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