Council of the European Union

Brussels, 21 September 2018
(OR. en)

12405/18

AG 24
INST 338
PE 116
DATAPROTECT 190

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	12 September 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2018) 637 final
Subject:	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*

Delegations will find attached document COM(2018) 637 final.

Encl.: COM(2018) 637 final

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.