European Commission - Press release

State of the Union 2018: European Commission proposes measures for securing free and fair European elections

Strasbourg, 12 September 2018

European Commission proposes measures for securing free and fair European elections.

On 12 September 2018, on the occasion of his State of the Union Address, President Jean-Claude **Juncker** said: *"We must protect our free and fair elections. This is why the Commission is today proposing new rules to better protect our democratic processes from manipulation by third countries or private interests."*

To help make sure that next year's elections to the European Parliament are organised in a free, fair and secure manner, President Jean-Claude **Juncker** announced in his State of the Union Address a set of concrete measures, including greater transparency in online political advertisements and the possibility to impose sanctions for the illegal use of personal data in order to deliberately influence the outcome of the European elections. The objective of today's Commission proposals is to address potential threats to elections and thereby strengthen the resilience of the Union's democratic systems.

Recent cases have shown the risks for citizens to be targeted by mass online disinformation campaigns with the aim to discredit and delegitimise elections. Peoples' personal data are also believed to have been illegally misused.In addition, attacks against electoral infrastructure and campaign information systems are hybrid threats that need to be addressed. Ahead of the European elections next year, it is therefore essential to bolster Europe's democratic resilience and make sure that the off-line rules created on transparency and to protect the electoral process from foreign interference also apply online.

First Vice-President Frans **Timmermans** said: *"Together with the rule of law and fundamental rights, democracy is part of 'who we are' and defines our Union. We must not be naive: there are those who want to disrupt European elections and their tools are sophisticated. And that is why we all must work together urgently to beef up our democratic resilience. Today's elections package is a strong contribution to that effort."*

Commissioner for Justice, Consumers and Gender Equality, Věra **Jourová** added: *"We need to draw lessons from the recent elections and referenda. We want to minimise the risk in the upcoming elections, ranging from non-transparent political advertising to misuse of people's personal data, especially by foreign actors. I want Europeans to be able to make a free decision when casting their vote. To ensure this, the online anarchy of election rules must end."*

The set of measures presented today by the European Commission consists of:

- **A Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns**: Member States are encouraged to set up a national election cooperation network of relevant authorities – such as electoral, cybersecurity, data protection and law enforcement authorities – and to appoint a contact point to participate in a European-level election cooperation network. This will enable authorities to quickly detect potential threats, exchange information and ensure a swift and well-coordinated response.
- **The Commission is also recommending greater transparency in online political advertisements and targeting**. European and national political parties, foundations and campaign organisations should make available information on their expenditure on online advertising campaigns, by disclosing which party or political support group is behind online political advertisements as well as by publishing information on targeting criteria used to disseminate information to citizens. Where these principles are not followed, Member States should apply national sanctions.
- **National authorities, political parties and media should also take measures to protect their network and information systems from cybersecurity threats**, based on guidance developed by national authorities within the Network and Information Systems (NIS) cooperation group, with the EU Cybersecurity Agency and the European Commission.
- **Guidance on the application of EU data protection law**. The guidance will help national authorities and European and national political parties to apply the data protection obligations under EU law in the electoral context.The EU's General Data Protection Regulation applies since May 2018 and also covers all European and national political parties and other actors in the electoral context like data brokers and social media platforms. In light of the Cambridge Analytica case and more generally the growing impact of micro-targeting of voters based on their personal data, the Commission recalls the data protection obligations for all actors in the European elections.

- **A legislative amendment to tighten the rules on European political party funding**. The targeted change of the 2014 Regulation on party funding will make it possible to impose financial sanctions for breaching data protection rules in order to deliberately influence the outcome of the European elections. Sanctions would amount to 5% of the annual budget of the European political party or foundation concerned. The sanction will be enforced by the Authority for European political parties and European political foundations. In addition, those found to be in breach would not be able to apply for funding from the general budget of the European Union in the year in which the sanction is imposed.
- **A Regulation to pool resources and expertise in cybersecurity technology**. To keep up with the ever-evolving cyber threats, the Commission is proposing to create a Network of Cybersecurity Competence Centres to better target and coordinate available funding for cybersecurity cooperation, research and innovation. A new European Cybersecurity Competence Centre will manage cybersecurity-related financial support from the EU's budget and facilitate joint investment by the Union, Member States and industry to boost the EU's cybersecurity industry and make sure our defence systems are state-of-the-art.

The actions proposed today complement other actions carried out by the Commission, such as the entry into application of the new EU data protection rules, the wide-ranging set of measures to build strong cybersecurity in the EU currently negotiated by the European Parliament and the Council, and the ongoing efforts to tackle disinformation online.

Background

The European elections of May 2019 will take place in a very different political and legal environment compared to 2014. All actors involved in the elections, in particular Member State authorities and political parties, have to assume special responsibility to protect the democratic process from foreign interference and illegal manipulation.

The General Data Protection Regulation is directly applicable since 25 May 2018, giving the European Union the tools to address instances of unlawful use of personal data also in the electoral context.

The Parliament and the Council have agreed on amending the Act governing the elections to the European Parliament, providing for enhanced transparency for the elections of the members of the European Parliament. The Regulation on the statute and funding of European political parties and European political foundations, amended on 3 May 2018, increases the visibility, recognition, effectiveness, transparency and accountability of European political parties and European political foundations.

The European Commission also issued a Recommendation in February 2018 which highlights key steps to further enhance the efficient conduct of the 2019 elections.

Election periods have also proven to be a particularly strategic and sensitive target of hybrid threats. To this end the European Commission and the High Representative identified areas where additional steps need to be taken in June 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.

To equip Europe with the right tools to deal with cyber-attacks, the European Commission proposed in September 2017 a wide-ranging set of measures to build strong cybersecurity in the EU. This included a proposal for strengthening the EU Agency for Cybersecurity as well as a new European certification scheme to ensure that products and services in the digital world are safe to use.

The Commission has also put forward a European approach for tackling online disinformation in its Communication of 26 April 2018. This includes a self-regulatory Code of Practice for the online platforms and advertising industry as an essential step for ensuring a transparent, fair and trustworthy online campaign ahead of the European elections. The online platforms and advertising industry are expected to agree with media, academics and fact-checkers representatives on the Code of Practice on disinformation in the coming weeks and to start applying it.

For more information

Website on the 2018 State of the Union

Factsheet: Securing free and fair European elections

Commission Communication on securing free and fair European elections

Commission Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament

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

Factsheet: Protecting Europeans' personal data in elections

Proposal for amending the Regulation on funding of European political parties

Factsheet: Building strong cybersecurity in Europe

Commission Regulation proposal establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

IP/18/5681

Press contacts:

- Christian WIGAND (+32 2 296 22 53)
- Melanie VOIN (+ 32 2 295 86 59)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

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	

EUROPEAN
COMMISSION

Brussels, 12.9.2018
C(2018) 5949 final

COMMISSION RECOMMENDATION

of 12.9.2018

on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament

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

COMMISSION RECOMMENDATION

of 12.9.2018

on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament

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

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas,

(1) Article 2 of the Treaty on European Union states that the Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.

(2) The Treaties recognise the essential role played by citizens of the Union in the democratic life of the Union. Article 10 of the Treaty on European Union states that the functioning of the Union is to be founded on representative democracy, that every Union citizen has the right to participate in the democratic life of the Union and that citizens are to be directly represented at Union level in the European Parliament. It also states that political parties at European level contribute to forming European political awareness and to expressing the will of citizens of the Union.

(3) Article 14 of the Treaty on European Union states that the European Parliament is to be composed of representatives of the Union's citizens. The members of the European Parliament are to be elected for a term of five years by direct universal suffrage in a free and secret ballot. Article 22 of the Treaty on the Functioning of the European Union states that every citizen of the Union residing in a Member State of which he is not a national is to have the right to vote and to stand as a candidate at European and municipal elections in the Member State in which he resides, under the same conditions as nationals of that State.

(4) The procedure for the elections to the European Parliament is in each Member State governed by its national provisions. Political parties fulfil an essential role in a representative democracy, creating a direct link between citizens and the political system. National and regional political parties put forward candidates and organise electoral campaigns. National authorities are in charge of monitoring the elections at national level. European political parties organise complementary campaigns at European level, including those for lead candidates for the role of President of the European Commission.

(5) Enhanced transparency in elections helps citizens better to engage in the democratic process of the Union and understand European politics.

(6) The Act concerning the election of the members of the European Parliament by direct universal suffrage, annexed to Council Decision 76/787/ECSC, EEC, Euratom[1] has recently been amended[2] to provide for additional transparency in the European electoral process.

(7) Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council[3] increases the visibility, recognition, effectiveness, transparency and accountability of European political parties and European political foundations, inter alia by requiring those political parties and foundations to respect the values on which the Union is founded, in particular democracy, fundamental rights and the rule of law, both in their programmes and in their activities. Regulation (EU, Euratom) No 1141/2014 requires transparency of the relationships between political parties at national and European levels. It also establishes an independent Authority for European political parties and European political foundations for the purpose of registering, controlling and, if necessary, imposing sanctions on European political parties and European political foundations, inter alia in cases where such entities fail to respect the values on which the Union is founded.

(8) To further enhance the efficient conduct of the 2019 elections to the European Parliament, it is appropriate to make further recommendations in addition to those set out in Commission Recommendations 2013/142/EU[4] and (EU) 2018/234[5], as well as Commission Communications COM(2015) 206 final[6], COM(2018) 95 final[7] and Commission Report 2017/030[8]. In Recommendation 2013/142/EU, the Commission called on Member States to encourage and facilitate the provision of information to the electorate on the affiliation between national parties and European political parties. It also called on national political parties to make publicly known, ahead of the elections, their affiliation with European political parties. Following the 2014 elections to the European Parliament, the Commission pledged in its Communication COM(2015) 206 final to identify ways of further enhancing the European dimension and the democratic

---

1 Decision 76/787/ECSC, EEC, Euratom of the representatives of the Member States meeting in the Council relating to the Act concerning the election of the representatives of the Assembly by direct universal suffrage (OJ L 278, 8.10.1976, p. 1).

2 Council Decision (EU, Euratom) 2018/994 of 13 July 2018 amending the Act concerning the election of the members of the European Parliament by direct universal suffrage, annexed to Council Decision 76/787/ECSC, EEC, Euratom of 20 September 1976 (OJ L 178, 16.7.2018, p. 1). In accordance with Article 2 thereof, Decision (EU, Euratom) 2018/994 is subject to approval by the Member States in accordance with their respective constitutional requirements, and will enter into force on the first day after the last notification of approval is received.

3 Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations (OJ L317, 4.11.2014, p. 1).

4 Commission Recommendation 2013/142/EU of 12 March 2013 on enhancing the democratic and efficient conduct of the elections to the European Parliament (OJ L 79, 21.3.2013, p. 29).

5 Commission Recommendation (EU) 2018/234 of 14 February 2018 on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament (OJ L 45, 17.2.2018, p. 40).

6 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Report on the 2014 European Parliament elections, COM/2015/0206 final.

7 Communication from the Commission to the European Parliament, the European Council and the Council, A Europe that delivers: Institutional options for making the European Union's work more efficient, COM/2018/095 final.

8 Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening Citizens' Rights in a Union of Democratic Change EU Citizenship Report 2017, COM/2017/030 final/2.

legitimacy of the Union decision-making process, and to examine further, and seek to address, the reasons for the persistently low turnout in some Member States. In its 2017 EU Citizenship report the Commission committed to promote, in the perspective of the 2019 elections to the European Parliament, best practices which help citizens vote in and stand for those elections, to support turnout and broad democratic participation. In its Communication COM(2018) 95 final, the Commission called for greater transparency on the links between national and European political parties and for parties to make an earlier start to their campaigns than in the past. In Recommendation (EU) 2018/234, the Commission invited competent national authorities to meet in spring 2018, with the support of the Commission, to exchange best practices and practical measures to support democratic participation and high turnout at the elections to the European Parliament. The competent national authorities were further encouraged to identify, based on the experiences of Member States, best practices in the identification, mitigation and management of risks to the electoral process from cyber incidents and from disinformation.

(9) Online communication has reduced the barriers to and the costs of interacting with citizens of the Union in the electoral context. At the same time, it has increased the possibilities to target citizens, often in a non-transparent way, through political advertisements and communications, and to process personal data of citizens unlawfully in the electoral context.

(10) 2019 will be the first European Parliament elections in the changed security environment. Member States that use paper ballots for voting also rely on electronic solutions, for example for the management of electoral lists, preparation of ballot stations, voter and candidate registration, vote counting or communication of results. Cyber incidents including cyberattacks targeting electoral processes, campaigns, political party infrastructure, candidates or public authorities' systems have the potential to undermine the integrity and fairness of the electoral process and citizens' trust in elected representatives that relies on free elections.

(11) It is of key importance to fight disinformation campaigns and not allow cyber incidents which could undermine the democratic process in the Union and the values on which the Union is founded.

(12) Election periods have proven to be particularly strategic and sensitive for online circumvention of conventional ("off-line") safeguards such as the rules applicable to political communication during election periods, transparency of and limits to electoral spending, silence periods and equal treatment of candidates, as well as for the prevention of cyber-enabled attacks.

(13) The need to further enhance the transparency of paid online political advertisements and communications vis-à-vis citizens of the Union ahead of the elections to the European Parliament is particularly apparent in the light of recent events, when citizens of the Union were targeted online by political advertisements and communications, which were not transparent about their source and purpose or were represented as something else, such as news editorial or social media posts. To further improve the transparency of elections to the European Parliament, whilst at the same time increasing the accountability of political parties participating in the electoral process in the Union and voters' trust in that process, citizens of the Union should be better able to recognise paid political advertisements and communications.

(14) In its Communication of 26 April 2018[9] on online disinformation, the Commission called for the development of an ambitious Code of Practice, which should commit online platforms and the advertising industry to ensuring transparency and restricting targeting options for political advertising. To that end, the Commission has convened a multi-stakeholder Forum that is elaborating a Code of Practice, which will include concrete commitments for online platforms and the advertising sector. The April 2018 Communication also calls for a more accountable online ecosystem, to increase trust in identifiable suppliers of information and encourage more responsible behaviour online.

(15) Further transparency commitments by European and national political parties, foundations and campaign organisations acting on behalf or in cooperation with political parties, involved in political campaigns for the elections to the European Parliament should be encouraged. Complementary actions by competent authorities, European and national political parties, foundations and campaign organisations as well as online platforms and the advertising industry should strengthen transparency and protection of citizens' democratic rights.

(16) Member States should encourage such transparency, in particular by promoting active disclosure of who is behind paid online political advertisements and communications during electoral campaigns, while fully respecting freedom of expression. Transparency of the sources and amount of campaign funding for online activities during the forthcoming elections to the European Parliament campaigns should be encouraged, including, where appropriate, by rules on transparency.

(17) European and national political parties, foundations and campaign organisations should also clearly identify the origin of the messages in their paid political advertisements and communications. This should be done in such a way that the information on the origin of the message can be easily understood by the citizen and cannot be readily removed. Such transparency should be ensured for paid advertisements advocating for or against candidates as well as for online paid communications on a specific issue during the European Parliament election campaign period. Member States can draw inspiration from Directive 2010/13/EU of the European Parliament and of the Council[10] which sets out requirements on the recognisability of audio-visual commercial communications and prohibits surreptitious audio-visual commercial communications, and Directive 2005/29/EC of the European Parliament and of the Council[11], which prohibits undisclosed paid advertising to promote goods and services in editorial content.

(18) Unlawful behaviour relying on the use of online technologies and potentially affecting the integrity of the electoral process in the Union should be closely monitored by

---

9 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – "Tackling online disinformation: a European Approach", COM(2018) 236 final.

10 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in the Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, p. 1).

11 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (OJ L 149, 11.6.2005, p. 22).

competent authorities. In line with their legal orders, authorities with competence for electoral matters should reinforce their cooperation with authorities in charge of monitoring and enforcing rules relating to online activities including data protection authorities and authorities in charge of cybersecurity as well as law enforcement authorities. Establishing such national election cooperation networks should contribute to quickly detecting potential threats to the elections to the European Parliament and swiftly enforcing existing rules, including by imposing sanctions in the relevant electoral context, for instance possible financial sanctions, such as the reimbursement of the public contribution or following criminal investigations criminal penalties. The national election cooperation networks should appoint contact points to take part in a European cooperation network for elections to the European Parliament. The European cooperation network would serve to alert on threats, exchange on best practices among national networks, discuss common solutions to identified challenges and encourage common projects and exercises among national networks.

(19) The national election cooperation networks should also serve as platforms to provide alerts on potential threats, to exchange information and best practices and to liaise on the application of electoral rules in the online world and on enforcement actions.

(20) Member States should support those networks and ensure that they have the necessary means to allow a rapid and secure sharing of information.

(21) Regulation (EU) No 910/2014 of the European Parliament and of the Council[12] provides for a regulatory environment to enable secure and seamless electronic interactions between citizens and public authorities.

(22) Article 8 of the Charter of Fundamental Rights of the European Union, Article 16 of the Treaty on the Functioning of the European Union and Regulation (EU) 2016/679 of the European Parliament and of the Council[13] guarantee the protection of natural persons with regard to the processing of their personal data including when their personal data are processed in the context of elections. Regulation (EU) 2016/679 sets out the conditions applicable to the processing of personal data including lawfulness, fairness, transparency and data security. It also specifies the rights for individuals such as the right of access, rectification and deletion. Directive 2002/58/EC of the European Parliament and of the Council[14] covers unsolicited communications for direct marketing purposes, including political messages conveyed by political parties and other actors involved in the electoral process. That Directive also ensures confidentiality and protects information stored on a user's terminal equipment, such as a smartphone or computer. Regulation (EU) 2016/679 provides for the appointment of independent data protection supervisory authorities responsible for monitoring and enforcing compliance with those provisions.

---

12 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

13 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).

14 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).

(23) It should be possible to impose sanctions on political parties or political foundations that take advantage of infringements of data protection rules with a view to deliberately influencing the outcome of elections to the European Parliament. Member States should be encouraged to provide for such sanctions at national level.

(24) At the European level, the Commission is proposing amendments to Regulation (EU, Euratom) No 1141/2014 to provide for such sanctions for European Political parties and foundations.

(25) Election processes are vulnerable to hybrid threats, including on the basis of cyber-enabled attacks and the online circumvention of conventional safeguards supported by third countries. With the 13 June 2018 joint Communication on Increasing resilience and bolstering capabilities to address hybrid threats[15], the High Representative of the Union for Foreign Affairs and Security Policy and the Commission identified areas where action should be intensified in order to further deepen and strengthen the EU's essential contribution to addressing hybrid threats, including on the capacity to detect hybrid threats, strategic communication and resilience and deterrence in the cybersecurity sector. A revised action plan focusing on tackling disinformation has been requested by the European Council and is being prepared for December 2018.

(26) Experience sharing across Member States on cyber incidents is essential. Such incidents are often similar in different Member States. The September 2017 joint Communication of the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission on cybersecurity[16] acknowledges the need for a comprehensive response for building strong cybersecurity for the Union based on resilience, deterrence and defence.

(27) Directive 2013/40/EU of the European Parliament and of the Council harmonises definitions of criminal offences and minimum maximum levels of penalties in relation to attacks against information systems. Attacks against information systems that affect critical infrastructure information systems are recognised as a specific aggravating circumstance. Where attacks against information systems target electoral processes, criminal investigations that may result in the prosecution of natural or legal persons with appropriate sanctions should be considered.

(28) Directive (EU) 2016/1148 of the European Parliament and of the Council lays down measures with a view to achieving a high common level of security of network and information systems and provides for the appointment of competent authorities monitoring its application. The Directive established a computer security incident response teams network ('CSIRTs network') which promotes swift and effective operational cooperation. This network should be relied upon for the exchange of operational information on computer security incidents. In order to support and facilitate strategic cooperation and exchange of information amongst Member States, the Directive also established the Cooperation Group composed of representatives of Member States, Commission and ENISA. With a view to the 2019 elections to the European Parliament, the European Parliament called upon the Group to introduce the cybersecurity of the 2019 elections. To this end, the Cooperation Group established under Directive (EU) 2016/1148 has worked and agreed on a Compendium on Cyber

---

15 Joint Communication to the European Parliament, the European Council and the Council, Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final.

16 Joint Communication to the European Parliament, the European Council and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final.

Security of Election Technology. The Compendium provides practical guidance for cyber security authorities and election management bodies.

(29) Participation in the democratic life of the Union is a matter of common interest. Although this Recommendation focusses on elections to the European Parliament, Member States are encouraged to apply the principles of this Recommendation to other elections and referenda they organise at national level.

HAS ADOPTED THIS RECOMMENDATION:

Election cooperation networks

(1) Each Member State should set up a national election network, involving national authorities with competence for electoral matters and authorities in charge of monitoring and enforcing rules related to online activities relevant to the electoral context, in particular:

- authorities referred to in the Act concerning the election of the members of the European Parliament by direct universal suffrage;
- authorities with competence for the organisations of elections to the European Parliament;
- supervisory authorities established under Article 51 of Regulation (EU) 2016/679;
- regulatory authorities and/or bodies designated under Directive 2010/13/EU;
- competent authorities designated pursuant to Directive (EU) 2016/1148.

(2) To support each national authority in its respective tasks, the networks referred to in point (1) should facilitate the swift, secured exchange of information on issues capable of affecting the elections to the European Parliament including by jointly identifying threats and gaps, sharing findings and expertise, and liaising on the application and enforcement of relevant rules in the online environment.

(3) The networks referred to in point (1) should, whenever appropriate, in accordance with national law, consult, and cooperate with the relevant national law enforcement authorities. Where appropriate, cooperation between national law enforcement authorities at European level may be facilitated by Europol.

(4) Member States should provide the necessary support to the networks referred to in point (1) and ensure that they have the necessary means to allow a rapid and secure sharing of information.

(5) In order to facilitate the sharing of expertise and best practices among Member States including on threats, gaps and enforcement, each Member State should designate a single point of contact for the implementation of this Recommendation. The contact details of the point of contact should be communicated to the other Member States and to the Commission. Member States are encouraged to meet, with the support of the Commission, in a European coordination network on the elections to the European Parliament, as soon as possible to be able to be best prepared to protect the 2019 elections.

(6) The supervisory authorities established under Article 51 of Regulation (EU) 2016/679 should, in compliance with their obligations under with Union and national

law, immediately and proactively inform the Authority for European political parties and European political foundations[17] of any decision finding that a natural or legal person has infringed applicable rules on the protection of personal data where it follows from that decision or there are otherwise reasonable grounds to believe that the infringement is linked to political activities by a European political party or European political foundation with a view to influencing elections to the European Parliament.

Transparency in political advertising ahead of the elections to the European Parliament

(7) Member States should, in line with their applicable rules, encourage and facilitate the transparency of paid online political advertisements and communications. Member States should promote 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. Where such transparency is not ensured, Member States should apply sanctions in the relevant electoral context.

(8) European and national political parties, foundations and campaign organisations should ensure that citizens of the Union can easily recognise online paid political advertisements and communications and the party, foundation or organisation behind them.

(9) European and national political parties, foundations and campaign organisations should make available on their websites information on their 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.

(10) European and national political parties, foundations and campaign organisations should make available on their websites their paid online political advertisements and communications or links to them.

Appropriate sanctions for infringements of rules on the protection of personal data in the context of the elections to the European Parliaments

(11) Member States should apply appropriate sanctions on political parties and foundations at national and regional level for cases of infringements of rules on the protection of personal data being used to deliberately influencing or attempting to influence the elections to the European Parliament.

Cybersecurity of elections for the European Parliament

(12) Member States should take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and

---

[17] Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations (OJ L 317, 4.11.2014, p. 1–27).

information systems used for the organisation of elections to the European Parliament.

(13) Taking into account the specificities of elections to the European Parliament, Member States should apply the Compendium developed by the Cooperation Group established by Directive (EU) 2016/1148 throughout the different stages of the election process.

(14) When organising the elections to the European Parliament, Member States should adopt specific technical measures to ensure the availability, authenticity, confidentiality and integrity of election services relying on network and information systems. To guarantee the smooth running of every phase of the election, Member States should adequately protect networks and systems used for registering voter rolls and candidates; collecting, processing and counting votes; publishing and communicating election results to the wider public.

(15) European and national political parties, foundations and campaign organisations should implement specific and appropriate measures to prevent cyber incidents and protect themselves against cyberattacks.

(16) Member States should perform a comprehensive assessment of risks associated with the elections to the European Parliament with a view to identifying potential cyber incidents that could affect the integrity of the electoral process. Member States should put in place the necessary procedures to prevent, detect, manage and respond to cyberattacks, aiming to minimise their impact, and guarantee a swift exchange of information at all relevant levels, from technical to operational and political. In order to do so, Member States should make sure that national authorities with competence for electoral matters have adequate resources, including technical equipment and trained personnel, in order to deal with such incidents and in line with point (1) work in close cooperation with national competent authorities on the security of network and information systems, designated in accordance with Article 8 of Directive (EU) 2016/1148.

(17) In the event of a cyber-incident involving attacks against information systems that target the electoral process, Member States should consider an appropriate criminal law response on the basis of Directive 2013/40/EU on attacks against information systems. Member States should ensure close cooperation between national competent authorities, cybersecurity authorities and law enforcement authorities as provided for by Directive (EU) 2016/1148 and in line with point 1, where appropriate coordinated at European level by Europol.

(18) Member States should acknowledge the vulnerability of election processes to hybrid threats and should consider an appropriate response to counter the hostile activities, including the measures addressed in the 13 June 2018 joint Communication of the High Representative of the Union for Foreign Affairs and Security Policy and the Commission on Increasing resilience and bolstering capabilities to address hybrid threats.

Awareness raising activities

(19) Member States should engage with third parties, including 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.

This Recommendation is addressed to the Member States and to the European and national political parties, foundations and campaign organisations. Member States are encouraged to apply the principles of this Recommendation to other elections and referenda they organise at national level.

Done at Brussels, 12.9.2018

For the Commission
Věra JOUROVÁ
Member of the Commission

CERTIFIED COPY
For the Secretary-General,

Jordi AYET PUIGARNAU
Director of the Registry
EUROPEAN COMMISSION

EUROPEAN
COMMISSION

Brussels, 12.9.2018
COM(2018) 637 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Securing free and fair European elections

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

Securing free and fair European elections

A crucial moment for the future of the European Union

The essence of the European Union is its defence of democracy and democratic values. These are imperative for a society where pluralism and tolerance prevail, and where European citizens can vote with the security that they are not being misled. Along with the rule of law and fundamental rights, democracy is part of "who we are" and defines our Union.

The European Parliament elections of May 2019 will be held in a very different context compared to all previous elections. The political challenges to the Union and its Member States are great. There is a clear need to forge a more robust Union which can act with credibility and strength on a world stage where global powers which do not necessarily share all our interests or values are vying for power. A robust Union built on effective judicial cooperation, exchange of information to tackle terrorism and organised crime, and a smoothly functioning Internal Market all require mutual trust between Member States, and in our democratic systems. Against this unique backdrop, the European elections of May 2019 will shape the future of the European Union in the years to come.

Ensuring the resilience of the Union's democratic systems is part of the Security Union: attacks against electoral infrastructure and campaign information systems are hybrid threats that the Union needs to address. Politically motivated mass online disinformation campaigns, including by third countries, with the specific aim to discredit and delegitimise elections, have been recognised as growing threats to our democracies[1]. The European Union should take all actions within its powers to defend its democratic processes against manipulation by third countries or private interests. Election periods have proven to be periods which are particularly prone to targeted disinformation. These attacks affect the integrity and fairness of the electoral process and citizens' trust in elected representatives and as such they challenge democracy itself.

European citizens should be able to vote with a full understanding of the political choices they have. This entails more awareness of threats and more transparency in our political process. An open public sphere, secure in its protection from undue influence, ensures a level playing field for political campaigning and electoral processes the public can trust[2]. It is essential for our democracies to provide room for a vibrant political campaign which provides voters with a clear and undistorted picture of the ideas and programmes of the parties competing for their vote. Therefore fraud and other deliberate attempts to manipulate elections should be actively combatted, including through sanctions.

---

[1] See Joint Communication to the European Parliament, the European Council and the Council, Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final and European Council conclusions of 28 June 2018, (http://www.consilium.europa.eu/en/press/press-releases/2018/06/29/20180628-euco-conclusions-final/pdf).

[2] The Venice Commission of the Council of Europe provides guidance on elections (http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e), including for the media environment (http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)006-e).

Online activities, including during the election processes, are developing fast, and thus increased security and a level political playing field are key. Conventional ("off-line") electoral safeguards, such as rules applicable to political communications during election periods, transparency of and limits to electoral spending, respect for silence periods and equal treatment of candidates should also apply online[3]. Transparency about and limits on political advertisements on TV or billboards, and transparency of political advertisements should apply similarly in the online world. This is not the case now, and that needs to be remedied before the next European elections.

New challenges and recent developments

While online communication has reduced the barriers and costs for political actors to interact with citizens and offers great opportunities, it has equally increased the possibilities for malicious actors to target the democratic debate and electoral processes. The online environment can make it easier for actors to present information while concealing its origin or purpose, including by not being transparent that a communication (such as a social media post) is a paid advertisement rather than factual reporting, presenting opinion as journalism, and selectively presenting reporting to inflame tensions or polarise debate. No one should harbour any illusions about these threats; the European Union and its political systems are not immune to such threats.

In addition, the integrity of elections can be seriously affected by "conventional" cyber incidents, including cyberattacks targeting electoral processes, campaigns, political party infrastructure, candidates or public authorities' systems and by misuse of personal data. Recent revelations, including around the "Facebook/Cambridge Analytica" case, are a case in point. Personal data are believed to have been misused and given unlawfully to third parties for very different uses from those originally intended. This has highlighted the potential risks of certain online activities being used to target citizens covertly with political advertisements and communications, unlawfully processing and abusing their personal data to manipulate opinion, spread disinformation or simply undermine the truth when it suits political purposes or increases divisions[4].

---

[3] See the recent publication of the Council of Europe "Internet and electoral campaigns – Study on the use of internet in electoral campaigns" prepared by the committee of experts on media pluralism and transparency of media ownership (MSI-MED) of the Council of Europe (https://www.coe.int/en/web/human-rights-rule-of-law/-/internet-and-electoral-campaigns-a-new-study-has-been-published). The study examines the implications of the shift of electoral advertising to the internet, in particularly as regards electoral spending and advertising techniques based on micro-targeting of voters with personalised messages. See also the Council of Europe Recommendation CM/Rec(2016)5 on Internet freedom, which refers to the responsibilities of governments, platforms and intermediaries for political campaigning undertaken by political parties, candidates and other individuals online.

[4] See the interim report published by the UK Data Protection authority (ICO) following the launch of a formal investigation into the use of data analytics for political purposes after allegations were made about unlawful data processing and micro target of political adverts during the EU Referendum (https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf). The report highlights that "*rapid social and technological developments in the use of big data mean that there is limited knowledge of – or transparency around – the 'behind the scenes' data processing techniques (including algorithms, analysis, data matching and profiling) being used by organisations and businesses to micro-target individuals. What is clear is that these tools can have a significant impact on people's privacy. It*

Supporting free and fair elections in Europe

European institutions do not run elections. Action in this context remains primarily a responsibility of the Member States. Member States are responsible for the organisation of elections and for monitoring the conduct of the election process[5]. Nevertheless, there is an obvious Union dimension. By putting forward candidates for elections to the European Parliament, national and regional political parties are primary players in the European electoral campaigns. European political parties and their associated foundations have an important function in organising complementary campaigns at European level, including campaigns for the lead candidates for the role of President of the European Commission.

Following the 2014 elections to the European Parliament, the Commission had pledged in its 2015 post-election report[6] to identify ways of further enhancing the European dimension and the democratic legitimacy of the Union decision-making process, and to examine further, and seek to address, the reasons for the persistently low turnout in some Member States. In February 2018, the Commission called for early and ongoing engagement with citizens in debates on European issues, an earlier start to political parties' campaigns for the elections to the European Parliament, including those of their candidates for President of the European Commission, more transparency about the links between national and European political parties and the promotion by Member States of the right to vote, in particular for underrepresented groups.

The European Union has also already taken some important steps to build democratic resilience in Europe, including with the new European data protection framework in place since May this year. This General Data Protection Regulation, which became directly applicable across the European Union, provides the tools necessary to address instances of unlawful use of personal data in the electoral context. Work is also ongoing to promote a more secure online environment by increasing our overall resilience to cyber threats, including online disinformation and behavioural manipulation.

It is important to have as much clarity as possible on how to implement the European data protection rules in this new context, while similarly we need to scale up our efforts to increase awareness, transparency, and security. Citizens should be able to discern who is speaking to them online through advertising and political messages, and who is paying for political advertisements or political messages. Guidance on how to implement the new data protection rules in the context of the European elections should contribute to more clarity and a better understanding, as more cooperation and exchange of information between competent authorities, and with others contribute to more security.

---

is important that there is greater and genuine transparency about the use of such techniques to ensure that people have control over their own data and that the law is upheld. When the purpose for using these techniques is related to the democratic process, the case for high standards of transparency is very strong". The importance of better integrating data protection considerations into the wider regulatory framework governing elections is also highlighted.

[5] Within the framework of EU law and their international obligations.

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Report on the 2014 European Parliament elections (COM(2015) 206 final).

The package for bolstering democratic resilience presented together with this Communication comprises balanced, comprehensive and targeted actions to support the integrity and effective conduct of the 2019 elections to the European Parliament. This is a joint responsibility of all actors involved in the electoral process. It requires constant vigilance and flexible adaptation to a dynamic environment and new technological developments. By providing for guidance, recommendations and necessary tools European and national political parties, national governments, authorities, private entities and stakeholders, can all work together with greater clarity in creating a more secure democratic environment and on a level playing field.

Member States are also encouraged to apply the principles to other elections and referenda they organise at national level.

The measures proposed in this package aim at:

1. Providing specific guidance regarding the processing of personal data in elections;
2. Recommending best practices for addressing risks from disinformation and cyberattacks and promoting online transparency and accountability in the EU electoral process; and enhancing cooperation between competent authorities, and putting the tools in place to allow them to intervene and as necessary introduce sanctions to safeguard the integrity of the electoral process.
3. Addressing situations in which political parties or associated foundations benefit from practices infringing data protection rules, with a view to deliberately influencing or attempting to influence the outcome of European elections.

In bringing forward this package, the Commission has taken care to avoid unnecessary administrative burdens and inappropriately limiting the margin of manoeuvre for European, regional and national political parties and foundations.

1. Current EU defences to protect free and fair elections

The Union has already taken important steps to protect the integrity of elections and to strengthen the democratic process.

With the General Data Protection Regulation (GDPR)[7] directly applicable across the Union since 25 May 2018, the European Union is now fully equipped to help prevent and address cases of unlawful use of personal data. As such the European Union is a standard setter in this area.

Furthermore, the act concerning the election of the members of the European Parliament has been amended recently, including to provide for additional transparency in the European

[7] 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).

electoral process[8]. The revised Regulation on the statute and funding of European political parties[9], adopted on 3 May 2018, increases the recognition, effectiveness, transparency and accountability of European political parties and European political foundations. Commission Recommendation (EU) 2018/234[10] highlights key steps to further enhance the efficient conduct of the 2019 elections to the European Parliament.

Directive 2002/58/EC of the European Parliament and of the Council (Directive on privacy and electronic communications[11]) applies to unsolicited communications for direct marketing purposes, including political messages conveyed by political parties and other actors involved in the political process. It also ensures confidentiality and protects information stored on a user's terminal equipment, such as a smartphone or computer[12]. The proposed Regulation on Privacy and Electronic Communications[13], currently under negotiation, will further strengthen citizens' control by enhancing transparency and widen the scope of protection beyond traditional telecom operators to include internet-based electronic communication services.

In addition, the Commission has recently put forward a European approach for tackling online disinformation in its Communication of 26 April 2018[14]. Through this Communication the Commission seeks to promote a more transparent, trustworthy and accountable online environment. One of its key deliverables is the development of an ambitious **Code of Practice on Disinformation** which notably should commit online platforms and the advertising industry to ensuring transparency and restricting targeting options for political advertising.[15] The Code is expected to be published in September 2018[16] and should produce measurable results by October.

More specifically, signatories of the Code of Practice should agree to deprive "impostor" websites and websites hosting disinformation of advertising revenues and ensure transparency about sponsored content, in particular political and issue-based advertising, establish clear

---

[8] Council Decision (EU, Euratom) 2018/994 of 13 July 2018 amending the Act concerning the election of the members of the European Parliament by direct universal suffrage, annexed to Council Decision 76/787/ECSC, EEC, Euratom of 20 September 1976 (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018D0994&qid=1531826494620).

[9] Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations, (OJ L 317, 4.11.2014, p.1).

[10] Commission Recommendation (EU) 2018/234 of 14 February 2018 on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament (OJ L 45, 17.2.2018, p. 40).

[11] 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).

[12] User consent is required before websites can access such information or track a user's online behaviour, such as by storing cookies on the user's device.

[13] 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.

[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tacking online disinformation: a European Approach (COM(2018) 236 final).

[15] To prepare this Code of Practice, the Commission convened a Forum in May 2018, which consists of a "Working Group" (composed of the major online platforms and representatives of the advertising industry and major advertisers) and a "Sounding Board" (composed of representatives of the media and civil society).

[16] After the Sounding Board has issued its opinion.

marking systems and rules for bots[17] to ensure that their activities cannot be confused with human interactions and intensify efforts to close fake accounts. The signatories should also agree to facilitate user assessment of content by encouraging the development of indicators of trustworthiness of content sources, dilute the visibility of disinformation by improving the findability of trustworthy content and provide users information on prioritisation of content by algorithms. Further, signatories should provide trusted fact-checking organisations and academia with access to platform data. An assessment of the Code of Practice will be part of the work towards an action plan with specific proposals for a coordinated EU response to the challenge of disinformation, to be presented by the Commission and the High Representative before the end of the year.

As far as more "traditional" cyber incidents are concerned, such as hacking into IT systems or defacing websites, definitions of offences and minimum maximum levels of penalties for attacks against information system have been harmonised at European Union level by Directive 2013/40/EU on Attacks against information systems.

The Cooperation Group established under Directive (EU) 2016/1148 of the European Parliament and of the Council[18], has identified cybersecurity of elections as a common challenge. This Cooperation Group, which comprises the national competent authorities responsible for cybersecurity, the Commission, and the European Union Agency for Network and Information Security ('ENISA') has mapped existing national initiatives on cybersecurity of network and information systems used for elections. It has identified risks associated with an insufficient level of cybersecurity potentially affecting the next elections to the European Parliament and has drawn up a Compendium on Cyber Security of Election Technology, including technical and organisation measures based on experiences and best practices. The Compendium provides practical guidance for cyber security authorities and election management bodies.

2. Further bolstering democratic resilience: enhancing cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament

Given the magnitude of the challenge, and since formal responsibilities in this field are shared between multiple authorities, meaningful results will only be achieved if all the relevant actors work together.

This Communication is accompanied by a Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting

[17] Bots include automated posting on social media platforms and more interactive applications such as chatbots, which interact directly with users.

[18] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

disinformation campaigns in the context of elections to the European Parliament. In order to ensure free and fair elections this Recommendation should be implemented by all actors in good time for the 2019 elections to the European Parliament.

In the Recommendation, we encourage each Member State to establish and support a national elections network. Member States authorities with competences in electoral matters should cooperate with authorities in connected fields (such as data protection authorities, media regulators, cyber security authorities etc.) timely and effectively. Where necessary, they should also engage with law enforcement authorities. This will enable them quickly to detect potential threats to the elections to the European Parliament and swiftly enforce existing rules, including available financial sanctions, such as reimbursement of the public contribution. EU and national legislation must be respected and enforced. In this perspective, the Commission calls upon Member States to promote, in compliance with the applicable national and Union law, the sharing of information by data protection authorities to authorities in charge of monitoring elections and the monitoring of political parties' activities and financing where it follows from their decisions, or where there are otherwise reasonable grounds to believe, that an infringement is linked to political activities by national political parties or foundations in the context of elections to the European Parliament.

It is also recommended that Member States appoint contact points to take part in a European cooperation network for elections to the European Parliament. The Commission will support these cooperation networks by convening a first meeting of the designated contact points by January 2019. While respecting the national competences and the procedural requirements applicable to the concerned authorities, this forum will provide the nucleus for a real time European alert process and a forum for exchange of information and practices among Member State authorities.

Political parties, foundations and campaign organisations need to guarantee transparent practices in their political communications to citizens and to ensure that the European electoral process is not distorted by unfair practices. The Commission presents concrete measures to strengthen transparency so that citizens can see who is behind the political communication they receive and who is paying for it[19]. Member States should support and facilitate such transparency and the efforts of competent authorities in monitoring breaches and enforcing rules including by applying sanctions where necessary. Where relevant, law enforcement authorities should also be involved to ensure an appropriate response to incidents and the application of appropriate penalties[20].

[19] These proposals are complementary to the Code of Practice being elaborated by the multi-stakeholder Forum convened by the Commission following its Communication of 26 April 2018 on online disinformation.

[20] This would concern in particular cases where an election process is targeted with malicious intent, including incidents based on attacks against information systems. Depending on the circumstances, criminal investigations that may result in criminal penalties may be appropriate. As noted above, definitions of offences and minimum maximum levels of penalties for attacks against information system have been harmonised by Directive 2013/40/EU.

Resilience, deterrence and defence are essential to building strong cybersecurity for the European Union[21]. Competent European and national authorities, political parties, foundations and campaign organisations should be fully aware of the risks for next year's elections and deploy appropriate efforts to protect their network and information systems[22].

3. Applying data protection rules in the electoral process

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)[23], 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.

Since it is the very 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 for all actors involved in election processes – such as national electoral authorities, political parties, data brokers and analysts, social media platforms and online ad networks – to understand clearly how best to apply these rules and what is and is not allowed by them.

The Commission has thus prepared specific guidance to highlight the data protection obligations of relevance in the electoral context. In order to combat malicious attempts to abuse people's personal data, in particular for micro-targeting purposes, 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.

4. Strengthening the rules on funding of European political parties

Political parties and foundations are of course the key actors in elections. They compete for the vote of the electorate through their campaigns. To ensure a level political playing field, and to protect all political parties and foundations from malfeasance it is essential to prevent

[21] The September 2017 joint Communication of the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission acknowledges the need for a comprehensive response for building strong cybersecurity for the Union that is based on resilience, deterrence and defence, JOIN(2017) 450 final.

[22] The Compendium developed by the Cooperation Group established under Directive (EU) 2016/1148 provides useful guidance in this respect. Directive (EU) 2016/1148 aims at achieving a high common level of cybersecurity resilience across the Union. In order to meet this objective, the Directive supports the development of national cybersecurity capabilities and protects the provision of essential services in key sectors. In order to reinforce the efforts towards a proper implementation of the Directive, the Commission is providing over EUR 50 million in funding until 2020 through the Connecting Europe Facility (CEF) programme. The risk management measures of the Directive (EU) 2016/1148 are relevant benchmarks for the electoral process. The GDPR also provides for obligations to implement appropriate technical and organisational measures to ensure a level of security to personal data being processed. It is applicable to all actors involved in the electoral process and also contains an obligation to communicate personal data breaches to the competent data protection authorities and to the concerned individuals (see guidance issued by the Commission).

[23] 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).

situations in which any one party can benefit from illegal practices infringing data protection rules. For these who do not only breach people's privacy, they could also potentially influence the outcome of elections to the European Parliament, should be sanctioned. Alongside a call for Member States to apply such sanctions for parties and foundations at national level where appropriate, the Commission is proposing to introduce a targeted amendment to Regulation (EU, Euratom) No 1141/2014 to provide for proportionate sanctions in cases involving European-level political parties and foundations. That amendment, which reinforces existing rules, aims to ensure that the elections to the European Parliament can be held under strong democratic rules and in full respect for the values on which the Union is founded, in particular democracy, fundamental rights and the rule of law.

The Commission urges the European Parliament and the Council to ensure that those focused changes are in place before the 2019 elections to the European Parliament.

5. Conclusions

Recent events have shown that the risks of manipulation of the electoral process, whether via attacks on information systems, misuse of personal data and opaque practices, are real and acute. The EU is not immune. Online activities in the electoral context present a novel threat and require specific protection. We serve the citizens and democracy best by preparing now. We cannot wait until after elections or referenda have taken place to discover such activities and respond to them only then.

Protecting democracy in the Union is a shared and solemn responsibility of the European Union and its Member States. It is also a matter of urgency. All involved actors have to step up their efforts and cooperate to deter, prevent and sanction malicious interference in the electoral system. The measures put forward by the Commission in this package support these efforts.

The Commission will report after the 2019 elections to the European Parliament on the implementation of this package of measures.

Next steps ahead of the 2019 elections to the European Parliament

- *The Commission urges the European Parliament and the Council to ensure that the proposed targeted changes to Regulation (EU, Euratom) No 1141/2014 are in place in time for the 2019 elections to the European Parliament.*

- *Together with the High Representative, the Commission will be supporting the preparation of common European responses addressing any foreign involvement in elections in the European Union*[24]*. As a follow up on the European Council Conclusions of June 2018, they will present in cooperation with Member States an action plan by December 2018 with specific proposals for a coordinated EU response to the challenge of disinformation.*

- *The Commission will raise awareness and maintain its dialogue with Member States' authorities through the high-level conference on cyber-enabled threats to elections on 15 and 16 October 2018, the outcome of which will feed into the next Colloquium on Fundamental Rights (26 and 27 November 2018), focused on "Democracy in the European Union".*

[24] This could also include the use of measures developed under the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.

EUROPEAN
COMMISSION

Brussels, 12.9.2018
COM(2018) 636 final/2

2018/0336 (COD)

CORRIGENDUM

This document corrects document COM(2018) 636 final of 12.9.2018

Concerns English, French and German language versions

Correction of the Procedure number

The text shall read as follows:

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

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

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Democracy is one of the fundamental values on which the European Union is founded. To ensure the functioning of a representative democracy at the European level, the Treaties determine that the citizens of the European Union are directly represented in the European Parliament.

Political parties fulfil an essential role in a representative democracy, creating a direct link between citizens and the political system, thereby enhancing the legitimacy of the system. According to Article 10 of the Treaty on European Union, "political parties at European level contribute to forming European political awareness and to expressing the will of citizens of the Union". Article 12(2) of the Charter of Fundamental Rights of the European Union expresses the same principle.

In February 2018, the Commission issued a Recommendation[1] on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament, addressed to Member States and to European and national political parties. It included calls on European political parties and national parties to increase transparency on their respective affiliation and links and called on those political parties to help raise citizens' awareness on the issues at stake at Union level and on how they intend to address them during the upcoming legislature.

In the EU, data protection is a fundamental right and the General Data Protection Regulation[2] sets strong rules to protect this fundamental right. In particular, personal data must be processed lawfully and fairly.

Online communication has the potential of allowing closer and direct interaction between political actors and European citizens. At the same, it brings an increased risk of unlawfully processing personal data of citizens in the electoral context. A number of recent events show that abuses of data protection rules can affect the democratic debate and free elections, including elections to the European Parliament.

In 2018, the Facebook/Cambridge Analytica case concerning the alleged unlawful processing of user personal data acquired from Facebook by the company Cambridge Analytica raised serious concerns on the impact of data protection infringements on electoral processes. Investigations are ongoing in relation to this particular case, *inter alia* by the UK Information Commissioner's Office, the data protection supervisory authority which is leading the European investigation in cooperation with other European data protection supervisory authorities. The Commission is in close contact with the data protection supervisory authorities and is following this process closely. The U.S. Federal Trade Commission has opened an investigation in the case. A series of hearings took place in the European Parliament on the case and its impact on individuals' personal data in the Union.

Regulation No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations[3] was introduced to increase the visibility, recognition, effectiveness, transparency and accountability of European political parties and their affiliated political foundations. In the light of this Regulation,

---

1 Commission Recommendation (EU) 2018/234 of 14 February 2018 on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament (OJ L 45, 17.2.2018, p. 40).

2 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).

3 OJ L 317, 4.11.2014, p. 1.

European political parties and foundations satisfying a number of conditions were offered the opportunity to become European legal entities by registering at European level, thereby obtaining access to European financial support. These conditions include the respect, both in their programme and activities, of the values on which EU is founded – listed in Article 2 of the Treaty on European Union: respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights including the rights of people belonging to minorities. An independent Authority for European political parties and foundations ("the Authority") was created, for the purpose of registering, monitoring and, if necessary, imposing sanctions on European political parties and foundations, including to consider cases where such entities allegedly fail to respect these fundamental European values.

However, the existing rules do not allow to effectively dissuade and sanction abuses of data protection rules which may affect the democratic debate and free elections.

In order to ensure that the elections to the European Parliament take place under strong democratic rules and in full respect of the European values of democracy, rule of law and respect of fundamental rights, the Commission is proposing a targeted amendment to Regulation No 1141/2014. It aims to allow financial sanctions on European political parties or foundations that use infringements of data protection rules to deliberately influence or attempt to influence the outcome of elections to the European Parliament.

The proposal will also enable the Authority to operate in a smooth and effective manner, by ensuring that it has its own allocation of staff and that its Director becomes the appointing authority. This should allow the Authority to fully fulfil its tasks, including the new ones foreseen in this proposal, and to do so in an independent way. In parallel, in order to respond to the calls of the Authority for an increased number of staff and in view of the Authority's key role in the period closely preceding the elections to the European Parliament, the Commission is ready to immediately make available the 6 additional staff requested by the Authority, on a detachment basis, which will end once the permanent staffing arrangements would be in place.

The procedure for the elections to the European Parliament is in each Member State governed by its national provisions. Political parties fulfil an essential role in a representative democracy, creating a direct link between citizens and the political system. National and regional political parties put forward candidates and organise electoral campaigns. National authorities are in charge of monitoring the elections at national level. European political parties organise complementary campaigns at European level, including those for lead candidates for the role of President of the European Commission.

The amending Regulation, together with the Commission guidance on the application of Union data protection law in the electoral context[4], the Commission Recommendation on election cooperation networks, online transparency and protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament[5] and a Commission Communication on Securing free and fair European elections[6] adopted on the same day, forms part of a security package. It is a contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018.

The Recommendation encourages data protection supervisory authorities in compliance with applicable Union and national law, to inform immediately and proactively the Authority for European political parties and European political foundations of their decisions finding that a European political party, a European political foundation or another natural or legal person has

---

4 COM (2018) 638.
5 C (2018) 5949.
6 COM (2018) 637.

infringed applicable rules on protection of personal data. This information should be provided where it follows from that decision, or where there are otherwise reasonable grounds to believe, that the infringement is linked to political activities by a European political party or European political foundation in the context of elections to the European Parliament. The Recommendation also encourages Member States to apply appropriate sanctions on political parties and foundations at national and regional level for cases of infringements of rules on the protection of personal data being used with a view to influencing or attempting to influence the elections to the European Parliament.

The focused changes to Regulation No 1141/2014 should be in place before the 2019 elections to the European Parliament.

- **Consistency with other Union policies**

Since 25 May 2018, the General Data Protection Regulation[7] applies in all EU Member States. It sets high data protection standards that are fit for the digital economy and make organisations processing data – including European political parties and the European political foundations – more accountable and more responsible in how they deal with personal data.

In its Recommendation of 14 February 2018[8] on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament, the Commission called on the competent national authorities to identify best practices in the identification, mitigation and management of risks to the electoral process form cyber-attacks and disinformation. In April 2018, the Commission organised a meeting with the electoral commissions of Member States to discuss, exchange best practices and raise awareness among national authorities of the issues of security, disinformation campaigns and the enforcement of electoral rules online.

In April 2018, the Commission published a Communication on "Tackling online disinformation"[9], which defined the roles and responsibilities of relevant stakeholders and formulated a set of actions, including strengthening the Commission's strategic communications response to disinformation.

This proposal is consistent with the Commission's proposal[10] for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (e-Privacy Regulation) that reviews the existing e-privacy Directive[11] which will enhance transparency and widen the scope of protection beyond traditional telecom operators to include internet-based electronic communication services and which should be promptly adopted by the co-legislators.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The proposal is based on Article 224 of the Treaty on the Functioning of the European Union, which states that "*the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the regulations governing political parties at*

---

7 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).

8 Commission Recommendation (EU) 2018/234 of 14 February 2018 on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament (OJ L 45 of 17 February 2018, p. 40).

9 COM(2018) 235 final.

10 COM (2017) 10 final.

11 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).

European level referred to in Article 10(4) of the Treaty on European Union and in particular the rules regarding their funding" as well as on Article 106a of the Treaty establishing the European Atomic Energy Community[12].

- **Subsidiarity**

Since the existing Regulation provides for an EU-level system, including a specific European legal personality for parties and foundations and funding from the EU budget, any shortcomings in this system can only be remedied through EU legislation. Action by Member States alone is therefore not a relevant option.

The proposed focused changes therefore fully comply with the principle of subsidiarity. The EU level is the only one at which rules governing the statute and funding of European political parties and European political foundations can be laid down. In setting out possible reform measures, the Commission has been careful to reflect the principles contained in Protocol No. 2 to the Treaties.

- **Proportionality**

As explained in Section 5, the targeted measures proposed do not go beyond what is necessary to achieve the long-term objective of developing and strengthening European democracy and the legitimacy of the EU Institutions.

The proposal complies with the principle of proportionality. The proposed sanctions are built on the regime set by Regulation 1141/2014, establishing proportionate sanctions. The proposed measures ensure that there is no double penalisation of the same behaviour: infringements of data protection rules will be penalised by the competent data protection supervisory authorities established by the General Data Protection Regulation. The behaviour sanctioned by this proposal is the taking advantage of infringements of data protection rules to deliberately influence or to attempt to influence the elections to the European Parliament. The Authority will not impose sanctions on infringements of data protection rules as such.

- **Choice of the instrument**

Only a Regulation can amend an existing Regulation.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

In preparing the current proposal, the Commission took into account the calls expressed during the debates and hearings in the European Parliament regarding the Facebook/Cambridge Analytica case, which concerned allegations of use of Facebook' users' data by Cambridge Analytica and its impact on the protection of individual's personal data in the Union (hearings of 4 June 2018, 25 June 2018 and 2 July 2018).

Such debates and hearings brought to light that the use of misleading and manipulative techniques of micro targeting, aiming at unfairly influencing the result of polls, are closely connected to the question of illegal transfer and processing of personal data. EU rules already ensure the effective protection of personal data.

- **Impact assessment**

[12] https://europa.eu/european-union/sites/europaeu/files/docs/body/consolidated_version_of_the_treaty_establishing_the_european_atomic_energy_community_en.pdf

This proposal is not accompanied by a specific impact assessment. It is not expected to have wider significant economic, social and environmental impacts. The proposed changes build on the existing verification and sanctions regimes established by Regulation No 1141/2014.

- **Fundamental rights**

Article 2 of the Treaty on European Union (TEU) provides that "*The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.*"

Article 10(1) and (2) TEU provide that "*The functioning of the Union shall be founded on representative democracy*" and that "*Citizens are directly represented at Union level in the European Parliament*". Subparagraph 4 of the same provision stipulates: "*political parties at European level contribute to forming European political awareness and to expressing the will of citizens of the Union*". Articles 11 and 12 of the Charter of Fundamental Rights of the EU enshrine the right to freedom of expression and of association. Article 7 of the Charter of Fundamental Rights of the European Union reads that *"Everyone has the right to respect for his or her private and family life, home and communications*". Article 8 of the Charter of Fundamental Rights of the European Union reads that *"(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."*

The amendments which are the subject of this proposal pursue the objectives of these provisions, and are compatible with and give effect to the fundamental rights guaranteed by Articles 7, 8 and 12 of the Charter.

4. BUDGETARY IMPLICATIONS

In order for this proposal to be effective, as it adds tasks to the Authority, there needs to be a more permanent staffing arrangement for the Authority. The budgetary implications are detailed in the Legislative Financial Statement attached to this proposal. More permanent staffing provisions should be made through the redeployment of existing resources, and will require the modification of the establishment plans of the contributing Institutions. Therefore, these elements should be included in the forthcoming Amending Letter to Draft Budget 2019. Given the size of the Authority, a separate establishment plan in not necessary, but a footnote detailing the size and nature of the staffing shall be entered in the Section I – European Parliament.

5. OTHER ELEMENTS

- **Detailed explanation of the specific provisions of the proposal**

In order to sanction financially European political parties or foundations using infringements of data protection rules to deliberately influence or attempt to influence the outcome of elections to the European Parliament, the Commission proposes the following targeted changes to the Regulation:

It is proposed to create a verification procedure related to infringements of rules on the protection of personal data which would require the Authority to trigger an opinion of the committee of independent eminent persons, shortly after a decision by a competent data protection supervisory authority. The committee's opinion – to be delivered within a short deadline set by the Authority –

would assess whether such infringement was used to deliberately influence or attempt to influence the outcome of elections to the European Parliament. The triggering of this new procedure does not prevent the triggering of the procedure of verification of compliance with registration conditions and requirements set out in the Article 10 of the Regulation for cases of manifest and serious breaches by the European political parties or foundations of the values on which the Union is founded. The new procedure would be introduced by the insertion of a new Article 10a.

To ensure such procedure can be triggered at any moment, including close to the date of elections to the European Parliament, it is proposed to clarify that the time limitations of the procedure of verification of compliance with registration conditions and requirements set in Article 10 do not apply to it, by amending the third sub-paragraph of Article 10(3).

Article 11, on the committee of independent eminent persons, will be amended to expressly refer to the opinion on the influencing of the outcome of elections to the European Parliament.

A new ground for financial sanctions will be added in Article 27 in the case the opinion of the committee of independent eminent persons finds that a European political party or a foundation has deliberately influenced or attempted to influence the outcome of elections of the European Parliament by taking advantage of an infringement of the applicable rules on protection of personal data.

This new ground will be added to the list of infringements which prevent a European political party or foundation to apply for funding from the general budget of the European Union in the year when the sanction was imposed. This will be done by amending Article 18.

Since the new verification procedure is triggered by a decision of a competent data protection supervisory authority, it is proposed to allow for the review of the sanction if the competent data protection supervisory authority's decision is repealed or where a remedy against such decision has been successful, by adding a new paragraph in Article 27.

Finally, in order to enable the Authority to operate in an independent and effective manner, the Commission is proposing the Authority to be staffed in a permanent way and to confer the powers of an appointing authority on the Director of the Authority, by amending paragraph 5 of Article 6.

2018/0336 (COD)

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

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 224 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular, Article 106a thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[13],

Having regard to the opinion of the Committee of the Regions[14],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Regulation (EU, Euratom) No 1141/2014[15] established a specific European legal status for European political parties and European political foundations and provides for their funding from the general budget of the European Union, it also establishes an Authority for European political parties and European political foundations ("the Authority").

(2) In order to enable the Authority to fully fulfil its tasks, including the new ones foreseen in this Regulation, and to do so in an independent manner, it is necessary to staff it in a permanent way and to confer the powers of an appointing authority on the Director of the Authority.

(3) Recent events have demonstrated the potential risks to electoral processes and democracy that can arise from the unlawful use of personal data. It is therefore necessary to protect the integrity of the European democratic process by providing for financial sanctions in situations where European political parties and European political foundations take

---

13 OJ C , , p. .

14 OJ C , , p. .

15 Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations (OJ L317, 4.11.2014, p. 1).

advantage of infringements of data protection rules with a view to influencing the outcome of elections to the European Parliament.

(4) To that end, a verification procedure should be established whereby the Authority must, in certain circumstances, ask the committee of independent eminent persons to assess whether a European political party or a European political foundation has deliberately influenced or attempted to influence the outcome of elections to the European Parliament by taking advantage of an infringement of the applicable rules on protection of personal data. Where the committee finds that to be the case, the Authority should impose sanctions in line with the effective, proportionate and dissuasive sanctioning system established by the Regulation (EU, Euratom) No 1141/2014.

(5) The new procedure should exist alongside the current procedures used for verification of compliance with registration conditions and in cases of manifest and serious breaches of the values on which the Union is founded. However, the time limits for verification of compliance with registration conditions and requirements set in Article 10 of Regulation (EU, Euratom) No 1141/2014 should not apply to the new procedure.

(6) Since the new procedure is triggered by a decision of a competent data protection supervisory authority, it should be possible for the European political party or European political foundation concerned to request that the sanction be reviewed if the decision of the supervisory authority is repealed or a remedy against that decision is successful.

(7) In order to ensure that the 2019 elections to the European Parliament take place under strong democratic rules and in full respect of the European values of democracy, rule of law and respect of fundamental rights it is important that the proposed verification procedure enters into force in timely manner and is applicable as soon as possible. In order to achieve this the proposed amendments to Regulation (EU, Euratom) No 1141/2014 introduced by this Regulation should enter into force on a date of its publication in the *Official Journal of the European Union*.

(8) Regulation (EU, Euratom) No 1141/2014 should therefore be amended accordingly,

HAVE ADOPTED THIS REGULATION:

Article 1

Regulation (EU, Euratom) No 1141/2014 is amended as follows:

(1) Article 6(5) is replaced by the following:

'The Director of the Authority shall be assisted by staff, with respect to which he shall exercise the powers conferred by the Staff Regulations on the appointing authority and by the Conditions of Employment of Other Servants on the authority empowered to conclude a contract of employment of other servants ('the appointing authority powers').[16] The Authority may make use in any areas of its work of other seconded national experts or other staff not employed by the Authority.

---

16 Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community, (OJ P 045 14.6.1962, p. 1385)

The Staff Regulations and the Conditions of Employment of Other Servants and the rules adopted by agreement between the institutions of the Union for giving effect to those Staff Regulations and the Conditions of Employment of Other Servants shall apply to the staff of the Authority.'

(2) In Article 10(3) the following sentence is added at the end of the third subparagraph:

"That time limitation shall not apply with regard to the procedure set out in Article 10a.";

(3) the following Article 10a is inserted:

"Article 10a

Verification procedure related to infringements of rules on the protection of personal data

If the Authority becomes aware of a decision of a supervisory authority within the meaning of point 21 of Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council[17] finding that a natural or legal person has infringed applicable rules on the protection of personal data and if it follows from that decision, or where there are otherwise reasonable grounds to believe, that the infringement is linked to political activities by a European political party or a European political foundation in the context of elections to the European Parliament, the Authority shall refer this matter to the committee of independent eminent persons established by Article 11. The committee shall give an opinion as to whether the European political party or the European political foundation concerned has deliberately influenced or attempted to influence the outcome of elections to the European Parliament by taking advantage of that infringement. The Authority shall request the opinion without undue delay and no later than 1 month after the decision of the supervisory authority. The committee shall deliver its opinion within a short, reasonable deadline set by the Authority.

The procedure set out in this Article is without prejudice to the procedure set in Article 10.";

(4) in Article 11(3), the second sentence of the first subparagraph is replaced by the following:

"When requested by the Authority, the committee shall give an opinion on whether a European political party or a European political foundation has deliberately influenced or attempted to influence the outcome of elections to the European Parliament by taking advantage of an infringement of the applicable rules on the protection of personal data. In both cases the committee may request any relevant document and evidence from the Authority, the European Parliament, the European political party or European political foundation concerned, other political parties, political foundations or other stakeholders, and it may request to hear their representatives. In the case of opinions on whether a European political party or a European political foundation has deliberately influenced or attempted to influence the outcome of elections to the European Parliament by taking advantage of an infringement of the applicable rules on the protection of personal data, the supervisory authorities referred to in the Article 10(a) shall cooperate with the committee in accordance with applicable law."

(5) in Article 18(2), the words "and in point (a) (v) and (vi) of Article 27(2)" are replaced by the words" and in point (a) (v), (vi) and (vii) of Article 27(2)";

(6) Article 27 is amended as follows:

(a) in point (a) of paragraph (2), the following point (vii) is added:

---

17 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).

"(vii) where, in accordance with Article 10a, the committee issues an opinion finding that a European political party or a European political foundation has deliberately influenced or attempted to influence the outcome of elections to the European Parliament by taking advantage of an infringement of the applicable rules on the protection of personal data.";

(b) the following paragraph 7 is added:

"7. Where a decision of the supervisory authority as referred to in Article 10a has been repealed or where a remedy against such decision has been successful, the Authority shall review any sanction imposed pursuant to point (a)(vii) of paragraph 2 at the request of the European political party or European political foundation concerned."

Article 2

This Regulation shall enter into force on the day of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned in the ABM/ABB structure

1.3. Nature of the proposal/initiative

1.4. Objective(s)

1.5. Grounds for the proposal/initiative

1.6. Duration and financial impact

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

3.2.2. Estimated impact on operational appropriations

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

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

1.2. Policy area(s) concerned

Fundamental rights

1.3. The proposal relates to

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[18]

X **the extension of an existing action**

☐ **a merger of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

Recent events have demonstrated the potential risks to electoral processes and democracy that can arise from the unlawful use of personal data. It is therefore necessary to protect the integrity of the European democratic process by providing for financial sanctions in situations where European political parties and European political foundations take advantage of infringements of data protection rules with a view to influencing the outcome of elections to the European Parliament.

1.4.2. Specific objective(s)

A verification procedure should be established whereby the Authority established by Article 6 of Regulation (EU, Euratom) No 1141/2014 ("the Authority") must, in certain circumstances, ask the committee of independent eminent persons to assess whether a European political party or a European political foundation has deliberately influenced or attempted to influence the outcome of elections to the European Parliament by taking advantage of an infringement of the applicable rules on protection of personal data. Where the committee finds that to be the case, the Authority should impose sanctions in line with the effective, proportionate and dissuasive sanctioning system established by the Regulation (EU, Euratom) No 1141/2014.

It is necessary that the Authority has sufficent resources fully to complete its tasks, both those provided for by the existing Regulation (EU, Euratom) No 1141/2014 and the new ones envisaged by the present amending proposal. This requires stable staffing and strengthening of the human resources currently provided to the Authority.

1.4.3. .Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

[18] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

The proposal aims to deter European political parties and foundations from making use of the results of infringements of data protection rules with a view to deliberately influencing the outcome of elections to the European Parliament by providing for financial sanctions for any such improper behaviour.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Sanctions should be imposed in good time on any European political party or foundation found to have taken advantage of infringements of data protection rules with a view to deliberately influencing the outcome of elections to the European Parliament.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The above-mentioned sanctions regime should be in place well before the elections to the European Parliament of 2019 in order to deter the improper actions decribed. To make this operational, and to ensure the Authority is fully equipped effectively to manage all its task, additional human resources should be provided as soon as practicable, and in the first instance through the redeployment of resources carrying out these tasks prior to the creation of the Authority.

To simplify and provide greater independence for its operations, the powers of the appointing authority under the Staff Regulations and the Conditions of Employment of Other Servants [Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1)] should be delegated to the Director of the Authority.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

This proposal concerns the system for European political parties and European political foundations established at European level. Pursuant to Regulation (EU, Euratom) No 1141/2014, these are bodies with European legal personality. The Authority is also a body with legal personality under Union law. It is therefore only via action at Union level that the objectives described above can be pursued.

The proposal will have achieved its goals if either (a) the proposed sanctions regime deters any European political party or foundation from improperly using the results of infringements of rules on protection of personal data or (b) any such acts that do take place are duly sanctioned.

The Authority should be in a position to fully undertake all its duties, in particular in the run-up and aftermath of the European electoral period of 2019.

1.5.3. Lessons learned from similar experiences in the past

The Authority's first annual report, for 2017, states that "The APPF [the Authority] currently comprises two full-time employees and the Director. More precisely, in November 2016, the European Parliament seconded an administrative assistant to support the Director in setting up the APPF and the registration process of EU parties and

foundations. In June 2017, a legal advisor joined the APPF to provide advice on procedural, substantive and financial matters. At this stage, the entirety of the staff of the APPF is provided by the European Parliament. The current number of staff is insufficient for the APPF to properly carry out the tasks conferred on it by Regulation (EU, Euratom) No 1141/2014. Moreover, that lack of staff is also capable of affecting the independence and business continuity of the APPF."

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The present proposal would not imply any change to the ceiling of administrative spending for the Union institutions provided for in the Multiannaul Financial Framework.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The proposed increase in staffing for the Authority will be met first and foremost by redeployment of existing resources.

1.6. Duration and financial impact

☐ Proposal/initiative of **limited duration**

– ☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY

X unlimited duration

– Implementation with a start-up period from YYYY to YYYY,

– followed by full-scale operation.

1.7. Management mode(s) planned[19]

X Direct management by the European Parliament through the Authority

– ☐ executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

☐ international organisations and their agencies (to be specified);

☐the EIB and the European Investment Fund;

☐ bodies referred to in Articles 70 and 71;

☐ public law bodies;

☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

[19] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Comments

The Authority is financed from a specific budget title (Title 5) of the European Parliament. The number and composition of the staff shall be indicated in the budgetary remarks of the specific title. The duties of the Authorising Officer of the European Parliament are delegated to the Director of the Authority according to point 7 of Article 6 of Regulation (EU, Euratom) No 1141/2014.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Authority will continue to issue an annual activity report under Article 10 of Regulation (EU, Euratom) No 1141/2014. The European Parliament will report on the financial operations involved as part of the Union's annual accouting cycle.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

Given the specific set-up of the Authority (an independent body, but whose budget is part of the budget of the European Parliament) the steps proposed are the only logical ones in the light of the requirments set out above.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

The financial risks are the same as for any other part of the adminsitrative expenditure of the Union institutions and in this case would be covered by the existing internal control system of the European Parliament.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

No new internal control system is proposed and the additional burden of these changes to the European Parliament's internal control system are not significant.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

The European Parliament's existing provisions for its administrative expenditure would apply to that set out here.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[20]	from EFTA countries [21]	from candidate countries[22]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
5	Section I – European Parliament	Diff./Non-diff.	NO	NO	NO	NO

20 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

21 EFTA: European Free Trade Association.

22 Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

Heading of multiannual financial framework	**5**	'Administrative expenditure'

EUR million (to three decimal places)

		Year N	Year N+1	Year N+2	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
European Parliament									
• Human Resources		1.43	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**10.01**
• Other administrative expenditure									
TOTAL European Parliament	Appropriations	1.43	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**10.01**

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)	1.43	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**10.01**

EUR million (to three decimal places)

		Year N[23]	Year N+1	Year N+2	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	1.43	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**10.01**
	Payments	1.43	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**10.01**

[23] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

3.2.2. Estimated impact on [body]'s appropriations

– X The proposal/initiative does not require the use of operational appropriations

– ☐ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year N		Year N+1		Year N+2		Year N+3		Enter as many years as necessary to show the duration of the impact (see point 1.6)						**TOTAL**	
	OUTPUTS																	
	Type[24]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[25]…																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTAL COST																		

24 Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

25 As described in point 1.4.2. 'Specific objective(s)…'

3.2.3. *Estimated impact on the Authority's human resources*

The resources set our below are the same ones as set out in section 3.2.1 above; they are repeated here for the sake of clarity that all the resources concerned are for the Authority.

3.2.3.1. Summary

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– X The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year N [26]	Year N+1	Year N+2	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
Officials/Temporary Agents (AD Grades)	0.715	0.715	0.715	0.715	0.715	0.715	0.715	0.715
Officials/Temporary agents (AST grades)	0.715	0.715	0.715	0.715	0.715	0.715	0.715	0.715
Contract staff								
Seconded National Experts								
TOTAL	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**1.43**	**10.01**

Staff requirements (FTE):

	Year N [27]	Year N+1	Year N+2	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
Officials/Temporary Agents (AD Grades)	5	5	5	5	5	5	**5**	**5**
Officials/Temporary agents (AST grades)	5	5	5	5	5	5	**5**	**5**
Contract staff								
Seconded National Experts								

[26] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

[27] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

TOTAL	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**70**

The human resources required will be met by staff from the Institutions who are already assigned to management of the action and/or have been redeployed within the Institution, together if necessary with any additional allocation which may be granted to the managing Institution under the annual budget procedure and in the light of budgetary constraints.

3.2.4. Compatibility with the current multiannual financial framework

– X The proposal/initiative is compatible the current multiannual financial framework.

– ☐ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts.
[…]

– ☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[28].

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.
[…]

3.2.5. Third-party contributions

– The proposal/initiative does not provide for co-financing by third parties.

[28] See Articles 11 and 17 of Council Regulation (EU, Euratom) No 1311/2013 laying down the multiannual financial framework for the years 2014-2020.

3.3. Estimated impact on revenue

– X The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

☐ on own resources

☐ on other revenue

☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[29]						
		Year N	Year N+1	Year N+2	Year N+3	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article								

For miscellaneous 'assigned' revenue, specify the budget expenditure line(s) affected.

[...]

Specify the method for calculating the impact on revenue.

[...]

[29] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.