



Guidelines on the processing of personal data for political campaigning purposes

Published on May 2017, revised in March 2019 and October 2021

CONTENTS		Page
1. Introduction	2
2. Definitions	2
3. Principles of Data Protection	3
4. Legal Basis of Processing	4
5. Postal and Telephony Communications	5
6. Door-to-Door Canvassing	5
7. Generalised Political Communication	5
8. Electronic Direct Marketing and Canvassing	5
9. Online Canvassing	6
9.1 Websites	6
9.2 Social Media	6
10. Transparency	7
11. Opting-Out	7
11.1 Opting Out from Telephone Campaigning	7
11.2 Opting Out from Electronic Direct Marketing	7
12. Contacting Voters on Election Day	8
13. Conclusion	8

1. Introduction

In any democratic society, political parties and campaigners must be able to communicate effectively with constituents. For the integrity of elections and democracy, it is therefore critical that all those involved in political campaigning, handle and process personal data in a way that is compliant with the data protection laws.

The *Guidelines on the processing of personal data for political campaigning purposes* (the “**Guidelines**”) have been adopted to provide a clear and uniform interpretation of the applicability of the General Data Protection Regulation¹ (the “**Regulation**”) and the Data Protection Act (Chapter 586 of the Laws of Malta) (the “**Act**”) in the political environment where political parties and candidates process personal data for the purposes of carrying out political campaigning and promoting their political ideologies and messages.

2. Definitions

For the purposes of these Guidelines, unless otherwise specified, the definitions contained in the Regulation should apply:

- a. data controller should mean any political party as defined under Article 2 of the General Elections Act (Chapter 354 of the Laws of Malta), any Member of Parliament, movement or candidate who runs for an election, be it the General Election, a Local Council election or a European Parliament election, either on a political party’s ticket or independently;
- b. consent should be defined in the Regulation as, *“any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”* ;
- c. direct marketing should include the promotion of the political aims and ideals of the data controller. The sending of a communication by a controller where the nature of such

¹ 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.

communication is not political but is intended to politically influence the data subject by means of a personal message, such as the sending of greeting cards, should also fall within the meaning of these Guidelines.

3. Principles of Data Protection

Political parties, candidates and those involved in processing of personal data, as part of canvassing or campaigning activities should ensure that they meet their data protection law responsibilities. This means that controllers should adhere to the data protection principles outlined in article 5 of the Regulation, which can be summarised as follows:

- a. personal data should only be used lawfully, fairly and in a transparent manner (*'lawfulness, fairness and transparency'*);
- b. personal data should only be collected for one or more specified, explicit, and legitimate purposes, and cannot be used in a way that is incompatible with those purposes (*'purpose limitation'*);
- c. personal data should be is adequate, relevant and limited to what is necessary for the purpose it is processed (*'data minimisation'*);
- d. personal data should be kept accurate and up-to-date and erase or rectify any inaccurate data without delay (*'accuracy'*);
- e. personal data should not be retained for unreasonably long periods (*'storage limitation'*);
- f. personal data should be kept secured by using appropriate technical and/or organisational security measures (*'integrity and confidentiality'*); and
- g. the controller should be able to demonstrate compliance with the above principles (*'accountability'*).

Furthermore, a controller should also consider how to respond to data subjects' requests, particularly those seeking to exercise their data protection rights (*such as the right of access*), in a timely and effective manner, while keeping in mind that these requests should be responded to, without undue delay, and at least within one (1) month of receipt of the request.

4. Legal Basis of Processing

It is recognised that, to ensure a healthy democratic process, political parties and candidates, need to engage the interest of eligible voters by transmitting their political messages by means of a variety of communication methods.

Campaigners, like other controllers, are responsible for ensuring that any use of personal data is lawful. It is the responsibility of the controller to determine the legal basis for each processing activity, which may vary depending on the circumstances. When using consent as a legal basis for processing personal data, it should be freely given (the individual should have a real choice about whether to consent), specific (should relate to specific purpose), informed (the individual should have been given enough information to make an informed decision about whether or not to consent), and unambiguous (it should be clear and deliberate). In this context, the controller should process personal data, for the purpose of carrying out this processing activity, only after obtaining the data subject's consent. It is the responsibility of the controller to demonstrate, at any time when requested, that the data subject has indeed consented to the processing of their personal data.

Some of the personal data used by campaigners may fall under the category of special category of personal data, such as data indicating the political opinion of a particular data subject. In this regard, the Regulation provides special protection to the processing of special categories of personal data. This implies that, in the context of electoral activities, that for processing to be lawful, it should rely on a legal basis under article 6 of the Regulation, but also, if it **constitutes processing of special category of data**, meet one of the exceptions set out under article 9(2) of the Regulation.

In terms of Article 9(2)(d) of the Regulation, political parties should, in the course of their legitimate activities and with appropriate safeguards, process special categories of personal data concerning their registered members and of other persons who have regular contact with the party.

The controller should take all necessary measures to identify itself in any political message sent for political campaigning purposes and should observe the requirements for processing as listed under article 5 of the Regulation, particularly, the purpose limitation principle, which establishes that personal data, legitimately collected by the controller, should be solely processed for the purpose for which such data has been originally collected.

5. Postal and Telephony Communications

The controller may use the personal data contained in the Electoral Register or in the printed or online telephone directory services for the purpose of sending personalised political campaigning material or voice messages to the respective registered voters or listed subscribers, unless the data subject gives notice to object such processing.

6. Door-to-Door Canvassing

In the case of door-to-door canvassing, the controller should ensure that appropriate safeguards are in place to correctly record and protect any personal data gathered, including any data that reveals political beliefs. If constituents are requested for their contact details, the controller needs to ensure that such constituents consent to follow up contact with them. Moreover, it should be made clear to voters that they are not under an obligation to provide any information and that their data is only being collected with their permission.

7. Generalised Political Communication

Unaddressed postal mail sent to *'the occupant'* or *'the resident'* does not constitute personal data within the meaning of article 4(1) of the Regulation. Hence, the provisions of the Regulation and the Act should not apply where no personal data is processed by the controller for the purpose of carrying out a political campaign, for instance, where the communication material is manually distributed in letter boxes. Persons engaged to distribute such material should, nevertheless, respect those households who would have indicated their objection on the letter boxes to receiving political or any other types of marketing material.

8. Electronic Direct Marketing and Canvassing

The controller should ensure that political communications sent by electronic means are only addressed to data subjects who have given their prior consent or who have themselves provided their email addresses or mobile numbers during the membership enrolling process or during a political or related activity. Where the contact details are not obtained directly from the individual but from other sources, such as activists or other third parties who are in contact with the data subject, the controller should ensure that such consent had been obtained and documented. Additionally, in those cases to

ensure the transparency of processing, the controller should provide the data subject with the necessary information as stipulated in article 14 of the Regulation.

If campaigners want to engage in online political advertising or utilize third-party services for electoral purposes, they should ensure that they have a legal basis for exchanging personal data with the third-party service or advertising platform (especially since this may constitute processing of special category data in accordance with article 9 of the Regulation). Individuals should also be notified regarding any third parties with whom their personal data will be shared. Therefore, where the controller engages the services of a third party contractor to send bulk political communications on its behalf and specifically to mobile numbers which are held on the database of the same contractor, the controller should remain responsible for the messages that are transmitted. In these circumstances, the controller should ensure that the contractor has indeed obtained the consent of those recipients to whom the marketing messages are directed by retaining the necessary documentation indicating their wishes.

9. Online Canvassing

9.1 Websites

In instances where controllers operate a website, it should be guaranteed that all the transparency obligations are fulfilled by having an easily accessible, clearly visible, and easy to understand data protection statement. Furthermore, if such website uses cookies to collect user data, it should clearly explain this, detailing the terms of cookies usage and providing a means of giving or refusing consent to place cookies².

9.2 Social Media

The use of social media has become a widely adopted tool which may be used by a controller to carry out a political campaign. This means that the controller's activities, carried out through the registered profile or account, should be subject to the legal criteria and principles set out in the Regulation, where the principal legitimate basis for the processing of personal data should be the data subject's consent.

² For more information, refer to the *Guidance Note on Cookies Consent Requirements* available at: <https://idpc.org.mt/idpc-publications/guidance-note-on-cookies-consent-requirements/>

It is to be clarified that where a user of a social networking site, hence a data subject, associates himself with the profile or account of the controller by, for instance, liking or following a page, that action should be tantamount to consent. Consequently, any personal information available on the user's profile, such as a mobile number or an email address, should be used by the controller for political campaigning purposes. In any case, users should be provided with effective means, to exercise their right to object to the processing of their personal data for the purposes of the campaign, free of charge and without having to state the reason thereof.

10. Transparency

When using personal data in political campaigning, it is essential that controllers are transparent about the processing and provide the constituents with information on who the controller is and how can the controller be contacted; why is the data being collected and with whom the data will be shared, how long the controller will keep it, what is the legal basis for this processing; and outline the data protection rights of the data subjects.

11. Opting-Out

Controllers should provide data subjects with clear information to appropriately inform them of their right to object, at no cost, from receiving further communications. The opt-out option should be included on each communication and provide the data subject with a clear and simple option to exercise such right.

11.1 Opting Out from Telephone Campaigning

In the case of telephone calls, the controller should respect the decision of those constituents who expressly indicate the wish not to proceed with the call and delete their personal contact details accordingly.

11.2 Opting Out from Electronic Direct Marketing

An information clause should be included on each outgoing message informing the recipient of their right to oppose, at no charge and in a simple manner. Whereas in the case of emails the use of an unsubscribe link is the best-practice technical solution, in the case of SMSs, the controller could adopt

best-practice measures to ensure that the necessary contact information is provided to the data subject giving them an easy way to unsubscribe. In instances whereby the data subject is not capable of replying to the received message to unsubscribe, the controller should adopt other methods including the insertion of a contact number or an email address on each message.

12. Contacting Voters on Election Day

The controller may, on election day, adopt a system designed to implement a structured and dedicated process to contact eligible voters and encourage them to cast their vote, provided that the contact details have been supplied by the data subject himself, obtained from a telephone directory or made available on an open social media profile or account. A data subject should, nevertheless, have the right to oppose from proceeding with the call or to be re-contacted.

13. Conclusion

Compliance with data protection laws, especially during electoral activities and political campaigns, is critical for safeguarding democracy. It is also a method of preserving citizens' confidence, as well as the integrity of elections. Political parties, candidates and those providing services in the context of political campaigns, should be prepared to demonstrate compliance with the data protection principles, particularly the principles of lawfulness, fairness, and openness. To guarantee fair and lawful processing, the controller should assume the legal responsibility to comply with these Guidelines.