



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 10/2018 on the Commission Package on free and fair European elections



The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 ‘With respect to the processing of personal data... for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by the Union institutions and bodies’, and under Article 52(3)‘...for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data’.

Under Article 57(1)(g) of Regulation 2018/1725, the EDPS shall ‘advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons’ rights and freedoms with regard to the processing of personal data’.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and to foster accountable policymaking in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. It provides for several recommendations in relation to the proposed Regulation in order to further improve the articulation between data protection legal framework on the one hand and the purpose of this initiative on the other hand.

Executive Summary

The functioning of the Union is founded on representative democracy. Political communication is essential to the participation of citizens, political forces and candidates in democratic life and to the fundamental right to freedom of expression. These rights and freedoms are interdependent with the right to respect for private and family life, home and communications and the right the protection of personal data. Earlier this year, in his Opinion 3/2018 on online manipulation, the EDPS highlighted the risks to fundamental rights of concentrated markets.

In the context of the 2018 State of the Union speech, the Commission presented a security package focusing on Free and fair European elections. This package is composed of a Communication, a Guidance document on the application of Union data protection law in the electoral context, a Recommendation and a proposal for a Regulation 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. The EDPS recognises the reference made to the role of social media platforms and on how this initiative would be coherent with the Code of Practice on online disinformation. In light of the upcoming European Parliament elections in May next year, and the numerous other national elections scheduled for 2019, the EDPS also recognises the recommendations for the setting up of national election networks and a European coordination network. He takes this opportunity to show his availability to participate in this European network. It would complement EDPS action in this area, in particular the workshop which he organises in February next year. The EDPS also recognises the recommendation to Member States to 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 and underlines the urgency of this matter.

In general, the EDPS considers that, for further clarity, a reference could have been included to the processing of personal data by the European Parliament, the Authority for European political parties and European political foundations and the Committee of independent persons, as being within the scope of Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (previously, Regulation 45/2001). In addition and more specifically, the EDPS makes several recommendations in relation to the proposed Regulation, among which clarifying the scope of the measures and the complementary aims of such sanctions, including EDPS decisions finding an infringement to Regulation 2018/1725 and a reference to the current data protection legal framework for cooperation between national data protection supervisory authorities and the EDPS as well as ensuring the confidentiality of the exchange of information in the context of the cooperation between data protection supervisory authorities and the Committee of independent persons.

TABLE OF CONTENTS

| | |
|--|-----------|
| 1. Introduction and background | 5 |
| 2. Comments..... | 7 |
| 2.1. General Comments..... | 7 |
| 2.2. Comments on the Proposed Regulation | 9 |
| 2.3. Comments on the Recommendation | 10 |
| 2.4. Comments on the Guidance | 12 |
| 3. Conclusion | 13 |
| Notes | 14 |

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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)¹,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC², and in particular Articles 42(1), 57(1)(g) and 58(3)(c) thereof,

Having regard to Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA³,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction and background

1. In the context of the 2018 State of the Union speech, the Commission presented on 12 September 2018 a security package focusing on Free and fair European elections. It is composed of a legislative proposal accompanied by 3 non-legislative measures:
 - a **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** (COM (2018) 636 final/2) (hereafter the '*proposed Regulation*');
 - a **Communication on Securing free and fair European elections** (COM (2018) 637 final) (hereafter the '*Communication*');
 - a **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** (C (2018) 5949 final) (hereafter the '*Recommendation*') and
 - a **Guidance on the application of Union data protection law in the electoral context** (COM (2018) 638 final) (hereafter the '*Guidance*').
2. This package has been adopted with a view of securing fair and free elections to the European Parliament to be held in May 2019, taking into account the new challenges put forward by online communication and recent revelations such as the “Facebook/Cambridge Analytica” case⁴. It is presented together with a proposal for a Regulation of the European parliament and of the Council establishing the European Cybersecurity Industrial,

Technology and Research Competence Centre and the Network of National Coordination Centres (COM(2018) 630 final)⁵.

3. It is complementary to the Commission Communication of 26 April 2018 “Tackling online disinformation: a European approach” (COM/2018/236 final), which seeks to promote a more transparent, trustworthy and accountable online environment. One of its key deliverables, the self-regulatory Code of Practice on Disinformation, was published on 26 September 2018. The Commission has also published the opinion of the Sounding board of the Multi-stakeholder forum on the Code of Practice⁶. The actions foreseen in this Communication, including this Code of Practice, complement the ongoing work of the EEAS. Following the European Council conclusions of 28 June 2018⁷, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy will present in cooperation with Member States a revised action plan to fight disinformation, by the end of the year⁸.
4. The **proposed Regulation** “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”⁹. In addition to financial penalties which could be imposed on European political parties or foundations, of 5% of their annual budget¹⁰, a new ground would “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”¹¹. In its **Recommendation**, the Commission encourages national data protection supervisory authorities established under the General Data Protection Regulation (hereafter the ‘GDPR’) to inform immediately and proactively the Authority for European political parties and European political foundations (hereafter the ‘Authority’)¹² of their decisions finding an infringement of data protection rules, where the infringement is linked to political activities by a European political party or foundation “with a view to influencing elections to the European Parliament”¹³. The Commission also recommends, for cases involving political parties or foundations at national and regional level, Member States to “apply appropriate sanctions”¹⁴.
5. In addition, the **Recommendation** encourages the establishment of **a national election network in each Member State as well as a European coordination network on the elections to European Parliament**¹⁵. The latter is a follow up to the first exchange organised by the Commission between EU countries on electoral best practices in April 2018. It would be composed of national contact points and should meet in January and April 2019¹⁶. It is planned as a real time European alert process and as a forum for exchange of information. The national networks would inter alia aim at exchanging information on issues capable of affecting the European elections, between national authorities with competence for electoral matters and for cybersecurity as well as national data protection authorities and national audio-visual regulatory authorities or bodies. It is recommended that these national networks consult and cooperate with the relevant national law enforcement authorities in accordance with national law¹⁷ and that where appropriate, cooperation between national law enforcement authorities at European level may be facilitated by Europol. According to the Commission, “[t]his 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”¹⁸.
6. The Commission finally presents several recommendations¹⁹ to facilitate **transparency in political advertising** ahead of the elections to the European Parliament and encourages Member States to take appropriate **measures in the area of cybersecurity** of the European Parliament electoral process and to engage in **awareness raising activities** with third

parties, including online platforms and information technology providers, for better transparency and trust building in the electoral process.

7. The **Guidance** highlights the existing Union data protection framework and its application in the **electoral context**. According to the Commission, since it is the first time that the GDPR will be applied in the European electoral context, it is important for all actors involved in election processes to understand clearly how best to apply these rules. The Commission underlines that the national data protection authorities “*have to make full use of their strengthened powers to address possible infringements*”²⁰.
8. On 18 October 2018, the European Council called for measures to “*protect the Union's democratic systems and combat disinformation, including in the context of the upcoming European elections, in full respect of fundamental rights. In this respect, the measures proposed by the Commission on election cooperation networks, online transparency, protection against cybersecurity incidents, unlawful data manipulation and fighting disinformation campaigns and tightening the rules on European political party funding deserve rapid examination and operational follow-up by the competent authorities*²¹”.
9. On 25 October 2018, the European Parliament adopted a resolution recalling “*the measures proposed by the Commission for securing free and fair European elections, in particular the legislative amendment to tighten up the rules on European political party funding, creating the possibility to impose financial sanctions for breaching data protection rules in order to deliberately influence the outcome of the European elections*” and that “*the processing of personal data by political parties in the EU is subject to the GDPR, and that the breach of the principles, rights and obligations encompassed within this law would result in additional fines and sanctions*”. The resolution considers that “*election interference to be a huge risk for democracy, the tackling of which requires a joint effort involving service providers, regulators and political actors and parties*” and welcomes this Commission package²². On 3 December 2018, the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament adopted its opinion on the proposed Regulation²³. On 6 December 2018, the Committee on Constitutional Affairs adopted its report on the proposed Regulation²⁴.
10. The European Data Protection Supervisor (hereafter the ‘EDPS’) welcomes the informal consultation by the Commission on the proposed Regulation, the Recommendation and the Guidance prior to their adoption and the fact that part of his informal comments were taken into account. He underlines however that due to the short notice, these were preliminary comments. Therefore, he makes the following formal comments. In this regard, he would like to recall that, when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, as it is the case here, the Commission shall consult the EDPS.

2. Comments

2.1. General Comments

11. The EDPS **recognises political communication** as essential to the participation of citizens, political forces and candidates in democratic life and to the fundamental right to freedom of expression, and that these rights and freedoms are interdependent with the right under Article 7 of the Charter of Fundamental Rights of the European Union (hereafter the ‘*Charter*’) to respect for private and family life, home and communications, and the right under Article 8 of the Charter to the protection of personal data.
12. Article 2 of the Treaty on European Union (hereafter the ‘*TEU*’) provides that “[t]he 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.” According to Article 10(4) TEU, “[p]olitical 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 expresses the same principle. Article 3 of Protocol I to the European Convention of Human Rights guarantees everyone a right to free election. Freedom, fairness and transparency are recognised as key principles of democratic elections²⁵. In the EU context, Article 10(1) and (2) TEU provide that “[t]he functioning of the Union shall be founded on representative democracy” and that “[c]itizens are directly represented at Union level in the European Parliament”. Article 39 of the Charter guarantees the right to vote in European Parliament elections. The **principle of electoral transparency** would appear to be compromised where the voters have no freedom to seek, receive and impart information about the process and the candidates, including about the source and spending of financial support received by a candidate or a party²⁶. Article 11 of the Charter contains the requirement for the **freedom and pluralism of the media** to be respected. The Resolution of the European Parliament on media pluralism and media freedom in the European Union adopted on 3 May 2018 referred to the “concentration of power of media conglomerates, platform operators and internet intermediaries and media control by economic corporations and political actors risk[ing] causing negative consequences for the pluralism of public debate and access to information (...)"²⁷. The EDPS and most recently the EDPB have also highlighted the risks to fundamental rights of concentrated markets²⁸. Data protection supervisory authorities have underlined the **importance of the use of personal data for political communication** within the framework of the International Conference of Data Protection and Privacy Commissioners²⁹. In this context, the EDPS would like to recall that according to Recital 56 GDPR “[w]here 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.”

13. Against this background, the EDPS recognises the direct reference made, in particular in the Communication and the Guidance, **to the role of social media platforms** and on how the initiative would be coherent with the Code of Practice on online disinformation³⁰. He also takes note that the assessment of the code “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”³¹. Political advertisements are increasingly targeted on the basis of large scale personal data processing, profiling and algorithmic decision making for which social media platforms in question are accountable under the GDPR and other relevant regulation. The EDPS would like therefore to reiterate its support for a swift adoption of a new ePrivacy Regulation³² with the ambition to provide a high level of protection with respect to both content and metadata and the objective of extending the confidentiality obligations to a broader range of services - including the so-called ‘over the top’ services (OTTs) - which reflects the progress of technology³³.
14. Also, for purpose of clarity, the initiative could have included a reference to the processing of personal data by the Authority, the European Parliament and the Committee of independent eminent persons as being within the scope of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC)

No 45/2001 and Decision No 1247/2002/EC Text with EEA relevance (see Article 33 of Regulation No 1141/2014³⁴).

2.2. Comments on the proposed Regulation

15. The explanatory memorandum to the proposed Regulation states that “*existing rules do not allow to effectively dissuade and sanction abuses of data protection rules which may affect the democratic debate and free elections*”. The aim of the proposed amendments is therefore to financially sanction “*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*”³⁵. The proposed Regulation creates a verification procedure related to infringements of rules on the protection of personal data, whereby:
 - 1) without undue delay and no later than 1 month after the decision of a data protection supervisory authority within the meaning of point 21 of Article 4 GDPR “*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 request the opinion of the Committee of independent eminent persons (hereafter the ‘Committee’)³⁶;
 - 2) “*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*”³⁷.
 - 3) where the opinion of the Committee finds 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*”, the Authority shall impose financial sanctions³⁸.
16. The EDPS understands that such mechanism is supposed to be complementary to the sanctions, and in particular to the administrative fines, that national data protection supervisory authorities are entitled to impose under the GDPR. According to the explanatory memorandum of the proposed Regulation, “*there is no double penalisation of the same behaviour*” as 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*”³⁹.
17. In this regard, the EDPS considers that the proposed Regulation would benefit from further **clarification of the scope of the measures** taken. In other words, bearing in mind the competences of data protection supervisory authorities under the GDPR and the *ne bis in idem* principle enshrined in Article 50 of the Charter as interpreted by the Court of Justice of the European Union⁴⁰, the body of the proposed Regulation should be very clear, as it seems *prima facie* from the proposed Regulation, that **the Authority would not impose sanctions for infringements of the GDPR as such**. The Committee and the Authority should of course not be expected to undertake a new and separate assessment of the infringement of the GDPR which has already been determined by the competent data protection supervisory authorities defined in Article 4 (21) GDPR. It should be clear that the Committee and the Authority build on the assessment of the data protection supervisory

authority on the infringement of the GDPR and the scope of the measure taken by the Authority should be limited to sanctioning an unlawful conduct consisting in the breach of the one or more provisions of Regulation No 1141/2014 for which it is competent (e.g. electoral fraud or manipulation), which, under the proposed Regulation, would include a breach achieved by means of the infringement of data protection rules.

18. In that respect, **the proposed Regulation could clarify the legal rules (e.g. Regulation No 1141/2014 and not the GDPR) whose infringement would be sanctioned by the Authority and the complementary aims of such sanction.**
19. Also **the link between this new provision and Article 33(8)** of Regulation No 1141/2014 could be clarified⁴¹.
20. According to the proposed Regulation, the Authority shall refer the matter to the Committee only where a decision has been issued by a national data protection supervisory authority finding an infringement of data protection law and that, either “*it follows from that decision (...) that the infringement is linked to political activities by a European party or foundation*” or “*there are otherwise reasonable grounds to believe the infringement is linked to political activities*”⁴². **We would suggest clarifying whether the ‘reasonable grounds’ for believing an infringement is linked to political activities are to be determined solely by the Authority or also potentially in cooperation with the data protection supervisory authority.**
21. Moreover, this new procedure would give rise to a **new sharing of information** by the national data protection supervisory authorities with the Committee⁴³. For instance, the Committee might need, to adopt a meaningful opinion, to access preliminary or interim investigation reports of data protection authorities. The EDPS welcomes the fact that the proposed Regulation provides that such cooperation shall take place “*in accordance with applicable law*”. Due to the sensitivity of the matter, it is of utmost importance to ensure the confidentiality of such exchange of information. He notes however that such cooperation between the **Committee and the national data protection authorities is not covered by Article 28 of Regulation No 1141/2014, which specifically provides for an agreement with the Member States “on practical arrangements for (...) exchange of information, including the rules regarding the disclosure of confidential information or evidence”**. This provision does not concern the cooperation with the Committee. **The EDPS recommends therefore to also amend that provision so that Member States and the Committee shall conclude such practical arrangements as well.**
22. Furthermore, the implementation of the new procedure would in some cases require a **cooperation between the national data protection supervisory authorities and the EDPS** to facilitate the gathering of evidence proving an infringement of the GDPR. **The EDPS recommends that a short reference be made to the current Data Protection legal framework for such cooperation.**
23. Finally, the EDPS observes that as it stands, the proposed Regulation would not cover **cases of infringements of Regulation (EU) 2018/1725**, as the latter falls under the supervision of the EDPS and not of the national data protection supervisory authorities under the GDPR. In order to fully achieve the objectives of the proposed Regulation, the EDPS therefore recommends to **include EDPS decisions finding such infringement together with the aforementioned safeguards as to the cooperation with the Committee in the framework of this new procedure.**

2.3. Comments on the Recommendation

24. The EDPS **recognises the recommendation for the setting up of national election networks**. He also recognises the recommendation for the **European coordination**

network on the elections to the European Parliament which should take place with the support of the Commission. **The EDPS takes this opportunity to show his availability to participate, either as member or as an observer, in this network.**

25. The EDPS has for several years argued for greater collaboration between data protection authorities and other regulators to safeguard the rights and interests of individuals in the digital society. In particular, given the concentrated nature of digital markets and the pivotal role of a very small number of major platforms in mediating and targeting political advertisements in recent years, the EDPS has recommended that **competition authorities**, who are responsible for determining cases of alleged abuse of dominance and proposed mergers, and **consumer protection authorities** concerned with the transparency and fairness of the terms of use of online services, be integrated into this dialogue⁴⁴. Such an initiative would contribute to the enforcement of the data protection rules -especially the GDPR- with rigour and in tandem with other norms for elections and media pluralism and would complement EDPS action in this area, in particular the **workshop which will take place early next year** between national regulators in the area of data protection, electoral and audio-visual law⁴⁵.
26. The EDPS takes note of **recommendation (6) which aims at encouraging national supervisory authorities under the GDPR to cooperate with the Authority**. The Recommendation, while not binding, implies a new task for national supervisory authorities under the GDPR to systematically assess whether it follows from their decision or whether there are otherwise ‘reasonable grounds’ to believe that the data protection law infringement found in their decision is linked to political activities by a European political party or European political foundation with a view to influencing elections to the European Parliament and to immediately and proactively inform the Authority. As mentioned above for the proposed Regulation, the EDPS underlines that such cooperation may only take place in accordance with the national data protection supervisory authorities’ obligations under the applicable legal framework and therefore, welcomes the fact that the Recommendation specifies that the national supervisory authorities under the GDPR should cooperate “*in compliance with their obligations under (...) Union and national law*”.
27. **With regard to cybersecurity**, the Recommendation emphasizes existing principles laid down in the NIS Directive (EU) 2016/1148⁴⁶ and the eID Regulation (EU) 910/2014⁴⁷. The security requirements of these instruments are complemented by the relevant provisions on the security of personal data laid down in the GDPR. The EDPS therefore recognises that national competent authorities designated according to the NIS Directive shall be part of the recommended national election networks.
28. The EDPS **takes note of the attention given to the network and information security considering all information systems used for the organisation of elections** (recommendation (12)). He underlines that such systems play a central role, even when no electronic voting tools are offered to voters. The management of voter lists, preparation of ballot stations, registration of nominated candidates, lists and parties, aggregation and compilation of voting results and subsequent processes usually rely on information systems and complex networks of such systems. Alleged or real attacks on the integrity, confidentiality or availability of such systems and networks may be used to undermine the credibility and put in doubt the legitimacy of the vote, even if no actual damage has been achieved.
29. Stakes and risks are much higher when the actual voting process is carried out by electronic means, at ballot stations or even more where any form of online voting is used. Widespread electronic voting systems used in third countries and the EU have been found to suffer from

significant vulnerabilities. The complexity of such systems, caused inter alia by the apparently contradictory objectives of keeping the votes secret and ensuring the possibility to verify the correctness of the voting results, makes it difficult or impossible to explain the integrity of such systems to many citizens so that they may have the same level of confidence and transparency as it is possible with paper ballots. **The risk that real attacks or false claims of such attacks undermine the confidence in the election appears higher than in traditional paper ballot systems.** Even availability problems, such as temporary interruptions of the voting process due to small technical faults may cause some voters to lose the possibility to exercise their fundamental right or increase fears about manipulations.

30. On this background, the EDPS **recognises the recommendation to Member States to 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”**(recommendation (16)). In view of the complexity of this task and the subsequent implementation of appropriate technical and organisational measures, and the short time left until the elections, **the EDPS underlines the urgency of this matter and of launching the process without further delay.**

2.4. Comments on the Guidance

31. The EDPS **takes note of the Guidance** which aims at providing specific guidance regarding the processing of personal data in elections to European but also national political parties, national governments, authorities, private entities and stakeholders⁴⁸.
32. In general, while regretting that the Guidance lacks concrete examples of good practices, the EDPS welcomes the reference made to some of the rules or guidelines on data processing for political purposes developed by national data protection authorities and which contain such concrete examples of good practices⁴⁹.
33. The EDPS welcomes also the reference made, **under point 1 on the Union data protection framework**, to the **supervisory powers**, including the possible sanctions in case of infringement, as it is key for the actors concerned to be aware of the supervision process which is in place and of the possible sanctions in case of infringement of data protection law.
34. In addition, the EDPS recognises the fact that, **under point 2.1. on Data controllers and processors**, the need to undertake a case-by-case assessment of each situation is underlined and the fact that it is referred to the case where candidates run for election independently of any political party. Such candidates are the controllers of the data processed for the electoral campaign they are running for. However, the various scenarios possible for data controllers and data processors could have been further detailed: in particular, political parties and foundations are likely to be considered controllers, or joint controllers alongside the platforms, such as social media providers, used to target political messages⁵⁰. Data brokers and data analytics companies are more likely to be considered processors. Within an electoral process, these entities should only process data on behalf of data controllers and not act as such. Further guidance may be found in the Opinion 1/2010 of the Article 29 Data Protection Working Party on the concepts of “controller” and “processor”⁵¹.
35. Finally, the EDPS welcomes the reference made, **under points 2.3 on the transparency requirements and 2.4. on profiling, automated decision-making and micro-targeting**, with regard to social media platforms, to the **rights of the data subject** under the GDPR to information about data processing and to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

3. Conclusion

36. The EDPS recognises political communication as essential to the participation of citizens, political forces and candidates in democratic life and to the fundamental right to freedom of expression, and that these rights and freedoms are interdependent with the right under Article 7 of the Charter to respect for private and family life, home and communications, and the right under Article 8 of the Charter to the protection of personal data.
37. He recognises the reference made, in particular in the Communication and the Guidance, to the role of social media platforms and on how this initiative would be coherent with the Code of Practice on online disinformation.
38. In light of the upcoming European Parliament elections in May next year, and the numerous other national elections scheduled for 2019, the EDPS also recognises the recommendations for the setting up of national election networks and a European coordination network. He takes this opportunity to show his availability to participate in this European network. It would complement EDPS action in this area, in particular the workshop which he organises in February next year.
39. The EDPS also recognises the recommendation to Member States to 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 and underlines the urgency of this matter.
40. In general, the EDPS considers that, for further clarity, a reference could have been included to the processing of personal data by the European Parliament, the Authority and the Committee, as being within the scope of Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (previously, Regulation 45/2001).
41. In addition and more specifically, the EDPS makes several recommendations in relation to the proposed Regulation, among which:
 - clarifying the scope of the measures and the complementary aims of such sanctions;
 - including EDPS decisions finding an infringement to Regulation 2018/1725;
 - including a reference to the current data protection legal framework for cooperation between national data protection supervisory authorities and the EDPS; and
 - ensuring the confidentiality of the exchange of information in the context of the cooperation between data protection supervisory authorities and the Committee of independent persons.

Brussels,

(signed)

Giovanni BUTTARELLI

Notes

¹ OJ L 119, 4.5.2016, p. 1.

² OJ L 295, 21.11.2018, p. 39.

³ OJ L 119, 4.5.2016, p. 89.

⁴ Communication, p. 2.

⁵ http://europa.eu/rapid/press-release_IP-18-5681_en.htm

⁶ The Code and its Annex as well as the opinion of the Sounding board are available at: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

⁷ Available at: <https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf>.

⁸ Communication, p. 10.

⁹ Explanatory memorandum to the proposed Regulation, p. 2.

¹⁰ See Article 27(4) (a) of Regulation No 1141/2014 and the Commission factsheet on free and fair European elections available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf.

¹¹ Explanatory memorandum to the proposed Regulation, p. 6.

¹² This Authority was established under Regulation No 1141/2014 (Article 6).

¹³ Recommendation 6. Also, in its Communication, p. 7, the Commission “*calls also upon Member States to promote, in compliance with the applicable national and Union law, the sharing of information by the national data protection authorities to the authorities in charge of monitoring elections and 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*”. Emphasis added.

¹⁴ Recommendation 11.

¹⁵ Recommendations 1 to 5 included.

¹⁶ Communication, p. 7 and the Commission factsheet on free and fair European elections available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf.

¹⁷ Communication, footnote 20: “[t]his 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”.

¹⁸ Communication, p. 7.

¹⁹ Recommendations 7 to 10 included and 12 to 19 included.

²⁰ Communication, p. 8, point 3 “Applying Data protection rules in the electoral process”.

²¹ Conclusions available at: <https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf>.

²² See points 10 to 12 of the Resolution on the use of Facebook users’ data by Cambridge Analytica and the impact on data protection P8_TA-PROV(2018)0433 (2018/2855(RSP)), available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0433+0+DOC+PDF+V0//EN>, emphasis added.

²³ Available at: <http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-630.530&format=PDF&language=EN&secondRef=02>

²⁴ Available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2018-0435+0+DOC+PDF+V0//EN>

²⁵ [http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2010\)037-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2010)037-e)

European Commission for Democracy through Law (Venice Commission), ‘Report on the timeline and inventory of political criteria for assessing an election’ p. 4 and 5, Study no. 558/2009, Strasbourg, 21.10.2010.

²⁶ http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%202019%20-%20The%20new%20political%20campaigning_final.pdf

London School of Economic, Media Policy Brief 19 ‘The New Political Campaigning’ p.6. March 2017.

²⁷ See European Parliament resolution of 3 May 2018 on media pluralism and media freedom in the European Union P8_TA(2018)0204 (2017/2209(INI)), point S, available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0204+0+DOC+PDF+V0//EN>.

²⁸ EDPS Opinion 3/2018 on online manipulation and personal data and EDPB Statement the data protection impacts of economic concentration adopted on 27 August 2018.

²⁹ Resolution on the Use of Personal Data for Political Communication, Montreux (Switzerland), 14th to 16th September 2005.

³⁰ Communication, pp. 2 and 5 and the Guidance, point 2.4.

³¹ Communication, p. 6.

³² 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, 2017/0003 (COD).

³³ See EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) and his blog available at https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en.

³⁴ 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).

³⁵ Explanatory memorandum, p.2.

³⁶ Article 1(3) of the proposed Regulation introducing a new Article 10a. The Committee was established by Regulation No 1141/2014 (Article 11). See also Recital 4 of the proposed Regulation.

³⁷ Article 1(4) of the proposed Regulation introducing a second sentence to Article 11(3) subparagraph 1 of Regulation No 1141/2014.

³⁸ Article (6)(a) of the proposed Regulation introducing a new point (vii) to Article 27(2)(a) of Regulation No 1141/2014.

³⁹ Explanatory memorandum, p.4.

⁴⁰ See in particular points 40 and following of the Judgment of the Court (Grand Chamber) of 20 March 2018, Garlsson Real Estate SA v. Commissione Nazionale per le Società e la Borsa (Consob), C-537/16, ECLI:EU:C:2018:193, whereby the Court stated that "*the fact that the imposition of that criminal penalty depends on an additional constituent element in relation to the administrative fine of a criminal nature is not, in itself, capable of calling into question the identity of the material facts at issue. Subject to verification by the referring court, the administrative fine of a criminal nature and the criminal proceedings at issue in the main proceedings appear therefore to relate to the same offence*" and that "*a limitation to the ne bis in idem principle guaranteed by Article 50 of the Charter may be justified on the basis of Article 52(1) thereof*".

⁴¹ Article 33(8) of Regulation No 1141/2014 provides that "*European political parties and European political foundations, the Member States and the independent bodies or experts authorised to audit accounts under this Regulation shall be liable in accordance with applicable national law for any damage they cause in the processing of personal data pursuant to this Regulation. The Member States shall ensure that effective, proportionate and dissuasive sanctions are applied for infringements of this Regulation, of Directive 95/46/EC and of the national provisions adopted pursuant thereto, and in particular for the fraudulent use of personal data*".

⁴² Article 1(3) of the proposed Regulation.

⁴³ Article 1(4) of the proposed Regulation amending Article 11 of Regulation No 1141/2014.

⁴⁴ EDPS Opinion on online manipulation and personal data, p. 19. See also the Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy adopted on 23 October 2018 by the International Conference of Data Protection and Privacy Commissioners, available at: https://icdppc.org/wp-content/uploads/2018/10/20180918_ICDPPC-40th_DCCW-Resolution_ADOPTED.pdf

⁴⁵ EDPS Opinion 3/2018 on online manipulation and personal data, p. 22.

⁴⁶ 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.

⁴⁷ 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.

⁴⁸ Communication, p. 4.

⁴⁹ See footnote 1 referring to the report issued in July 2018 by the Information Commissioner's Office (ICO) summarising the policy findings from the investigation it conducted into the use of data analytics for political purposes, with a particular focus on the EU referendum campaign and the use of social media and footnote 3 referring to the rules adopted by the Italian Data Protection Authority in March 2014, the additional guidelines

provided by the French National Data Protection Commission (CNIL) in November 2016 to its 2012 recommendations on political communication, specifying the rules for processing of personal data on social networks and the Guidance on political campaigning published by ICO.

⁵⁰ See Judgment of the Court of Justice of the European Union (Grand Chamber) of 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, ECLI:EU:C:2018:388.

⁵¹ Opinion 00264/10/EN, WP 169, available in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, to be updated in the light of the GDPR in a near future.