for the European elections and recalls the measures proposed by the Commission for securing free and fair European elections, in particular the legislative amendment to tighten up the rules on European political party funding, creating the possibility to impose financial sanctions for taking advantage of the infringements of applicable data protection rules in order to deliberately influence or attempt to influence the outcome of the European elections. It also recalls that the processing of personal data by political parties in the European Union is subject to the GDPR, and that the breach of the principles, rights and obligations encompassed within this law would result in additional fines and sanctions.

The resolution calls for the following actions:

* Member States to adapt the electoral rules on online campaigning, including those pertaining to transparency on funding, election silence periods, the role of the media and disinformation;
* Banning profiling for electoral purposes, including use of online behaviour that may reveal political preferences;
* All online platforms to urgently roll out planned political advertising transparency features in consultation with national electoral authorities;
* Social media to label content shared by bots, speed up removing fake accounts and work with independent fact-checkers to fight disinformation;
* Member States to take measures to address the risks posed to the security of network and information systems used for the organisation of elections;
* Member States to engage with stakeholders in awareness‑raising activities to increase transparency and build trust in the electoral process;
* Investigations should be carried out by the Member States with the support of Eurojust, into alleged misuse of the online political space by foreign forces.
1. **Response to the requests in the resolution and overview of the action taken, or intended to be taken, by the Commission:**

The Commission is pleased to reply below to the requests made in the resolution, while noting that further measures will be set out in the Action Plan which is currently being prepared following the call by the European Council of 28 June 2018.

Misuse of personal data for political advertising

As part of its Electoral package presented on 12 September, the Commission has issued a **guidance on data protection in the electoral context** reminding national electoral authorities, political parties, data brokers and data analytics companies, social media platforms and online ad networks of the principles and obligations of GDPR regarding the lawfulness of processing of personal data (including sensitive data such as political opinions), transparency requirements, automated decision-making and micro-targeting.

The guidance also stresses that the national data protection authorities, as enforcers of the GDPR, have to make full use of their strengthened powers to address possible infringements.

The Commission welcomes the Parliament’s request for Facebook to make changes to its platform to comply with European Union data protection law.

The Commission agrees with the Parliament’s about the necessity for the Member States to provide data protection authorities with adequate funding to meet new challenges, including in the context of enforcing electoral rules online. The Commission has on several occasions reminded the Member States of the importance of fulfilling their obligations in this respect[[1]](#footnote-1). Commissioner Jourová has also sent a letter to all responsible ministers in the European Union on 25 May 2018 reminding them about this obligation.

Investigations into alleged misuse of the online political space by foreign forces should be carried out by the Member States. They can use the support of Eurojust, if the conditions in its legal base are met.

With respect to the Privacy Shield, the Commission agrees with the European Parliament on the importance of robust enforcement of the framework by the American authorities. This was already reflected in the report on the first annual review of the Privacy Shield; the concerns expressed by the Parliament, which the Commission shares, were again raised in the second annual review which took place on 18 and 19 October 2018. A periodic review is foreseen in both the Commission’s Privacy Shield adequacy decision and the General Data Protection Regulation as a mechanism to assess whether the Commission’s findings in an adequacy decision are still justified.

As indicated, the need for proactive compliance monitoring and enforcement were, among other topics, central elements of the review. In this regard, the U.S. Federal Trade Commission (FTC) reported that its investigation of Facebook’s privacy practices is ongoing and again confirmed that it covers potential Privacy Shield violations. The FTC also informed about its ongoing enforcement activities more generally, in particular the more proactive control of companies' compliance with privacy rules. Also, the Department of Commerce assured the Commission that it will revoke the certification of companies that do not comply with the Privacy Shield framework[[2]](#footnote-2). The Commission will closely follow any development in this regard.

The Commission’s findings are reflected in the report to the European Parliament and the Council (COM(2018)860 final) as well as the accompanying staff working document (SWD(2018)497 final), published on 19 December 2018. The report concludes that the Privacy Shield continues to ensure an adequate level of protection for personal data transferred from the European Union to participating companies. At the same time, the Commission identified certain areas that will be closely monitored, including in the context of future reviews. This includes the progress and outcome of the Federal Trade Commission’s ongoing investigations.

Regarding paragraph 31 in which Parliament calls on the Commission to upgrade competition rules to reflect the possible monopoly situation of social media platforms and to propose amendments to the European Electronic Communications Code to overcome the lock-in effect for their users the Commission has analysed trading practices which fall outside of the realms of competition law and made a proposal for a regulation on promoting fairness and transparency for business users of online intermediation services[[3]](#footnote-3). The proposal includes a series of transparency obligations and mechanisms for redress and is accompanied by an Observatory of the online platform economy to analyse emerging and problematic practices which may deserve further policy attention. The Commission considers that the Parliament’s call on it to propose amendments to the European Electronic Communications Code (paragraph 31) has been superseded by the fact that on 14 November 2018 the Plenary of the European Parliament adopted its position at first reading with a view to adopting the European Electronic Communications Code. On the substance of the request, i.e. to require “over-the-top communications providers to interconnect” the Commission understands that the Parliament refers to the concept of “interoperability” between over-the-top (OTT) services. It should be noted that the Code already foresees in its Article 61(2) the empowerment of National Regulatory Authorities or other competent authorities to impose interoperability obligations on certain OTT providers in justified cases.

Regarding the Parliament’s request in paragraph 35 for the Commission to audit the activities of the advertising industry on social media and propose legislation in the event that the sector and concerned parties are unable to reach agreement on voluntary Codes of Conduct with dissuasive measures the Commission has set up[[4]](#footnote-4) the Observatory on online platform economy, with a specific mandate to perform expert analysis on issues of particular importance related, amongst other, to transparency and accountability in business-to-business commercial relations in online advertising and possible impacts on consumers. The Observatory should consider a broader set of issues, supporting the Commission’s evidence base and assessment of the suitable policy interventions, where necessary.

Election interference

Ensuring fair and free elections to the European Parliament in 2019 is a priority for the Commission. On 12 September 2018 the Commission issued the **Electoral package**, which aims to address potential threats to elections and thereby strengthen the resilience of the Union's democratic systems. Together with the **Code of Practice on Disinformation**, which was recently finalised, these measures cover a number of important areas.

1/ **Introducing a Code of practice improving transparency and fighting disinformation** by:

* + **deploying policies to disrupt advertising and monetisation incentives** for purveyors of disinformation;
	+ **ensuring transparency about political and issue-based advertising**, as well as restricting targeting options for political advertising;
	+ **empowering consumers** by investing in products and technologies to prioritise relevant, authentic and authoritative information in search, feeds or other automatically ranked distribution channels, as well as to make it easier for users to discover different news sources representing alternative viewpoints and to make informed decisions when they encounter news that may be false;
	+ **introducing measures to identify and close fake accounts** and to tackle the issue of automatic bots;
	+ empower the research community by support independent efforts to track disinformation and understand its impact, as well as through collaborations with fact-checkers and academic researchers;

Several major tech companies, such as Facebook, Google, YouTube, Twitter and Mozilla, as well as the European trade associations representing online platforms, advertisers and the advertising industry have already signed up to the Code of Practice.

2/ **Strengthening fact-checking, collective knowledge and monitoring capacity on disinformation.** The Commission has taken a number of steps to facilitate the creation of an independent European Union network of fact checkers ahead of the European Parliament elections. These efforts have allowed to:

* mapping and networking together independent fact-checking organisations in the Member states;
* ascertaining which tools and services are essential and can improve fact-checking activities and their impact;
* identifying professional and ethical standards for independent fact-checking, and
* providing tools and infrastructural support to fact-checking organisations, notably through projects funded under the Horizon 2020 programme.

3**/** **Transparency of political advertising:** while the Code of Practice on disinformation refers to the tech sector, the Recommendation on free and fair elections from the electoral package is calling for complementary measures to be taken by competent authorities, political parties and other stakeholders. The objective is to ensure the active disclosure to citizens of the Union of information on the political party, political campaign or political support group behind paid online political advertisements and communications. Member States should also encourage the disclosure of information on campaign expenditure for online activities, including paid online political advertisements and communications, as well as information on any targeting criteria used in the dissemination of such advertisements and communications.

4/ **Giving guidance on data protection in the electoral context**: reminding national electoral authorities, political parties, data brokers and data analytics companies, social media platforms and online ad networks of the principles and obligations of GDPR regarding the lawfulness of processing of personal data (including sensitive data such as political opinions), transparency requirements, automated decision-making and micro-targeting. The guidance also stresses that 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.

5/ **Enhancing cyber security**: calling the Member States and political parties to put in place the necessary procedures to prevent, detect, manage and respond to cyberattacks. The aim is to minimize their impact, and guarantee a swift exchange of information at all relevant levels. The Commission also recommend political parties, foundations and campaign organizations to implement measures to prevent cyber incidents and protect themselves against cyberattacks.

6a/ **Establishing cooperation networks in each Member State** with the objective to quickly detect potential threats and gaps, sharing findings and expertise, exchange information and ensure a swift and well-coordinated response.

6b/ **Raising awareness of the issues raised by the scandal, in advance of the elections**. Member States should engage with media, online platforms and information technology providers, in awareness raising activities aimed at increasing the transparency of elections and building trust in the electoral processes.

**7/** **Introducing sanctions on the European political parties and foundations (**a **targeted legislative amendment** of Regulation 1141/2014/EU)**.** The Commission proposed to make it possible for the Authority for European political parties and European political foundations to impose financial sanctions on the European political parties and foundations for taking advantage of the infringements of applicable data protection rules which are intended to deliberately to influence or attempt to influence the outcome of the European elections. Sanctions would amount to 5% of the annual budget of the European political party or foundation concerned and prohibition to apply for next year’s funding.

1. In particular Communication of 24 January 2018 on Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, COM(2018) 43 final, page 11, and Communication of 15 May 2018 on Completing a Trusted Digital Single Market for all, COM(2018) 320 final, p.4 [↑](#footnote-ref-1)
2. See Joint Press Statement from Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross on the Second Annual EU-U.S. Privacy Shield Review, 19 October 2018, available at:  http://europa.eu/rapid/press-release\_STATEMENT-18-6157\_en.htm [↑](#footnote-ref-2)
3. <https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services> [↑](#footnote-ref-3)
4. <https://ec.europa.eu/digital-single-market/en/news/commission-decision-group-experts-observatory-online-platform-economy> [↑](#footnote-ref-4)