ЦЕНТРАЛНА ИЗБИРАТЕЛНА КОМИСИЯ

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

GUIDELINES ON THE PROCESSING AND PROTECTION OF PERSONAL DATA IN THE ELECTION PROCESS

adopted jointly by the Central Electoral Commission and the Commission for Personal Data Protection pursuant to Article 57(1)(49) of the Election Code

PROCESSING OF PERSONAL DATA IN THE ELECTION PROCESS

I. GENERAL PROVISIONS

Since May 25th 2018, the new data protection rules have been implemented in the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) lays down the obligations and requirements for all public bodies, private entities and natural persons — data controllers — with regard to the protection and processing of personal data.

The General Regulation recognises that for the purpose of the election process, including during election campaigns, the political parties, competent bodies and other entities that compile personal data about the political views of data subjects, which is considered sensitive by default and therefore subject to more stringent protection requirements. For this reason, the current Guidelines aim to provide guidance to all actors in the election process in respect of the applicable provisions and their specific obligations with regard the processing of personal data.

The document has been developed on the basis of the provisions laid down in Regulation (EU) 2016/679, the Commission Guidance on the application of Union data protection law in the election context of 12.09.2018[1] and the practice of the Commission for Personal Data Protection (CPDP).

[1] Guidance Document COM(2018) 638 final

1. Applicable legislation

Personal data protection in the election process must comply with the provisions laid down in several statutory acts:

Firstly, **Regulation (EU) 2016/679 (the Regulation)** is directly applicable in its entirety. It is supplemented and specified by the **Personal Data Protection Act**.

The **Election Code** sets out specific rules for the processing of personal data in the election process, for example the purposes of data processing, personal data categories, etc. It is important to emphasize that the Bill amending and supplementing the Personal Data Protection Act, adopted at the beginning of 2019, introduced changes and supplemented the provisions laid down in the Election Code, and in particular the time periods for compiling lists of voters supporting the registration of a political entity (parties, coalitions, initiative committees, independent candidates, etc.) [2]. The amendments in question introduced a requirement for **voters to verify their identity at the time of signing their name to the list**. This limits the possibilities for personal data abuse through the inclusion of voters in registration lists without their knowledge and consent. The preventative measure has been introduced in order to protect the interests of both natural persons and those of the political entities collecting signatures.

2. Data controllers and processors in the election process

In order to ensure correct understanding and compliance with the requirements for personal data protection, it is essential that the role of each party involved in the election process be strictly defined in accordance with the provisions laid down in the General Regulation.

In accordance with Regulation (EU) 2016/679 **data controller** means 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law' (Article 4(7) of the General Regulation) as in the case of personal data processing in the election process.

The capacity of controller is directly linked to the fact that a certain legal or natural person or another entity (for example an initiative committee, civil association, etc.) processes personal data for

[2] See Articles 133(3), 140(6), 257(2), 320(2), 367(2) and 416(2) of the Election Code.

purposes that are determined by law (for example in the Election Code, for financial reporting purposes, in order to compile a list of donors in accordance with the restrictions applicable to natural persons, etc.) or have chosen to process data for other purposes, regardless of whether there are directly related to elections, based on a contract, legitimate interest, etc. The controller must take appropriate technical and organisational measures to ensure data security in light of the nature, scope, context and purposes of data processing and any existing risks for the rights and freedoms of the data subjects. **Furthermore, in line with the principle of accountability, the data controller must be able to demonstrate compliance, at any time, with the requirements laid down in the Regulation, i.e. it must properly document the personal data processing actions taken.**

Regulation (EU) 2016/679 also introduces the concept **personal data processor**. According to the definition 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4(8) of the General Regulation).

The key difference between a data controller and data processor is that the latter does not act independently but on behalf of the data controller. Their relations are governed by a contract or another statutory instrument (for example an agreement establishing a coalition of political parties), which sets out the subject-matter, the length of the data processing actions, the nature and purpose of processing, the type of personal data and the rights and obligations of the controller, including to conduct checks to verify compliance with the requirements for the processing of personal data. The General Regulation introduces specific obligations for data processors, which are not limited to ensuring data safety. For example, the processor has an obligation to process personal data only on the basis of documented (in writing or in another verifiable manner) instructions from the controller. Where the volume of work requires the involvement of another processor, an authorisation from the controller is required. In addition, for the avoidance of doubt, according to the Regulation where a processor has the possibility to determine the purposes and means of processing, it is to be automatically considered a controller in respect of that processing and assumes full responsibility for the processing actions. Unlike the old rules, the Regulation introduces joint and several liability of the controller and processor for infringements of personal data processing rules. This means that the natural person whose personal data has been processed unlawfully may file a claim against either the controller or the processor at their own discretion.

The separation of roles and responsibilities between the controller and the processor is appraised on a case-by-case basis. It is not a formality but aims to ensure that personal data processing complies with the requirements laid down in the Regulation and ensures protection of the rights of data subjects, when they are natural persons.

In view of the above, the key players in the election process have the following roles and responsibilities with regard to personal data processing:

- **Political parties** – They are the key participants in the election process. The purposes and means of processing of personal data by political parties are stipulated by law, meaning that the latter have the capacity of **data controllers**.

- **Coalitions** – the coalition of political parties may be an independent **data controller** only when it exists as a permanent structure and has set up working and sustainable mechanisms for decision-making in relation to the processing of personal data. Such mechanisms should be set out in a coalition agreement. Such an agreement may stipulate that only one or several coalition members process personal data for the purpose of registration of the coalition or the coalition in general. In the latter case, the coalition, in its capacity as data controller, should exercise internal control over the designated coalition processors because the coalition bears responsibility for data processing as a legal entity.

The allocation of the roles and responsibilities within a given coalition prior to and after its registration with the Central Electoral Commission is as follows:

- in the period from the signature of a coalition agreement up to the entry into force of the decision on the coalition registration, the constituent political parties have the capacity as **joint controllers** and share the responsibility for data processing within the meaning of Article 26 of the General Regulation, regardless any provisions laid down in the coalition agreement that may envisage other arrangements;

- From the time when the coalition is established, i.e. after the entry into force of the decision adopted by the CEC, the coalition assumes the capacity as **independent data controller**.

Where the coalition ceases to have a legal existence or its original structure is modified (change of name, change of members, etc.), its former members have the capacity as **joint controllers** within the meaning of Article 26 of the General Regulation in respect of all personal data processing operations carried out while the coalition existed, even where the coalition sets out provisions to the contrary. This is so because of the imperative nature of the provision laid down in Article 26 of the Regulation. In this case, the data subject may exercise their rights, respectively the CPDP may exercise its sanctioning powers under the General Regulation, against each of the parties in the coalition (Article 26(3) of the General Regulation).

- **Initiative committees** – Initiative committees may nominate independent candidates for Members of Parliament, President and Vice President of the Republic, mayors and members of

municipal councils. According to the Election Code initiative committees are not permanent entities and cease to exist after the respective election has taken place. For this reason, according to the Election Code **the data controllers** in this case **are the members of the initiative committee**.
Each member of an initiative committee who signs the voters' list, which contains personal data of the individual voters, is personally responsible for data processing and storage, including when the signatory is not personally involved in signature collection but acts through third-party intermediaries. The responsibility for the processing of the personal data in the lists remains for the initiative committee and its members even after the lists have been handed over to the CEC.
In all other actions, except those relating to registration lists, the members of the initiative committee shall act as **joint controllers** within the meaning of Article 26 of the General Regulation, including in their work with polling agencies, social media, intercessors, etc. This remains valid even after the discontinuation of the initiative committee, including the deletion of its registration pursuant to Article 155 of the Election Code. In the case of a complaint or an alert, the members of the initiative committee (natural persons) shall continue to be considered as joint controllers.
As all other data controllers, as from 25 May 2018 initiative committees or their members are no longer subject to registration with the Commission for Personal Data Protection.

- **Election commissions** – The Central Electoral Commission (CEC), regional election commissions (REC) in Bulgaria and overseas, and in the case of local elections, the municipal election commissions (MEC) shall act as independent **data controllers** designated in accordance with the provisions laid down in national law. In light of the new rules, they all have independent powers and, like other data controllers, are not subject to registration with the CPDP.

- **Other public bodies** to which tasks are delegated and into which powers are vested under the Election Code include local government bodies, executive agencies (Ministry of Interior, Ministry of Regional Development and Public Works, etc.), other institutions (Ministry of Foreign Affairs, respectively diplomatic and consular services; the Ministry of Justice, respectively prisons and detention facilities, etc.). As a general rule, they are also independent **data controllers** whose purposes and means of processing of personal data in the election process are clearly stipulated in national law.

- **Private-law entities** – entities governed by private law are also involved in the election process, notably media, polling agencies, advertising companies, social media, etc. In light of their specific role and relations with other players in the election process, they could act as independent **data controller** (for example an advertising agency processing personal data on behalf of a political

party on the basis of documented instructions for the purpose of election campaigning; a polling agency conducting targeted voter polls on the basis of personal data received in advance from the political data subject, etc.).

II. GUIDANCE FOR DATA CONTROLLERS

1. Removal of the requirement for registration with the CPDP

As from 25 May 2018, when Regulation (EU) 2016/679 started to apply, **there is no longer a requirement for all data controllers to register with the CPDP**. It was replaced by the requirement for compliance with the principle of accountability, including through compiling and keeping internal documentation, and in particular of records of processing activities envisaged in Article 30 of the General Regulation.

2. Principles of personal data processing

All parties involved in the election process, regardless of whether governed by public or private law, have an obligation to process personal data in accordance with the following principles set out in Article 5 of Regulation (EU) 2016/679:

- Lawfulness, fairness and transparency;
- Purpose limitation — personal data shall be processed solely for the purpose for which it has been collected (for example personal data collected for the purpose of concluding an employment contract or a fixed-term contract or for the purpose of the supply of goods or provision of services may not be used for the purpose of the list required to register in an election or in the election campaign);
- Data minimisation — the purpose should be achieved with the minimum personal data necessary (for example personal data collected for the purpose of registering with the CEC may not exceed the data specified in the Election Code);
- Storage limitation — data may not be processed when grounds for the processing of such data no longer exist;
- Accuracy, integrity and confidentiality (for example to ensure the accuracy of processed data, the latest amendments to the Election Code envisage that the identity of the signatories to the voters' list for the purpose of registration is to be verified);
- Accountability — clearly documenting data processing actions taken.

3. Legal grounds for the processing of personal data

The processing of personal data by data controllers in the public and private domain shall be lawful only if and to the extent that at least one of the following conditions stipulated in Article 6(1) of Regulation (EU) 2016/679 applies:

- consent;
- conclusion or performance of a contract;
- legal obligation to which the controller is subject;
- necessity to protect the vital interests of the data subject or of another natural person;
- performance of a task carried out in the public interest or in the exercise of official powers vested in the controller;
- legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (*inapplicable to public bodies*).

It is important to bear in mind that **when personal data has been collected or otherwise processed pursuant to a statutory act, such as the Election Code, data subject consent is not required**. Such cases include the compilation, announcement and publishing of voter lists, the verification of the identity of voters by Local Election Commissions, the entries attesting to the votes cast, etc.

There are also **cases when consent is the principal or only possible ground for the processing of personal data**, such as the **collection of signatures in support of the registration of a political entity** for the respective type of election, conducting opinion polls or sending personalised e-mails by political parties or companies hired by political parties, telephone calls, text messages (SMS) or faxes in the context of election campaigning. When consent is used as a legal ground, the General Regulation requires that it be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement. A failure to ensure compliance with this requirement constitutes an infringement of data processing rules. At the same time, according to the General Regulation the withdrawal of the consent has a future effect and does not affect the legality of data processing performed up to the time of withdrawal.

4. Processing of ‘sensitive’ personal data

Certain categories of personal data are, by nature, particularly sensitive from the point of view of the fundamental rights and freedoms of individuals and therefore subject to special protection. This category includes **political views** (Article 9(1) of Regulation (EU) 2016/679). The processing of such data is allowed solely if any of the conditions envisaged in Article 9(2) of the General Regulation has been satisfied.

In accordance with Article 9(2)(d) of Regulation (EU) 2016/679 processing is carried out in the course of its legitimate activities with appropriate safeguards by political parties:
- on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes;
- and that the personal data are not disclosed outside that body without the consent of the data subjects.

However, the cited provision may not be used by a political party for the purpose of processing personal data of prospective members, supporters or voters because there is no durable permanent link to the political entity. In this case, another valid legal ground must be present, such as explicit consent of the data subject.

In an election context, the main legal ground for processing is the existence of a substantial public interest, on the basis of Union or Member State law (the Constitution, the Election Code) which is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9(2)(g) of Regulation (EU) 2016/679).

Other possible grounds include the case where the person has given explicit consent or where personal data which are manifestly made public by the data subject (Article 9(2)(a) and (e) of Regulation (EC) 2016/679).

5. Time periods for storing personal data

In accordance with Article 5(1)(e) of the General Regulation (principle of storage limitation) personal data should be kept for as long as is necessary for the purposes for which the personal data are processed and must thereafter be erased.

As a general rule, the time periods for the storage of personal data collected for the purposes of an election or referendum are stipulated in the Election Code (for example, Articles 135 and 142 of the Election Code) and all data controllers involved in the election process must ensure compliance with the relevant time periods.

In certain cases, data may be stored for longer periods insofar as this is done in the public interest or the data controller has a legitimate interest in doing so, which overrides the interests of the data subject. Such cases include:

- the establishment, exercise or defence of legal claims, when it would be lawful and proportionate for the respective controller involved in the election process to store the personal data upon the filing of a claim until the respective judicial proceedings have ended;

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes – always ensuring that sufficient guarantees for the protection of the rights of data subjects are available, for example through data anonymization (for example in the case of internal party statistical data about voting results per electoral district);
- for the purpose of exercising the right to freedom of expression and the right to information – in principle this ground for data storage is applicable to the media reporting on the election process.

6. Data security

Security is particularly important in the election context in view of the large volume of personal data processed and the sensitive nature of such data. In accordance with the General Regulation both data controllers and data processors must implement appropriate technical and organisational measures to ensure the highest level of protection of personal data, taking into account the risks data processing poses for the rights and freedoms of natural persons.

The Regulation introduces a requirement for data controllers to notify the CPDP of breaches of personal data security within a period of 72 hours. When a security breach is likely to cause a high risk to arise for the rights and freedoms of natural persons, the data controller must also take action to notify the persons affected by the data breach.

7. Information to be provided to data subjects

The principles of fair and transparent processing require that natural persons be informed about operations relating to the processing of their personal data and the purposes of such processing. The General Regulation clearly sets out the responsibilities of data controllers in this regard. They have an obligation to inform data subjects about key aspects relating to the processing of their personal data, such as:

- identifying the data controller – name and contact details;
- the categories of personal data processed (only where the data has not been directly collected from the person);
- the purposes of processing (as defined in the Election Code or by the controller);
- the categories of personal data recipients (CEC, REC, MEC, LEC, the National Audit Office, the Office of the Provincial Governor);
- the time period for data storage;
- the existence of specific rights of data subjects (right to access, rectification or erasure of personal data, limitation of processing or objection against processing) and the rules for the exercise of those rights;
- the right of data subjects to submit a complaint to the CPDP or file a court claim;

- whether the provision of personal data is mandatory by law or another contractual provision and the potential consequences of non-provision of data;
- (where applicable) whether automated decision-making, including profiling, is used.
- any other information necessary to ensure fair and transparent data processing.

Furthermore, the General Regulation on data protection requires that information be provided in an intelligible and easily accessible form, using clear and plain language. Information must be provided at each stage of processing and not only at the stage of collection.

The General Regulation allows certain exceptions from the obligation to provide information, in particular when:

- the information is already available to the data subject;
- the provision of such information is not possible or requires unreasonable effort (for example the provision of new or additional information to the persons who signed the registration list);
- receiving or disclosing the personal data is expressly allowed under EU or national law (for example publishing electoral lists, provision of data to the CPDP or the respective court, etc.).

8. Rights of data subjects

Regulation (EU) 2016/679 confers to natural persons certain additional and enhanced rights in the election context such as:

- right to access to their personal data processed by the data controller or processor;
- right to request the erasure of their personal data, if processing is based on consent and the consent has been withdrawn, if the data exceeds that, which is required, or if processing is unlawful. The withdrawal has a forward effect and any processing performed prior to consent withdrawal is to be considered lawful;
- the right to rectification of untruthful, incorrect or incomplete personal data;
- the right to object against a specific form of data processing by a political entity (for example data collected in the registration list, which is processed for another purpose such as election campaigning);
- the right to file a complaint to the CPDP or directly to the competent court.

It should be noted that the rights of data subjects are not absolute and should be compared to and balanced against the rights of other affected parties and against public interest, when applicable. For example, the data controller could refuse a personal data erasure request (the 'right to be forgotten'), if personal data is necessary to:

- ensure compliance with the legal obligation envisaged in EU or national law (for example the Election Code) or the performance of a task in the public interest or of official powers vested in the

data controller (CEC, REC, MEC and the office of the Provincial Governor, the Ministry of Interior, the Ministry of Foreign Affairs, etc.);

- establish, exercise or defend legal claims (for example, the defence of the data controller in the event of a complaint being filed with the CPDP or a court of law);
- exercise freedom of expression and the freedom of information (media, etc.).

The CEC notifies all data controllers involved in the election process of their obligation to inform data subjects/voters of the possibilities to exercise the above rights.

9. Penalties for infringements of data protection rules

9.1 Penalties levied at the national level

Regulation (EU) 2016/679 envisages very serious penalties for **infringements of personal data protection rules** that may reach EUR 20 million. It is important to emphasize that before levying a 'fine' on a natural person acting in the capacity as data controller or processor or a 'pecuniary penalty' on a legal person acting in the capacity as data controller or processor, the CPDP must carry out an appraisal, taking into account a number of factors and circumstances, including:

- the nature, gravity and duration of the infringement, taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- the intentional or negligent character of the infringement;
- any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them;
- any relevant previous infringements by the controller or processor;
- the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- any other aggravating or mitigating factor applicable to the circumstances of the case.

9.2. Penalties at EU level

Regulation (EU, EURATOM) 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 aims to enhance the visibility, recognition, effectiveness, transparency and

accountability of the European political parties and the political foundations related to them. The Regulation establishes an independent **Authority for European Political Parties and Foundations** tasked with the registration, monitoring and, when necessary, sanctioning of European political parties and foundations.

In order to ensure that the European Parliament elections are conducted in accordance with the robust democratic rules and in full compliance with the European values of democracy, rule of law and fundamental rights, the European Commission has proposed that Regulation 1141/2014 be amended and supplemented. The aim is to ensure that a possibility is available to levy penalties on European political parties or foundations that rely on infringements of personal data rules to intentionally influence or attempt to intentionally influence the results of European Parliament elections.

The amendment of Regulation (EU, EURATOM) 1141/2014 envisages that data protection supervisory authorities such as the **CPDP immediately notify the Authority for European Political Parties and Foundations** of their decisions finding that a given European political party, respectively national political party which is a member of the European entity, or another natural or legal person has infringed applicable data protection rules. On the basis of the national decision, the Authority for European Political Parties and Foundations may levy a financial penalty on the respective European political party, withholding its EU financing.
The proposal to amend Regulation (EU, EURATOM) 1141/2014 in connection with personal data protection in the election process is at a very advanced stage of adoption and is expected to come into effect before the European Parliament election in May 2019.

III. ADDITIONAL GUIDANCE RECEIVED FROM THE EUROPEAN COMMISSION

In recent months, the European Parliament has adopted a series of documents aiming to ensure a free and fair European Parliament election. More specifically, in September 2018 the European Commission published a document entitled Guidance on the application of Union data protection law in the election context, which stipulates certain additional obligations of political parties and other actors in the election process. These new commitments arise from the General Regulation on personal data protection and from the risks relating to the use of new technologies, such as the abuse of personal data of Facebook users by Cambridge Analytica.

1. Use of profiling, automated decision-making and social media

According to the General Regulation ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at

work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4(4) of GDPR).

Within the meaning of the General Regulation 'automated decision making' means a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (Article 22 of GDPR).

Dynamic technological development and the ever more pervasive use of various algorithms, incl. artificial intelligence, create possibilities for unprecedented encroachment, in terms of volume and depth, of the personal space and privacy of natural persons. The Cambridge Analytica and Facebook scandals have shone the light on the particular challenges arising from the microtargeting methods used in social media. Both commercial and political organisations may perform smart analysis of data collected from social media users in order to profile and target voters. This would allow such organisations to ultimately target susceptible voters and thus influence the outcome of elections.

In principle, Regulation (EU) 2016/679 does not prohibit the use of profiling and automated decision making, but in view of the high level of risk these forms of processes create for the rights and freedoms of natural persons, more stringent requirements and specific obligations for data controllers as well as specific rights of data subjects have been introduced.

Automated decision making and profiling on the basis of special categories of personal data, including political views, is subject to more stringent requirements, notably the express consent of the data subject or the existence of a substantial public interest, on the basis of European Union or national law, which is proportionate to the aim pursued.

In view of the lack of rules and regulations governing this type of personal data processing in election law and of appropriate and effective safeguards for the rights and freedoms of natural persons, **the hypothetical use of profiling and automated decision making in the election process in Bulgaria would be high-risk personal data processing while failing to ensure compliance with the more stringent requirements for personal data processing in breach of data processing rules.**

2. Data protection impact assessment

Regulation (EU) 2016/679 introduces a new requirement for data controllers, including those engaged in the election process, to **carry out an assessment of the impact of the envisaged processing operations on the protection of personal data**. Such assessment is to be carried out when there is a risk that certain type of processing is likely to result in a high risk to the rights and freedoms of natural

persons in view of its nature, scope, context and purposes of the processing (Article 35(1) of Regulation (EU) 2016/679).

The Commission Guidance on the application of Union data protection law in the election context requires that all political parties and other actors in the election process carry out such an impact assessment in respect of personal data.

An impact assessment must contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purpose;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

According to the General Regulation one of the cases in which such high risk is deemed to exist is **the processing on a large scale of special categories of data, including political views**.

It is not necessary to carry out such an impact assessment, if the processing has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis (Article 35(1) of Regulation (EU) 2016/679). In this connection, the **CEC and other electoral commissions as well as other public bodies in which specific obligations relating to the election process are vested are exempt from the requirement for carrying out an assessment of impact on personal data**. The other participants in the election process, including political parties, are not exempt from this requirement.

3. Direct marketing and unsolicited commercial messages

Unlike previous elections, the General Regulation regards the sending of *personal* electronic messages by e-mail, telephone call, text messages (SMS) or fax as direct marketing. The European Commission has envisaged stronger requirements for the processing of this type of personal data, equating them to unsolicited commercial messages within the meaning of Article 6 of the **Electronic Commerce Act**, respectively Article 261 of the **Electronic Communications Act.** The messages in

question require the prior consent of the party, including where the message has been sent in the context of election campaigning in accordance with Article 181 of the Election Code. Political parties are required to comply with the general rules on direct marketing and unsolicited commercial messages and provide an easy and efficient possibility for the withdrawal of consent to receive such messages by sending an e-mail containing a short message, using a link to a website or in another appropriate manner.
