CENTRAL ELECTORAL COMMISSION of the Republic of Bulgaria

COMMISSION FOR PRESONAL DATA PROTECTION

GUIDANCE ON THE PROCESSING AND PROTECTION OF PERSONAL DATA IN THE ELECTORAL PROCESS

Adopted jointly by the Central Election Commission and the Commission for Personal Data Protection on the basis of Article 57 (1) (49) of the Election Code

PROCESSING OF PERSONAL DATA IN THE ELECTORAL PROCESS

I. GENERAL

Since 25 May 2018, new rules on the protection of personal data apply in the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation) is the legal act that sets out the requirements and obligations of all public authorities, private companies and data controllers relating to the protection of personal data when processed.

The General Data Protection Regulation takes into account the fact that, for the purposes of the electoral process, including during election activities, political parties, competent institutions and other bodies collect and/or have access to personal data, including on the political views of citizens, who are generally considered to be sensitive data and are subject to increased protection. Election agents, representatives of parties and observers, as well as the media, have access to and may process personal data in relation to their role in the electoral process. For this reason, these guidelines aim to provide guidance to all participants in the electoral process on the applicable legal rules and their specific rights and obligations in relation to the processing of personal data.

The document is based on the provisions of Regulation (EU) 2016/679, the European Commission Guidelines on the application of Union data protection law in the electoral context from 12 September 2018[1], as well as the practice of the Commission for Personal Data Protection (CPDP).

[1] Document COM(2018) 638 final

1. Applicable legislation

The processing of personal data in the electoral process should comply with several legal acts:

First, **Regulation (EU) 2016/679 (the Regulation)** is directly applicable and binding in its entirety. The measures for its implementation are introduced by the **Personal Data Protection Act.**

The Election Code explicitly regulates the rights and obligations of all participants in the electoral process — political parties, coalitions of parties, initiative committees, candidates, representatives, election agents, observers, media representatives and electoral commissions in the various types of elections.

The processing of personal data in the electoral process is carried out in compliance with the rules of Regulation (EU) 2016/679, taking into account the specificities of the electoral process and the legislation applicable thereto.

2. Controllers, processors and persons who process personal data in the electoral process upon instructions by the controller.

Determining the role of each of the participants in the electoral process from the point of view of the General Regulation is essential for a proper understanding of and compliance with data protection requirements.

According to Regulation (EU) 2016/679, **'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. The controller, as well as the purposes and means of processing, may be determined by EU law or by the law of the Republic of Bulgaria (Article 4 (7) of the General Regulation), as is the case with the processing of personal data in the electoral process.

The status of controller is a direct consequence of the fact that a specific legal or natural person or other body (e.g. initiative committee, civil society association, etc.) processes personal data for purposes that are regulated by a legal act (e.g. under the Election Code, for financial reporting purposes, for the preparation of a list of donors, subject to limitations on natural persons, etc.).The status of controller is also acquired if the entities concerned have themselves chosen to process personal data for other legitimate purposes, regardless whether they are directly related to elections (in performance of a contract, processing of personal data subject to the requirements of the Labour Code, accounting or video surveillance for security purposes, etc.).

The General Regulation imposes a set of obligations on the controller. It must take appropriate technical and organisational measures relating to data security, taking into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects. **Furthermore, in accordance with the accountability principle, the controller should at**

all times be able to demonstrate compliance with the requirements laid down in the Regulation, i.e. to document the processing of personal data carried out by the controller.

Regulation (EU) 2016/679 also introduces the concept of **'processor'.** According to the definition, a processor is any 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 main difference between a controller and a processor is that the latter acts not independently but on behalf of the data controller. Their relations are governed by a contract or other legal act (for example: the agreement establishing a coalition of parties), which regulates the subject matter, the duration of the processing operations, the nature and purpose of the processing, the type of personal data and the obligations and rights of the controller, including to carry out inspections on compliance with the requirements for the processing of personal data. The General Regulation also introduces specific obligations for the processor which are not limited to data security only. For example, it is only obliged to process personal data on documentary (written or otherwise verifiable) instructions from the controller. Where it is necessary to involve another processor, this shall be subject to the express written consent of the controller. In addition, for the sake of clarity, the Regulation expressly provides that if the processor starts to determine the purposes and means of the processing himself, he automatically becomes a controller and is subject to the relevant liability. Unlike the old regime, the Regulation introduces joint liability for infringements of personal data processing between the controller and the processor. This means that the individual whose personal data are unlawfully processed may direct his claim to each of them of his choice.

The distribution of roles and responsibilities between the controller and the processor shall be assessed on a case-by-case basis. It is not a legal formality and aims to ensure that the processing of personal data takes place in accordance with the requirements of the Regulation and thus protects the rights of data subjects.

In view of the above, the main actors involved in the electoral process have the following roles and responsibilities with regard to the processing of personal data:

- **Parties** — they are key players in the electoral process. The purposes and means of processing personal data by political parties are defined by law or independently by them and therefore have the status of **data controllers.**

- **Coalitions** — the coalition of parties could be an autonomous **personal data controller** in cases where it persists over time as a stand-alone entity and has workable and robust decision-making mechanisms relevant to the processing of personal data. These mechanisms should be defined by the conclusion of a coalition agreement. It may determine that only one or more members of the coalition process personal data for the purposes of registration of the coalition or for the purposes of the

coalition in general. In the latter case, the coalition, as a data controller, should exercise internal control over the processing members of the coalition, as the responsibility falls on the coalition as an entity.

The distribution of roles within a coalition varies in the period before and after its registration at the CEC:

- Between the conclusion of the coalition agreement and the entry into force of the decision to register the coalition, the parties in the coalition are **joint controllers** and share joint liability for the processing of personal data under Article 26 of the General Regulation, even if the coalition agreement provides otherwise;

- as soon as the coalition is established, that is to say after the decision of the CEC enteres into force, it becomes an **autonomous controller.**

In the event that the coalition ceases to exist in the legal order or changes to its original form occur (change of name, change of membership, etc.), its members are **joint controllers** under Article 26 of the General Regulation in respect to all personal data processing operations carried out during the period of existence, even if the coalition agreement provides otherwise, since Article 26 of the Regulation is mandatory. In this case, the data subject may exercise his rights, and the CPDP may invoke its sanctioning powers under the General Regulation against any of the parties in the coalition (Article 26 (3) of Regulation (EU) 2016/679).

■ **Initiative Committees** — Initiative Committees nominate candidates for MPs, President and Vice President, Mayors and Municipal Councillors. The Initiative Committees under the Election Code do not have a lasting existence after the end of the relevant type of election. For this reason, the Election Code designates **the members of the Initiative Committee as data controllers.**

Each member of the initiative committee who signs the list of voters' personal data is personally responsible for processing and storing the data, including when he does not collect the signatures in person but through third parties.

The responsibility for processing data from the list remains with the initiative committee and its members including after the lists have been transmitted to the CEC.

In all other actions, other than the registration lists, the members of the initiative committee shall have the status of **joint controllers** under Article 26 of the General Regulation — including when working with sociological agencies, social media, advocates, etc. This remains valid even after the initiative committee ceases to exist, including when its registration under Article 155 of the Election Code has been cancelled. In the event of a complaint or an alert, natural persons who are members of it shall continue to be considered as joint controllers.

■ **Electoral commissions** — the Central Election Commission (CEC), the District Election Commissions (DEC), the Section Electoral Commissions (SICs) in and outside the country and, in the case of local elections, the Municipal Electoral Commissions (MEC), are autonomous personal data controllers defined by national law.

■ **Private entities** — in one form or another, private entities participate in the electoral process — media, sociological agencies, advertising companies, social media, etc. In view of their specific role and relationship with other actors and the electoral process, they could be an autonomous **data controllers** (e.g. printed or electronic media covering the election campaign) or **processors** (e.g. Information Service AD as a data processor, advertising companies that process personal data on behalf of a political party and on its documented instructions for election purposes; sociological agencies carrying out targeted voter surveys on the basis of personal data previously provided by the political entity, etc.).

■ **Other public bodies** having tasks and powers under the Election Code are local self-government bodies, executive authorities (Ministry of Interior, MRDPW, etc.), other institutions (MFA, respectively diplomatic and consular missions; Ministry of Justice, places of imprisonment, detention facilities, etc.). As a rule, they are also autonomous **personal data controllers**, where the purposes and means of processing in the electoral process are determined by the law of the Republic of Bulgaria.

■ **Election agents, observers and representatives of political parties and coalitions and initiative committees.** These electoral actors process personal data on the basis of Article 29 of the General Regulation, i.e. acting under the authority of the above-mentioned controllers and have access to the personal data. They do not have the status of controllers or processors. Their rights and obligations with regard to the processing of personal data are limited in so far as their rights and obligations in the electoral process are listed exhaustively and limited. The cases where these entities process personal data are explicitly defined in the Election Code (right to direct visibility when establishing voting results, right to receive a copy of the section protocol, etc.). When processing personal data, these entities may not go beyond the rights and obligations provided for in the Election Code.

■ **Mass media** They process personal data lawfully for the purpose of implementing freedom of expression and the right to information while simultaneously respecting privacy (Article 25h (1) PDPA). Media as mass media are controllers under the General Regulation. Journalists and operators who are employees of the media act on instructions from the controller under Article 29 of the General Regulation and are not be solely liable as controllers or processors of personal data. In cases where these journalists, video operators or photographers are freelancers and determine themselves the purposes and means of processing personal data (not acting on behalf and on the instructions of a data

controller), they become controller or processor, with the resulting obligations and responsibilities. These entities process personal data only for the purpose of exercising their rights when opening the election day (Article 230 (1) of the Election Code) and when opening the ballot boxes — Article 272 of the Election Code. In view of their purpose of providing information in accordance with the principle of freedom of expression, the media process personal data, including video filming, while respecting the privacy of individuals and respecting the secrecy of vote.

II. INSTRUCTIONS TO DATA CONTROLLERS

1. No obligation to register with the CPDP

As of 25 May 2018, when Regulation (EU) 2016/679 became applicable, the obligation for all data controllers to register with the CPDP was suspended. It has been replaced by the requirement to comply with the principle of accountability, including by maintaining internal documentation, in particular a register of personal data processing activities under Article 30 of the General Regulation.

2. Principles of personal data processing

All actors in the electoral process, whether public authorities or private legal entities, are obliged to process personal data in accordance with the principles set out in Article 5 of Regulation (EU) 2016/679:

- Lawfulness, fairness and transparency;
- Purpose limitation — the data collected shall be processed only for the purpose for which it was collected (e.g. personal data collected for the purpose of concluding an employment or civil contract or for the provision of goods and services cannot be used for the purposes of the registration list or election campaigning);
- Data minimisation — the purpose should be achieved with the minimum personal data necessary for this (e.g. personal data collected for the purpose of registration in the CEC may not exceed those specified in the Election Code);
- storage limitation — data may not be processed once the basis for their processing has ceased to exist;
- Accuracy, integrity and confidentiality (e.g. to ensure that correct data are processed, the latest amendments and additions to the Election Code provide for verification of the identity of the signatory of the registration list);
- Accountability — clearly documenting the data processing actions taken.

3. Legal grounds for processing personal data

The processing of personal data by data controllers in both the public and private spheres is lawful only if any of the legal grounds exhaustively listed in Article 6 (1) of Regulation (EU) 2016/679 apply:

- consent;
- conclusion or performance of a contract;
- a legal obligation of the controller;
- protection of vital interests of the data subject or of another natural person;
- the performance of a task carried out in the public interest or the exercise of official authority vested in the controller;
- legitimate interests of the controller or of a third party where they override the interests or fundamental rights and freedoms of the data subject *(not applicable to public authorities).*

It is important to bear in mind that **where personal data are collected or otherwise processed under a legal act, such as the Election Code, there is no need and consent of data subjects should not be required.** Such hypotheses include the drawing up, announcement and publication of the electoral roll, the verification of the identity of the voter by the CEC and the recording of his vote, etc.

There are also **cases where consent is the main or only possible reason for the processing of personal data**, such as when **collecting signatures in support of registration of a political entity** in the relevant type of choice, conducting sociological surveys or sending personal emails by a political entity or a company hired by him by e-mail, telephone calls, SMS or fax for election campaigning. When consent is used as a legal basis, the General Regulation requires it to be given by means of a clear affirmative action and to be freely given and informed. In any event, the possibility for the subject to withdraw his or her consent at any time should be clearly indicated. The absence of such a possibility is a breach of the rules on the processing of personal data. At the same time, under the General Regulation, the withdrawal of consent has only a forward effect and does not affect the lawfulness of the processing prior to that.

4. Processing of sensitive personal data

Certain categories of personal data are, by their nature, particularly sensitive from the point of view of the fundamental rights and freedoms of individuals and are specifically protected. These

include **political opinions** (Article 9 (1) of Regulation (EU) 2016/679). Their processing is permissible only if one of the conditions laid down in Article 9 (2) of the General Regulation is met.

In accordance with Article 9 (1) (d) of Regulation (EU) 2016/679 political parties may process such sensitive data, when appropriate safeguards are put in place and if all the following conditions are met:

- the processing relates solely to the members or former members of the party or to persons who have regular contact with it in relation to the activity and purposes and;
- personal data shall not be disclosed to third parties without the consent of the data subjects.

However, this provision cannot be used by a political party to process data of potential members, sympathisers or voters, as in the present case there is no clear and permanent link with the political entity. In such cases, there should be another valid legal basis, such as explicit consent of the data subject.

In the context of elections, the main legal basis for processing sensitive data is the existence of an important public interest, on the basis of EU law or the law of the Republic of Bulgaria (Constitution, Election Code), which is proportionate to the objective pursued, respects the essence of the right to data protection and provides for appropriate and specific measures to protect the fundamental rights and interests of the data subject (Article 9 (2) (g) of Regulation (EU) 2016/679).

Other possible reasons are that the person has given his explicit consent or made the data public (Article 9 (2) (a) and (e) of Regulation (EU) 2016/679).

5. Time limits for the storage of personal data

According to the general principle of 'storage limitation' in Article 5 (1) (e) of the General Regulation, personal data should be kept for no longer than is necessary to achieve the purposes for which they are processed and should then be erased.

As a rule, the time limits for the storage of personal data collected for the purposes of the relevant elections or referendum are laid down in the Election Code (e.g. Articles 135 and 142 of the Election Code) and all data controllers involved in the electoral process are obliged to comply with them.

In certain cases, the data may also be stored for a longer period where this is justified by a public interest or a legitimate interest of the controller which overrides the interests of the data subject. Similar assumptions are:

■ the establishment, exercise or defence of legal claims — for example, legitimate and proportionate — it would be for the relevant controller involved in the electoral process to preserve

the personal data upon lodging a complaint pending the conclusion of the relevant administrative or judicial proceedings;

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, providing sufficient safeguards to protect the rights of data subjects, e.g. through anonymisation of data (for example, the production of internal party statistics on election results by election district);

- in order to exercise the right to freedom of expression and the right to information, media outlets covering the electoral process may, in principle, benefit from this preservation ground.

6. Data Security

Security is of particular importance in the electoral context, given the large amount of personal data being processed and its sensitive nature. The General Regulation requires both controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that processing poses to the rights and freedoms of natural persons.

The Regulation introduces an obligation for data controllers to notify personal data breaches to the CPDP within 72 hours. Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also take action to inform the persons concerned by the breach.

7. Awareness of data subjects

The principles of fair and transparent processing require individuals to be informed of the existence of processing operations on their personal data and of their purposes. The General Regulation clarifies the obligations of data controllers in this respect. They must inform individuals about key aspects relating to the processing of their personal data, such as:

- identification of the data controller — name and means of contact;

- what categories of personal data are processed (only if the data are not collected directly from the individual);

- for what purposes they are processed (as determined by the Election Code or by the controller itself);

- the categories of recipients of personal data (CEC, DEC, MEC, SEC, Court of Auditors, regional administration, etc.);

- the data retention period;

- the existence of specific rights of data subjects (right to access, rectify or erase personal data, restriction of processing or objection to processing) and the procedures for exercising them;
- the right of data subjects to lodge a complaint with the CPDP or the court;
- whether the provision of personal data is mandatory by law or by contract, and the possible consequences of not providing such data;
- (if applicable) whether there is automated decision-making, including profiling.
- any other information necessary to ensure fair and transparent processing.

Furthermore, the General Data Protection Regulation requires information to be provided in a concise, transparent, intelligible and easily accessible form, in clear and intelligible language. Information must be provided to individuals at every stage of the processing and not only when the data are collected.

The General Regulation also allows for exceptions to the obligation to provide information, in particular where:

- the data subject already has the information;
- providing such information is impossible or requires a disproportionate effort (e.g. providing new or additional information to signatories to the registration list);
- obtaining or disclosing personal data is expressly authorised by EU or Bulgarian law (e.g. publication of the electoral roll, provision of data to the CPDP or the relevant court, etc.).

8. Rights of data subjects

Regulation (EU) 2016/679 grants individuals additional and enhanced rights, including, in the context of elections, particularly relevant:

- the right of access to their own personal data processed by the controller or processor;
- the right to request the erasure of their personal data if processing is based on consent and consent is withdrawn, if the data are no longer necessary or if processing is unlawful. Withdrawal of consent has effect for the future, therefore processing before that time remains lawful;
- the right to rectify incorrect, inaccurate or incomplete personal data;
- the right to object to a particular form of processing by a political entity (e.g. data collected in the registration list are processed for another purpose such as election campaigning);
- the right to lodge a complaint with the CPDP or directly to the competent court.

However, it should be borne in mind that the rights of data subjects are not absolute and should be matched and balanced with the rights of the other persons concerned as well as with the public interest, where applicable. For example, the data controller could refuse a request for erasure (right to be forgotten) if the personal data are necessary:

- for compliance with a legal obligation laid down in EU law or in the legislation of the Republic of Bulgaria (e.g. the Election Code) or for the performance of a task carried out in the public interest or in the exercise of official powers vested in the controller (CEC, DEC, municipal and regional administration, Ministry of Interior, Ministry of Foreign Affairs, etc.);
- for the establishment, exercise or defence of legal claims (e.g. to defend the controller in case of a complaint against it in the CPDP or in court);
- for the exercise of the right to freedom of expression and the right to information (media, etc.).

The CEC and all data controllers involved in the electoral process must inform the data subjects/voters how they can exercise the rights described above.

9. Processing of personal data by video recording and/or distribution (recording and/or live broadcast)

The media shall process personal data by video filming and/or dissemination only in the cases referred to in Articles 230, 232 and 272 of the Election Code (opening the Election day, closing the election day and establishing the results of voting) and drawing lots to determine the sequential numbers in the ballot papers. Video capture/distribution shall be carried out after standing, subject to the instructions of the chairperson of the SEC and in a manner that does not interfere with voting and the establishment of election results.

The purpose of processing personal data in the electoral process through video filming and/or dissemination is to ensure transparency, objectivity, lawfulness of the electoral process, equal treatment of those subject to it and ensuring freedom of expression and the right to information.

When processing personal data in the electoral process, mass media, photographers, journalists and freelance video operators shall comply with the rules and principles of Regulation (EU) 2016/679 and the PDPA and shall bear the responsibility provided for therein.

All other participants in the electoral process may not process personal data by video capture and/or dissemination due to the incompatibility of their role in the electoral process with the purpose of processing personal data by video filming in the electoral process. The functions and roles of these actors in the electoral process are explicitly and strictly defined in the Election Code.

10. Penalties for infringements of data protection rules

10.1. Penalties at national level

Regulation (EU) 2016/679 provides for very high administrative penalties for **infringements of personal data protection rules** of up to EUR 20 million. It is important to know that before imposing a 'fine' on a controller, processor, or a natural person, the CPDP assesses a number of factors and circumstances, including:

- the nature, gravity and duration of the infringement, taking into account the scope and purpose of the processing concerned as well as the number of data subjects affected and the degree of harm caused to 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 the technical and organisational measures taken by the controller or processor;
- previous infringements by the controller or processor;
- the degree of cooperation with the CPDP, 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 the controller or processor himself notified about the infringement;
- other aggravating or mitigating factors applicable to the case.

10.2. Penalties at EU level

Regulation No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations aims to increase the visibility, recognition, effectiveness, transparency and accountability of European political parties and their affiliated political foundations. It establishes at EU level an independent **Authority for European Political Parties and European Political Foundations**, tasked with registering, monitoring and, where necessary, sanctioning European political parties and foundations.

III. FURTHER GUIDANCE BY THE EUROPEAN COMMISSION

In September 2018, the European Commission published **Commission guidance on the application of Union data protection law in the electoral context**, setting out some additional obligations for political parties and other participants in the electoral process. These new commitments stem from the General Data Protection Regulation as well as from the risks associated with the use of new technologies.

1. Use of profiling, automatic decision-making and social networks

According to the General Regulation, 'profiling' is a 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 persons, economic situation, personal preferences, interests, behaviour, etc. (Article 4 (4) of the General Regulation).

'Automated decision-making' within the meaning of the General Regulation means the adoption of a decision by the controller based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him(Article 22 of the General Regulation).

The dynamic development of technologies and the increasing use of different algorithms, including artificial intelligence, create opportunities for an unprecedented volume and depth of intrusion into the private life and privacy of individuals. The case of Cambridge Analytica and Facebook revealed the particular challenges associated with methods of micro-targeting on social media. Both commercial and political organisations can carry out a smart analysis of data collected through social media users to create electoral profiles. This would allow these organisations to identify voters who can be more easily influenced and thus influence the results of the elections.

In principle, Regulation (EU) 2016/679 does not prohibit the use of profiling and automated decision-making, but given the high level of risk that these forms of processing pose to the rights and freedoms of natural persons, there are increased requirements and specific obligations for data controllers, as well as specific rights of data subjects.

Automated decision-making and profiling based on special categories of personal data, including political opinions, is subject to even stricter conditions, namely the existence of the data subject's explicit consent or of an important public interest on the basis of EU or Bulgarian law which is proportionate to the objective pursued.

Given the lack of legal regulation of such forms of processing of personal data in electoral legislation and of appropriate and effective safeguards for the rights and freedoms of natural persons**, the possible use of profiling and automatic decision-making in the electoral process in the**

Republic of Bulgaria would be highly risky processing of personal data and, in case of non-compliance with the increased conditions for the processing of personal data, would be contrary to the rules on data processing.

2. Data protection impact assessment

Regulation (EU) 2016/679 introduces a new obligation for data controllers, including those involved in the electoral process, an **impact assessment on the protection of personal data** of certain processing operations. Such an assessment must be carried out where a type of processing is likely, given its nature, scope, context and purposes, to result in a **high risk** to the rights and freedoms of natural persons (Article 35 (1) of Regulation (EU) 2016/679).

The European Commission's guidance on the application of Union data protection law in the electoral context requires all political parties and other electoral actors to carry out such a data protection impact assessment.

The impact assessment should 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 purposes;
- an assessment of the risks to the rights and freedoms of data subjects;
- 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 the other persons concerned.

The General Regulation assumes that one of the situations in which such a high risk exists is **the large-scale processing of special categories of data, including political beliefs.**

An exception to the obligation to carry out an impact assessment is permissible if the processing is carried out pursuant to a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and such an assessment has already been carried out as part of the general impact assessment in the context of the adoption of the relevant legal act (Article 35 (10) of Regulation (EU) 2016/679). In this regard, it can be assumed that the **CEC and other electoral commissions, as well as other public bodies with specific electoral obligations, fall under the exception and do not have to carry out an impact assessment**

on the protection of personal data. Other participants in the electoral process, including parties, are not exempted from this obligation.

3. Direct marketing and unsolicited commercial communications

Unlike in previous elections, the General Regulation treats the sending of *personal* emails by e-mail, telephone calls, SMS or fax as direct marketing. The European Commission provides for increased requirements for this type of processing of personal data and equates them to 'unsolicited commercial communications' within the meaning of Article 6 of the **Electronic Commerce Act** and Article 261 of the **Electronic Communications Act.** Prior consent of the person is required for this type of communication, including in cases where they are sent for election purposes in accordance with Article 181 of the Election Code. Political parties must comply with the general rules on direct marketing and unsolicited commercial communications and provide an easy and effective opportunity to refuse to receive such communications or to withdraw the individual's consent, either by sending an e-mail, by means of a short message, by using a 'link' to a website or by any other appropriate means.