Putting the Fox in Charge? Political Parties and the GDPR: An Irish Perspective

Maeve McDonagh* & Mary Donnelly*

In the wake of Cambridge Analytica, the use of personal data by political parties has been subject to increased scrutiny. Given the specific policy challenges which such use poses, this article examines the conditions for the lawful processing of personal data under the General Data Protection Regulation (GDPR), as it applies to political parties. It identifies the extensive flexibilities afforded by the GDPR to Member States and argues that granular Member State analysis is required if the GDPR regime is to be meaningfully evaluated in this context. Using Ireland as a detailed case study and referencing the equivalent provisions of the UK Data Protection Act 2018 (DPA UK) for comparison, the article examines the different ways in which these Member States responded to the flexibility afforded by the GDPR. Based on this, the article argues that closer engagement with the issue of political parties by the European Data Protection Board is needed in order to provide a more fine-grained response which bridges the space between the 'one size fits all' approach in the GDPR and the wide-ranging discretion of the flexibilities afforded to Member States.

Keywords: GDPR, political parties, lawful processing, freedom of expression, public interest, European Data Protection Board

1 INTRODUCTION

Political parties have always collected personal data relating to their constituents and potential voters, whether through traditional doorstep conversations involving party canvassers or through political 'clinics'. This information may include constituents' personal details, their likely voting habits, and the issues that concern them and that could influence their voting behaviour.[1] For many years, scant attention was paid in data protection circles to the processing of personal data by political parties.[2] The situation changed utterly in early 2018 when the Cambridge

* Law School, University College Cork, Ireland. Email: m.mcdonagh@ucc.ie.

1 In fact, the impact of information gathered in this way on the development of political policy is unclear: *see* P. Öhberg & E. Naurin, *Party-Constrained Political Responsiveness: A Survey Experiment on Politician's Response to Citizen-Initiated Contacts*, 46(4) Brit. J. Pol. Sci. 785 (2016); M. Baekgaard et al., *The Role of Evidence in Politics: Motivated Reasoning and Persuasion Among Politicians*, Brit. J. Pol. Sci. (2017), https://doi-org.ucc.idm.oclc.org/10.1017/S0007123417000084.

2 The Art. 29 Working Party did not, e.g. issue an Opinion or Recommendation specifically focusing on this issue in over twenty years of operation. Academic legal commentary on this issue was also sparse.

McDonagh, Maeve & Donnelly, Mary. 'Putting the Fox in Charge? Political Parties and the GDPR: An Irish Perspective'. *European Public Law* 26, no. 2 (2020): 363–390.

Analytica revelations placed the spotlight firmly on the processing of personal data by political parties/political campaigners.[3] It became clear that both the nature of personal data being collected and its sources had undergone a radical transformation, in particular as a result of the growing use of social media and online advertising for political purposes.

The risks associated with the move away from more traditional approaches to the processing of personal data by political parties have been well documented.[4] The European Data Protection Board (EDPB) has, for example, warned that the extension to usage for political purposes of certain data processing techniques 'poses serious risks, not only to the rights to privacy and to data protection, but also to trust in the integrity of the democratic process'.[5] Problematic techniques identified include the use of predictive tools to classify or profile people's personality traits, characteristics, mood and other points of leverage 'in order to allow assumptions to be made about deep personality traits, including political views and other special categories of data'.[6]

Against this backdrop, the strengthening of data protection law with the entry into force in May 2018 of the General Data Protection Regulation (GDPR)[7] has significant implications for political parties. The operation of the GDPR in this context must be considered alongside the fundamental rights protected by the Charter of Fundamental Rights of the EU (CFEU).[8] The fundamental rights to respect for private life[9] and data protection[10] are clearly relevant to the processing of personal data by political parties. The protection of these rights must however be weighed against the need to protect other rights that are relevant to the activities of political parties, principally the right to freedom of expression and information[11] and the right to vote and stand as a candidate.[12]

---

3 Practices revealed included the use of personal data obtained from social media sites, data brokers and publicly available information sources to micro-target individual voters with messages in keeping with their particular interests and values: *see* European Data Protection Supervisor, *Opinion 3/2018 EDPS Opinion on Online Manipulation and Personal Data* 11–12 (19 Mar. 2018).

4 C. Bennett, *Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications*, 13(3/4) Surveillance & Soc'y 370 (2015); I. Rubinstein, *Voter Privacy in the Age of Big Data*, Wis. L. Rev. 861 (2014); F. Zuiderveen Borgesius et al., *Online Political Microtargeting: Promises and Threats for Democracy*, 14(1) Utrecht L. Rev. 83 (2018).

5 EDPB, *Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns* 1 (Mar. 2019).

6 *Ibid*.

7 Regulation (EU) 2016/679 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, [2016] OJ L 119/1.

8 [2012] OJ C 326/391; *see* M. Mostert et al., *Big Data in Medical Research and EU Data Protection Law: Challenges to the Consent or Anonymise Approach*, 24(7) Eur. J. Hum. Genetics 956–960, 957 (2016).

9 CFEU, Art. 7.

10 CFEU, Art. 8.

11 CFEU, Art. 11.

12 CFEU, Art. 39 protects the right to vote and stand as a candidate at elections to the European Parliament.

This article will focus on one aspect of the GDPR, the conditions for the lawful processing of personal data, including special categories of personal data.[13] It will consider the bases for the processing of such data by political parties[14] under the GDPR and will identify the extensive flexibilities afforded by the GDPR to Member States in setting the rules by means of national legislation. Then, using Ireland as a detailed case study and referencing the equivalent provisions of the UK Data Protection Act 2018 (DPA UK) for comparison, the article will examine the rules introduced at domestic level for the processing of personal data by political parties. This will facilitate an analysis of the broader implications of the flexibility afforded by the GDPR to Member States.

2 PROCESSING OF PERSONAL DATA BY POLITICAL PARTIES

Although political parties process personal data in a wide range of circumstances, the two main activities giving rise to such processing are: constituency work and political campaigning.[15]

Politicians may engage with the personal data of constituents when undertaking constituency work.[16] They may, for example, make representations to public or to private bodies on behalf of a constituent, often at the request of that constituent or of their family members.[17] Such data can include sensitive personal data, for example health data.[18]

In the course of political campaigning, political parties may engage in a range of activities which generally have as their starting point the collection of personal data about potential voters.[19] The collection of personal data may be undertaken

---

[13] The special categories of personal data are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person and data concerning health or data concerning a natural person's sex life or sexual orientation: Art. 9(1).

[14] The term 'political party' is not defined in the GDPR and as will be seen in the discussion of the Irish position, relevant legislation may extend to elected representatives and/or candidates for election and to political campaigners who are not affiliated to a political party.

[15] B. Shiner, *Big Data, Small Law: How Gaps in Regulation Are Affecting Political Campaigning Methods and the Need for Fundamental Reform*, Pub. L. 362–379, 367 (2019).

[16] The nature and degree of constituency work varies across different states and in accordance with differences in the way politicians perceive and present themselves: *see* e.g. B. Cain, J. Ferejohn & M. Fiorina, *The Personal Vote: Constituency Service and Electoral Independence* (Cambridge MA: Harvard University Press 1987); *Parliamentary Roles in Modern Legislatures* (M. Blomgren & O. Rozenberg eds, Abingdon: Routledge 2012).

[17] Data Protection Commission of Ireland, *Guidelines on the Processing of Personal Data by Elected Representatives Under Section 40 of the Data Protection Act 2018*, at 2, https://www.dataprotection.ie/sites/default/files/uploads/2018-12/Section40Guidelines.pdf.

[18] *Ibid.*, at 1.

[19] Data Protection Commission of Ireland, *Elected Representatives, the General Data Protection Regulation and the Data Protection Act 2018*, at 2, https://www.dataprotection.ie/sites/default/files/uploads/2018-12/Introduction.pdf.

directly or indirectly. Direct collection of personal data from data subjects can come about in a traditional fashion, for example through the compilation of mailing lists of attendees at political meetings or, in the online environment, when for example visitors to a party website are invited to supply data through forms or portals.[20] Personal data can be indirectly collected by political parties when it is collected from public sources such as the electoral register[21] or when it is obtained from data brokers.[22]

Personal data can be used by political parties to communicate with potential voters for political marketing purposes. Parties can also use personal data to assist them in formulating and refining their policies in order to maximize their appeal to voters. Political parties increasingly engage in the commissioning of analysis by third parties of the personal data of potential voters.[23] Campaign data analysts develop models using this data to 'produce individual-level predictions about citizens' likelihoods of performing certain political behaviours, of supporting candidates and issues, and of changing their support conditional on being targeted with specific campaign interventions'.[24]

2.1 Political parties and the GDPR requirements

Amongst the core provisions of the GDPR are the data protection principles which are set out in Article 5 of the GDPR, the first of which requires that personal data be processed lawfully, fairly and in a transparent manner.[25] Building on this requirement, Article 6(1) provides that processing of personal data will only be lawful if and to the extent that at least one of a list of conditions set out in Article 6 applies. Political parties, in common with other data controllers,[26] must therefore be able to identify at least one condition in Article 6(1) that provides the

---

[20] Data Protection Commission of Ireland, *Constituency Office – Best Practice in the Workplace*, at 6, https://www.dataprotection.ie/sites/default/files/uploads/2018-12/Office%20Practices.pdf.

[21] P. Howard & D. Kreiss, *Political Parties and Voter Privacy: Australia, Canada, the United Kingdom and the United States in Comparative Perspective*, 15(12) First Monday 2 (2010), https://firstmonday.org/article/view/2975/2627.

[22] UK Information Commissioner, *Democracy Disrupted?: Personal Information and Political Influence* 50 (July 2018).

[23] *See* D. Kreiss, *Prototype Politics: Technology Intensive Campaigning and the Data of Democracy* (New York: OUP 2016).

[24] D. Nickerson & T. Rogers, *Political Campaigns and Big Data*, Harvard Kennedy School, Faculty Research Working Paper Series, RWP13-045 (Revised Feb. 2014).

[25] Article 5(1)(a).

[26] A 'data controller' is defined as '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 here: Art. 4(7).

basis for the processing by them of personal data. Where the personal data in question belongs to a 'special category'[27] of personal data, the processing of such data is prohibited by Article 9 of the GDPR unless at least one of the exceptions provided for in that article applies. For special categories of data, meeting the requirements of Article 9 is not necessarily sufficient to ensure lawfulness under Article 6. The Article 29 Working Party (A29WP)[28] has indicated that analysis has to be undertaken on a case-by-case basis as to whether Article 9 'in itself provides for stricter and sufficient conditions, or whether a cumulative application of both Articles [6] and [9] is required to ensure full protection of data subjects'.[29]

Before examining the application of Articles 6 and 9 to political parties in more detail, it should be noted that establishing the lawfulness of the processing of personal data by political parties is not sufficient to fulfil the obligations imposed by the GDPR on political parties. As emphasized by the EDPB:

> Even where the processing is lawful, organisations need to observe their other duties pursuant to the GDPR, including the duty to be transparent and provide sufficient information to the individuals who are being analysed and whose personal data are being processed, whether data has been obtained directly or indirectly.[30]

Thus in addition to demonstrating compliance with the data protection principles, political parties must deliver upon the other rights conferred on data subjects by the GDPR such as the rights of transparency,[31] access,[32] rectification[33] and erasure,[34] the right to data portability,[35] the right to object,[36] and the right not to be subject to a decision based solely on automated processing.[37]

---

27 The special categories of personal data are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person and data concerning health or data concerning a natural person's sex life or sexual orientation: Art. 9(1).

28 The Art. 29 Working Party on Data Protection was established under DPD Art. 29 to play an advisory role in respect of the protection of individuals with regard to the processing of personal data. Since the coming into force of the GDPR (on 25 May 2018), it has been replaced by the European Data Protection Board.

29 Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, European Commission* 15 (9 Apr. 2014). The articles referenced in Opinion 06/2014 are Arts 7 and 8 of the Data Protection Directive which are the forerunners of Arts 6 and 9 respectively of the GDPR.

30 EDPB, *supra* n. 5, at 2.

31 Articles 12–14.

32 Article 15.

33 Article 16.

34 Article 17.

35 Article 20.

36 Article 21.

37 Article 22.

2.2 Lawful processing of personal data: Article 6

Article 6 provides a list of lawful processing conditions, at least one of which must be satisfied. The most relevant of these in the context of political parties are: that the data subject has given consent to the processing of his or her personal data for one or more specific purposes[38]; that processing is necessary for the performance of a task carried out in the public interest[39]; and that processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.[40]

2.2[a] *Consent*

The GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[41] The A29WP Guidelines on Consent ('A29WP Consent Guidelines') notes that if the data subject has no real choice as to whether to consent, feels compelled to consent, or will endure negative consequences if they do not consent, then consent will not be valid.[42] The data subject must have the right to withdraw consent to processing at any time and it must be as easy to withdraw as to give consent.[43] The A29WP Consent Guidelines set out the minimum amount of information which should be provided to ensure that consent to data processing is informed. This consists of: the data controller's name (and those of any parties to whom the data will be transferred); the purpose of each of the processing operations for which the consent is sought; what (type of) data will be collected and used; the existence of the right to withdraw consent; information about the use of data for automated decision-making (where relevant); and the possible risks of data transfers due to absence of an adequacy decision or of appropriate safeguards.[44] Other information may also be required, with the core question being whether the information provided is sufficient in order to 'allow the data subject to genuinely understand the processing operations at hand'.[45]

---

38 Article 6(1)(a). The conditions for the granting of consent are set out in Art. 7.
39 Article 6(1)(e).
40 Article 6(1)(f).
41 GDPR, Art. 4(11). In assessing whether consent is freely given, 'utmost account' must be taken of whether the performance of a contract is made conditional on consent to data processing: *see* M. Donnelly & M. McDonagh, *Health Research, Consent and the GDPR Exemption*, 26 Eur. J. Health L. 97, 101–107 (2019).
42 *Guidelines on Consent Under Regulation 2016/679*, adopted on 28 Nov. 2017, rev'd and adopted 10 Apr. 2018, WP257 rev.01, 5.
43 Article 7(3).
44 *Guidelines on Consent Under Regulation 2016/679*, *supra* n. 42.
45 WP29 Consent Guidelines at 13.

Where data is collected directly from a data subject, consent to its processing can be obtained from the individual data subject, for example through asking him or her to tick a box granting the political party permission to use the data subject's contact details to advise him or her of party meetings, events and fundraising activities. Where data is collected indirectly, political parties need to ensure that the appropriate consent has been obtained from the individuals concerned at the point of collection. In the case of both direct and indirect collection of personal data, political parties must ensure that individuals are informed in line with transparency requirements under the GDPR.[46]

Relying on consent as the basis for the processing of personal data can be problematic for political parties because of the effort involved in ensuring that the requirements for informed consent are met. This problem is exacerbated by the nature of the processing of personal data in an era of Big Data analytics,[47] which means that even where they are positively disposed to meet their transparency obligations, data controllers, including political parties, often lack knowledge at the point of collection of the use to which the data being collected may be put.[48] As a result, it is unlikely that compliance with the consent requirement will often provide the basis for lawful processing by political parties.

2.2[b] *Article 6(1)(e): Processing in the Public Interest*

Personal data can be processed where it is 'necessary for the performance of a task carried out in the public interest'. The requirement that the processing be 'necessary' means that it must be genuinely necessary as opposed to being unilaterally imposed on the data subject by the controller.[49] An important threshold requirement for the invocation of Article 6(1)(e) is that the basis for the processing of personal data in the public interest must be laid down by EU or Member State law to which the data controller is subject.[50] The law must also meet an objective of public interest and be proportionate to the legitimate aim pursued.[51] Member

---

46 *See* Arts 12–14. *See also* Art. 29 Working Party, Guidelines on transparency under Regulation 2016/679 adopted on 29 Nov. 2017, rev'd and adopted 11 Apr. 2018, WP260, rev.01.

47 M. Paterson & M. McDonagh, *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*, 44(1) Monash U. L. Rev. 1 (2018).

48 D. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1902 (2013); A. Mantelero, *The Future of Consumer Data Protection in the EU: Re-thinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics*, 30 Computer L. & Sec. Rev. 643, 645 (2014); F. Cate & V. Mayer-Schönberger, *Notice and Consent in a World of Big Data*, 3 Int'l Data Privacy L. 67, 67–68 (2013); UK Information Commissioner, *supra* n. 22.

49 *See* the discussion of 'necessary' in A29WP Opinion 06/2014 on the notion of legitimate interests of the data controller under Art. 7 of Directive 95/46/EC, European Commission 16 (9 Apr. 2014).

50 Article 6(3)(1).

51 Article 6(3)(2).

States may introduce more specific provisions to 'adapt the application of the rules' set out in Article 6(1)(e) by 'determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing'.[52] In particular, the legal basis for the processing of personal data under section 6(1)(e) may contain more specific provisions in respect of: general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing.[53] It is suggested that the adaptation of the rules envisaged by Article 6(3)(2) does not contemplate a weakening of GDPR rules by the Member States but rather the more detailed specification of such rules, in particular where Member States have 'sector-specific laws in areas that need more specific provisions'.[54]

Although not explicitly stated in the text of the GDPR, it appears that Article 6(1)(e) can be used as the basis for the processing of personal data by political parties. This is supported by recital 45 which states that it should 'be for Union or Member State law to determine whether a controller performing a task carried out in the public interest should be a public authority or another natural or legal person governed by public law'. Since political parties are governed by public law (in the form of electoral law), they fall into the category of bodies referred to in recital 45. The processing of personal data by political parties can be said to be in the public interest on the grounds that freedom of political expression on the part of political parties results in a well-informed electorate who can more effectively exercise their franchise[55] and the existence of an informed and knowledgeable citizenry is one of the most important requirements for the functioning of representative democracy in that it helps to structure the participation and competition that characterizes democracies.[56]

The applicability of Article 6(1)(e) to the processing of personal data by political parties and candidates is supported by the European Commission which, in a report on the application of EU data protection law in the electoral context, stated that '[p]olitical parties and foundations can also process data on the grounds of public interest if so provided by national law'.[57] The use of Article 6(1)(e) as a

---

52 Article 6(2).
53 Article 6(3)(2).
54 Recital 10.
55 T. Besley & R. Burgess, *The Political Economy of Government Responsiveness: Theory and Evidence from India*, 117(4) Q. J. Econ. 1415 (2002); R. Pande, *Can Informed Voters Enforce Better Governance? Experiments in Low-Income Democracies*, 3 Ann. Rev. Econ. 215–237 (2011).
56 G. Rawnsley, *Political Communication and Democracy* 15 (Palgrave MacMillan 2005).
57 European Commission, *Free and Fair Elections: Guidance on the Application of Union Data Protection Law in the Electoral Context*, COM(2018) 638 final at 5.

basis for the processing of personal data by political parties has the advantage from the political parties' point of view of providing a clear legal basis for the processing by them of personal data. It does, however, raise the question of how Member States determine 'public interest' in the political sphere. Ultimately, the GDPR leaves the determination of public interest to the discretion of Member States, which leaves open the possibility of manipulation to suit the agendas of the political parties in power in those Member States.

2.2[c] *Article 6(1)(f): Processing Necessary for the Purposes of the Legitimate Interests of the Controller or a Third Party*

Article 6(1)(f) permits the processing of personal data necessary for the purposes of the legitimate interests pursued by the controller or by a third party. It includes the important proviso that processing on the basis of this condition may not be undertaken where 'such interests are overridden by the interests or fundamental rights and freedoms of the data subject'. Recital 47 states that the existence of a legitimate interest needs careful assessment, including whether a data subject can reasonably expect, at the time and in the context of the collection of the personal data, that processing for that purpose may take place.

The application of the legitimate interests condition calls for a balancing test in which the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject.[58] The A29WP states that in carrying out the balancing test, account must be taken of the nature and source of the legitimate interests and of the impact of the processing on the data subjects. Factors relevant to assessing the nature and source of the legitimate interests identified by the A29WP include: whether the exercise of any fundamental rights are at stake; the public interest or the interest of the wider community; whether any other legitimate interests are at stake; and the extent of legal and cultural/societal recognition of the legitimacy of the interests.[59] In terms of the impact on the data subject, the relevant factors are: the range of both positive and negative consequences of the processing; the nature of the data[60]; the way the data are being processed; the reasonable expectations of the data subject; and the status of the data controller and data subject.[61] The fundamental rights of which account must be taken are those provided for in the CFEU. The A29WP specifically references the need to balance the rights to privacy and to

---

[58] A29WP, *supra* n. 49, at 23.
[59] *Ibid.*, at 34–36.
[60] The more sensitive the data, the more it will weigh the balance in favour of the data subject's interests: A29WP, supra n. 49, at 39.
[61] *Ibid.*, at 37–40.

protection of personal data against other rights including the right to freedom of expression and information.[62]

Balancing the data controller's legitimate interests against the interests and fundamental rights of data subjects requires careful assessment which must take into account the circumstances of the specific case. It also requires the undertaking of a proportionality analysis as provided for under Article 52(1) of the CFEU.[63] The A29WP cites the use by a candidate of the electoral register to send each potential voter in her election district an introduction letter promoting her campaign as an example of the exercise of the right to freedom of expression which renders the processing of personal data legitimate under Article 6(1)(f).[64] The use of the register for such a purpose was viewed by the A29WP as coming within the reasonable expectation of individuals, provided that it takes place in the pre-election period. In such circumstances, the interest of the controller was said to be clear and legitimate. The 'limited and focused use of the information' was viewed by the A29WP as tipping the balance in favour of the legitimate interest of the controller.

On the other hand, the collection and use of personal data to micro-target voters through sending messages in a manner that permits a political party to 'misleadingly, present itself as a one-issue party to different individuals'[65] could be viewed as not being justified on the basis of the legitimate interests of the political party. Thus, while it appears that the legitimate interests of a political party could well be invoked as the basis for the lawful processing of personal data by the political party, the balancing exercise and the proportionality analysis required make the operation of this basis both uncertain and potentially onerous.

2.3 Processing of special categories of personal data: Article 9

Article 9(1) prohibits the processing of 'special' categories of personal data (which includes data in respect of political opinions[66]) unless one of the exemptions in Article 9(2) applies. The most relevant exemptions in respect of political parties are: that the data subject has given explicit consent to the processing of his or her personal data for one or more specific purposes[67]; that processing is carried out in the course of its legitimate activities by a not-for-profit body with a political,

---

62 *Ibid.*, at 34.
63 CFEU, Art. 52(1). On the relationship between Art. 6(1)(f) GDPR and Art. 52(1) CFEU *see* D. Clifford & J. Ausloos, *Data Protection and the Role of Fairness*, 37 Y.B. Eur. L. 110 (2018).
64 A29WP, *supra* n. 49, at 60.
65 Borgesius et al., *supra* n. 4, at 82.
66 For full list, *see supra* n. 13.
67 Article 9(2)(a). The conditions for the granting of consent are set out in Art. 7.

philosophical, religious or trade union aim[68]; and that processing is necessary for reasons of substantial public interest.[69]

2.3[a] *Explicit Consent: Article 9(2)(a)*

The A29WP Consent Guidelines state that the term 'explicit' refers to the way consent is expressed by the data subject and requires that the data subject have given an express statement of consent.[70] The same informational requirements for informed consent apply in relation to the giving of explicit consent as are outlined in the A29WP Consent Guidelines concerning consent to the processing of personal data under Article 6(1)(a).[71] The use of a written statement of consent signed by the data subject is described by the A29WP as removing all possible doubt as to whether consent was explicit. Obtaining explicit consent by means of a telephone conversation is also identified by the A29WP as acceptable, provided that 'the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation)'. Acceptable indicators of explicit consent in the online context referred to by the A29WP include: the filling in an electronic form, the sending of an email, the uploading of a scanned document carrying the signature of the data subject and the use of an electronic signature.[72]

Having to rely on explicit consent as the basis for the processing of personal data would be likely to be viewed as especially demanding by political parties. Not only would the issue of meeting the requirements for informed consent and transparency arise but the standard required in establishing explicit consent would be significantly greater than that for consent simplicities. Thus, consent is even less likely to be the basis for political parties' processing of special categories of data.

2.3[b] *Processing by a Not-for-Profit Body with a Political Aim: Article 9(2)(d)*

The exemption in Article 9(2)(d) applies where the processing of special categories of data is carried out:

> in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to

---

68 Article 9(2)(d).
69 Article 9(2)(g).
70 A29WP Consent Guidelines, at 18.
71 *Ibid.*, at 13.
72 *Ibid.*, at 18–19.

> 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.

Assuming that political parties qualify as not-for-profit bodies with a political aim, this provision can be summarized as permitting the processing by political parties of special categories of personal data subject to the following conditions:

(1) that the processing be undertaken by political parties in the course of their legitimate activities and with appropriate safeguards;
(2) that the processing relates solely to members or former members of the political party or to persons who have regular contact with it in connection with its purposes;
(3) that the personal data may not be disclosed outside the political party without the consent of the data subjects.

It is notable that Article 9(2)(d) is not limited to the processing of personal data revealing political opinions but rather it applies to the processing by such bodies of any of the special categories of data. Thus, provided that the conditions referred to in exception 9(2)(d) are fulfilled, it could be used as the basis for processing by a political party of data relating to an individual's racial origin, for example.

In order to avail of the Article 9(2)(d) exemption, the processing must be undertaken in the course of the processor's 'legitimate activities', a term which is not defined. The level of 'appropriate safeguards' required to invoke exception 9 (2)(d) is also not specified, leaving it open to Member States to specify such safeguards in national legislation.[73] The personal data must relate to 'members or former members' of the body in question. It cannot, for example, be used by a political party to process data of prospective members or voters.[74] The scope of the term 'persons who have regular contact with' a political foundation or party 'in connection with its purposes' has been explored by the French data protection supervisory authority, the Commission Nationale de l'Informatique et Libertés (CNIL), which has drawn a distinction between regular contact and casual contact in this context. The CNIL has defined regular contacts as those who 'engage with a political party in a positive way in order to maintain regular exchanges in relation to the party's political action'. The CNIL has listed the following as coming within the scope of regular contacts for the purposes of Article 9(2)(d): those who follow someone on Twitter or become 'friends' on Facebook and, more generally, people who, through social networks, have clearly manifested their willingness to

[73] European Digital Rights (EDRi), *Proceed with Caution: Flexibilities in the General Data Protection Regulation* 10 (5 July 2016).
[74] European Commission, *supra* n. 57, at 6.

maintain regular contact with the party policy or candidate. On the other hand, according to CNIL, those who merely 'like', comment, share or 'retweet' content posted on social networks must be considered to be casual rather than regular contacts.[75]

While Article 9(2)(d) provides a useful basis for the processing of special category personal data by political parties, it is limited in some respects. In particular, it restricts political parties to processing personal data of members, former members, or persons who have regular contact with it. Furthermore political parties are not allowed to disclose data processed under Article 9(2)(d) to third parties, such as analytics companies: it can only be disclosed within the political party or foundation.[76]

2.3[c] *Processing Necessary for Reasons of Substantial Public Interest: Article 9(2)(g)*

The exemption set out in Article 9(2)(g), which applies where 'processing is necessary for reasons of substantial public interest on the basis of Union or Member State law',[77] is, like its counterpart in Article 6, reliant on EU or national law to provide the basis for such processing. The relevant law must be proportionate to the aim pursued, it must respect the essence of the right to data protection, and it must provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[78] In contrast to Article 6(1)(e), Article 9(2)(g) does not provide for the introduction by Member States of more specific provisions to 'adapt the application of the rules' set out in that article.

The requirement that the public interest be 'substantial' clearly sets a higher threshold for the application of exception in Article 9(2)(g) than is required by Article 6(1)(e) thereby rendering it more difficult to use this provision as the basis for the processing of special categories of personal data for electoral purposes. Further detail on this exemption is provided by recital 56. This recital supports the processing by political parties of personal data on political opinions on the basis that 'the operation of the democratic system in a Member State requires that political parties compile' such data. The processing must be 'in the course of

---

[75] Commission Nationale de l'Informatique et Libertés (CNIL), '*Elections 2016/2017: quelles règles doivent respecter les candidats et partis?* 18 (2016), https://www.cnil.fr/fr/elections-2016-2017-quelles-regles-doivent-respecter-les-candidats-et-partis as cited in C. Bennett, *Political Opinions, Political Affiliations, Political Behavior and Political Inferences: The Protection of Privacy in the Data-Driven Election*. *See also* C. Bennett, *Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America?*, 6(4) Int'l Data Privacy L. 261 (2016).

[76] European Commission, *supra* n. 57, at 5.

[77] And provided that certain conditions are met viz that the law is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

[78] Article 9(2)(g).

electoral activities' and 'appropriate safeguards' must be in place. There is no definition in the GDPR of either term. The European Commission has acknowledged that political parties can process special categories of data on the basis of Union or Member State law if there is substantial public interest and provided that appropriate safeguards are in place.[79] The exemption together with recital 56 has been described as legitimizing 'the UK practice of political parties compiling regional and wider databases on the political allegiances of all households, without the consent of the data subjects'[80] though it is clear that this is only possible under Article 9(2)(g) where such practices are permitted by law. As in the case of Article 6(1)(e), the use of this basis for the processing of personal data by political parties has the advantage from the parties' point of view of providing a clear legal basis for the processing by them of personal data.

3 APPLYING THE GDPR TO POLITICAL PARTIES: MEMBER STATES RESPONSES

Although introduced as a directly effective Regulation with the stated goal of harmonizing the data protection laws of the Member States, the GDPR contains a number of so-called 'flexibility' provisions that allow the Member States to set the rules in various contexts by means of national legislation.[81]

Where Member States seek to facilitate the processing of personal data by political parties on the basis that it is necessary for the performance of a task carried out in the public interest under Article 6(1)(e) or to facilitate the processing of special categories of personal data on the basis that it necessary for reasons of substantial public interest under Article 9(2) (g), the basis for such processing must be laid down in national legislation. The GDPR also implicitly requires domestic legislation to be introduced specifying the nature of the appropriate safeguards to be put in place for the processing by political parties of special categories of personal data on the basis of the legitimate interests of the political party under Article 9(2)(d).

3.1 Permitted flexibilities: The policy context

While permitting Member States to specify rules for the processing of personal data in certain circumstances facilitates the taking into account of different domestic legal imperatives, it also potentially undermines the operation of the GDPR. The

[79] European Commission, *supra* n. 57, at 5.
[80] EDRi, *Flexibilities in the General Data Protection Regulation* 11 (2018), https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf.
[81] EDRi, *Proceed with Caution: Flexibilities in the General Data Protection Regulation* 1 (5 July 2016).

non-governmental organization European Digital Rights has, for example, complained that in some areas the flexibilities provided for 'are so broad as to give states almost complete freedom to evade the normal requirements of the Regulation in large areas'.[82] In respect of political parties, concern has been expressed that Member States may take the opportunity to avail of the permitted flexibilities in a manner that, deliberately or otherwise, erodes the protection afforded by the GDPR. Ailidh Callander has, for example, argued that the flexibilities in respect of political parties have led to 'the jarring outcome that certain national laws in this way invites[sic] data exploitation rather than data protection'. [83] Issues concerning the implementation of the GDPR in its application to political parties via national legislation have been identified in several jurisdictions, including Romania,[84] Spain,[85] the UK[86] and Ireland.[87]

The GDPR flexibilities may also introduce significant variations in the operation of the GDPR at national level[88] thus reducing the extent to which a harmonized approach to the processing of personal data will be achieved under the GDPR. Such an outcome would clearly be inconsistent with the requirement of recital 10 of the GDPR that 'the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States'. A lack of harmonization is problematic in so far as the law of one Member State could facilitate the collection of data in cross border or online contexts for reasons that other Member States may not agree with.[89] In the context

82 *Ibid.*, at 3.

83 A. Callandar, *GDPR Loopholes Facilitate Data Exploitation by Political Parties*, 3 GDPR Today (25 Mar. 2019) https://www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties/.

84 Valentina Pavel, *European Commission Urged to Investigate Romanian GDPR Implementation*, 3 GDPR Today (25 Mar. 2019), https://www.gdprtoday.org/european-commission-urged-to-investigate-romanian-gdpr-implementation/.

85 Access Now, *MEP Sophie In't Veld Sent Letter to EDPB and Commission on Questionable Spanish Implementation of the GDPR*, GDPR Today (17 Dec. 2018), https://www.gdprtoday.org/mep-sophie-int-veld-sent-letter-to-edpb-and-commission-on-questionable-spanish-implementation-of-the-gdpr/; Open Rights Group, *Spain: DPA Limits the Use of Data in Political Campaigning*, 3 GDPR Today (25 Mar. 2019), https://www.gdprtoday.org/spain-dpa-limits-the-use-of-data-in-political-campaigning/.

86 The Independent, *UK Parties Poised to Gain Data Powers to Work Out How People Are Likely to Vote, Despite Cambridge Analytica Scandal* (22 Mar. 2018); Open Rights, *The Missing Piece from the DCMS Report? Themselves*, https://www.openrightsgroup.org/blog/2019/the-missing-piece-from-the-dcms-report-themselves; GDPR Today, *GDPR Loopholes Facilitate Data Exploitation by Political Parties*, https://www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties/; Privacy international, *UK Data Protection Act 2018 – 339 Pages Still Falls Short on Human Rights Protection* (13 June 2018), https://www.privacyinternational.org/blog/2074/uk-data-protection-act-2018-339-pages-still-falls-short-human-rights-protection.

87 Irish Times *New Bill Will Allow Harvesting of Personal Data for Elections, Experts Say* (19 Mar. 2018).

88 *Ibid.*

89 EDRi, *supra* n. 81, at 11.

of political parties, these differences are not just inconveniences but may directly impact on the operation of democratic processes in Member States.

Because of the level of flexibility permitted, a full understanding of the implications of the GDPR requires a close analysis of how individual Member States are availing of the permitted flexibilities. The approach adopted by the Irish Data Protection Act 2018 (DPA) is analysed below. As the location of the European headquarters of a number of the most globally significant social media companies, including Facebook, Twitter and Google the approach taken in Ireland could also potentially have ramifications for the processing of personal data by political parties in other jurisdictions. The analysis is presented against a backdrop of the broader Irish political context. Comparisons are made with the UK Data Protection Act 2018. This permits some broader conclusions to be drawn regarding the impact of the GDPR flexibilities.

3.2 Implementation of the GDPR's provisions concerning political parties in Ireland

The Irish legislature has long favoured a light touch towards the processing of data personal data for the purpose of electoral activities. This was evident in the transposition of the Data Protection Directive into Irish law[90] and a similar approach has been adopted in relation to the GDPR. It is worth pausing briefly to reflect on Irish political culture and why it might affect the willingness of the Irish legislature to fully embrace the protection of personal data in the electoral context.

3.2[a] *Background to the Irish Approach*

Michael Marsh has identified 'extensive door-to door canvassing by party workers and the candidates themselves' as a key feature of Irish politics.[91] The importance of this style of campaigning can be attributed to the significance of 'localism' in Irish politics[92] and in particular to the widely accepted view that the Irish electoral

---

[90] *See* e.g. the inclusion in the Data Protection Acts 1988–2003 of a lawful basis for the processing of data carried out by political parties in the course of electoral activities although no specific provision for processing of personal data on this ground had been provided for in Directive 95/46/EC: s. 2B(1)(x).

[91] M. Marsh et al., *The Irish Voter: The Nature of Electoral Competition in the Republic of Ireland* 5 (Manchester: Manchester University Press 2008); M. Marsh, *None of That Post-modern Stuff Around Here: Grassroots Campaigning in the 2002 Irish General Election*, 14 Brit. Elec. & Party Rev. 245, 246 (2004).

[92] M. Gallagher, *Candidate Selection in Ireland: The Impact of Localism and the Electoral System*, 10(4) Brit. J. Pol. Sci. 489, 491 (1980).

system is highly constituency oriented.[93] The emphasis on constituency is most commonly explained as being a consequence of Ireland's 'highly distinctive'[94] electoral system which consists of proportional representation based on a single transferable vote. A key feature of this system is that it involves multi-seat constituencies. This results in candidates in Irish elections facing 'significant pressure to distinguish themselves from their party colleagues, as in most constituencies several candidates face opponents from within their own party'.[95] One avenue open to candidates in terms of distinguishing themselves from competitors is to be seen to serve their constituents in a 'welfare-officer role' for individual constituents and/or as a promoter of the collective needs of their constituents.[96] Other reasons for strong constituency orientation of the Irish electoral system include: the small size of Irish society, inadequate parliamentary resources and procedures, problems in the administrative system and the weakness of local government.[97]

The strong emphasis placed by the Irish electoral system on serving the needs of constituents renders the collection of data concerning those constituents and their concerns essential in the eyes of candidates for elected office. The perceived importance of the processing of personal data for the purpose of electoral activities is borne out by the Oireachtas (parliamentary) debate concerning the lawful processing exception for data revealing political opinion in the Data Protection Bill 2018. The Minister responsible for promoting the Bill referred to the processing of data for electoral activities as allowing 'elected representatives and candidates for elective office to reflect the concerns, anxieties and priorities of the citizens of the State, that is, the electorate'.[98] Another contributor to the debate sought reassurance that campaigners would continue to be allowed to process personal data gleaned from registers about 'what people thought, what they did not think and whether they were going to vote' for broad purposes, rather than merely for electoral purposes.[99] This reflects a concern evident throughout the parliamentary debates that the GDPR should not impinge on the ability of Irish political parties and elected representatives to engage with their constituents not

---

93 R. Katz, *The Single Transferable Vote and Proportional Representation*, in *Choosing an Electoral System: Issues and Alternatives* 143 (A. Lijphart & B. Grofman eds, New York: Praeger 1984); R. Carty, *Party and Parish Pump: Electoral Politics in Ireland* 134 (1981), in *Politics in the Republic of Ireland* 103 (J. Coakley & M. Gallagher eds, 6th ed., Abindgon, Routledge 2018).

94 D. Farrell & R. Sinnott, *The Electoral System*, in *Ibid*., Ch. 5, at 105.

95 M. Sudulich & M. Wall, *Keeping Up with the Murphys? Candidate Cyber-Campaigning in the 2007 Irish General Election*, 62(3) Parliamentary Aff. 456–475, 459 (2009).

96 M. Gallagher & L. Komito, *The Constituency Role of Dáil Deputies*, in *Ibid.*, Ch. 8, at 191.

97 Farrell & Sinnott, *supra* n. 94, at 105.

98 Deputy Charles Flanagan, *Seanad Éireann Debates*, 256(13) Thursday: Data Protection Bill 2018, Report Stage (22 Mar. 2018).

99 Senator Michael McDowell, *Seanad Éireann Debates*, 256(13) Thursday: Data Protection Bill 2018, Report Stage (22 Mar. 2018).

only at election time. As the closer analysis which follows reveals, the provisions of the DPA that touch on the processing of personal data by political parties strongly reflect this political concern.

3.2[b] *The Processing of Personal Data by Political Parties Under the DPA*

The DPA makes extensive use of the 'flexibility' afforded by the GDPR in terms of the processing of personal data by political parties. Specific provision is made in three sections of the Act (sections 39, 40 and 48) for the processing of personal data by political parties. A 'political party' is defined as a political party registered in the Register of Political Parties in accordance with section 25 of the Electoral Act 1992.[100]

3.2[b][i] Section 39: Communication with Data Subjects by Political Parties

Section 39(1) of the DPA permits political parties, members of the national and European parliaments and local authorities, and candidates for election to such bodies to use personal data in the course of their electoral activities in the State for the purpose of communicating in writing with data subjects. There is no requirement that such communication be initiated by the data subject thus permitting the sending of unsolicited communications. 'Electoral activities' are defined as including 'the dissemination of information, including information as to a person's activities and policies, that might reasonably be of interest to electors'.[101] Notably, electoral activities are not limited by this definition to the pre-election period. The impact of this provision is reinforced by the exclusion by the Act of the right to object to direct marketing in the case of political parties acting in the course of their electoral activities.[102]

Communication in accordance with section 39(1) is deemed to constitute 'the performance of a task carried out in the public interest' for the purposes of Article 6(1)(e) of the GDPR.[103] However, neither the Act nor the Explanatory Memorandum explain what type of personal data may be processed for the purpose of communicating with the data subject in the public interest and, in particular, whether the permitted data use extends beyond the type of information included in the electoral register viz names and addresses to include, for example, personal

---

[100] DPA, s. 2(1). Under s. 25 of the Electoral Act 1992, the Clerk of the Dáil is designated the Registrar of Political Parties. A political party may apply to the Registrar for registration as a political party if is it a party organized in the State or in a part of the State to contest a Dáil, European or local election.

[101] DPA, s. 39(4).

[102] DPA, s. 58.

[103] DPA, s. 39(2).

data from social media sites. The section does not make reference to the processing of special categories of data under Article 9 to which the higher standard of substantial public interest applies and therefore, it is difficult to see that it covers this kind of data. However, section 51 of the DPA creates a power under which any Minister of the Government[104] may, in consultation with other Ministers and the Data Protection Commission, make regulations to permit the processing of special categories of personal data for reasons of substantial public interest as referred to in Article 9.2(g) of the GDPR. This provides scope for the expansion of the public interest basis for the processing of special categories of personal data by means secondary legislation alone.[105]

Section 39 establishes an open-ended exemption for political parties and elected representatives based on the public interest. Notably, the section 39 exemption does not extend to other political campaigning e.g. to referendum campaigns which play an especially significant role in the Irish political landscape. Thus, it may impede campaigners who are not affiliated with a political party and in this way potentially undermines the democratic process in this context. From a privacy perspective, section 39 also raises questions with respect to the section's compatibility with the ePrivacy Directive which prohibits the sending of unsolicited electronic communications such as emails and text messages without consent.[106]

Ireland is not the only Member State to take a liberal interpretation of the public interest aspect of the GDPR in respect of political parties. In the UK, although no specific provision is made in the DPA UK for the sending of unsolicited communications by political parties, a provision was included in the DPA UK by way of government amendment which has greatly expanded the scope for political parties to process personal data on public interest grounds. Section 8 of DPA UK lists forms of processing which constitute 'processing necessary for the performance of a task carried out in the public interest' for the purposes of Article 6(1)(e). This includes processing necessary for 'an activity that supports or promotes democratic engagement'.[107] While the term 'democratic

[104] If the Minister is not the Minister for Justice and Equality, s/he must first consult with the Minister for Equality and Justice. In all cases, there must be consultation with the Data Protection Commission: DPA, s. 51(6).

[105] A similar provision in the UK Data Protection Act (s. 10(6)) was the subject of much criticism. *See* House of Lords Delegated Powers and Regulatory Reform Committee, Report on the Data Protection Bill, 6th Report of Session 2017–19, HL Paper 29, 6 (24 Oct. 2017).

[106] Directive 2002/58/EC, [2002] OJ L 201, 37, Art. 13. The ePrivacy Directive will shortly be replaced by the ePrivacy Regulation. Proposal for a Regulation 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/2017/010 final, 2017/03. A similar prohibition on the sending of unsolicited communications is provided for in Art. 16 of the proposed Regulation.

[107] Section 8(e).

engagement' is not defined in DPA UK, examples of activities that could come within its scope referred to by the Member of Parliament (MP) who introduced the amendment included 'communicating with electors, campaigning activities, supporting candidates and elected representatives, casework, surveys and opinion gathering and fundraising to support any of those activities'.[108] Thus, this exemption is not linked to formal political parties. This aspect of the UK approach has been severely criticized.[109] Apart from criticism of the scope of activities that may qualify as activities supporting or promoting democratic engagement, concern has also been expressed that the provision does not place any limits on who may undertake such processing. On the latter point, the 'UK' Information Commissioner contrasted its wide scope with the treatment of the processing of the sensitive data revealing political opinions which 'are only able to be used by registered political parties rather than by any data controller'.[110]

3.2[b][ii] Section 40: Processing of Personal Data Pursuant to Representations

Two forms of processing are provided for in section 40: the processing of personal data by or on behalf of an elected representative pursuant to a representation made to him or her by or on behalf of a data subject[111]; and the processing of personal data by a third party in response to a representation made by an elected representative.[112]

Section 40(1) purports to render lawful the processing of personal data and of special categories of personal data by or on behalf of an elected representative (who may or may not be a member of a political party)[113] for the purpose of enabling the representative to perform his or her functions in circumstances where the representative receives a request or representation from the data subject or from another person on behalf of the data subject.

Where the elected representative processes special categories of personal data, s/he is required to impose limitations on access to that data to prevent unauthorized consultation, alteration, disclosure or erasure of the data.[114] However, the nature of these limitations is not specified in the Act.

---

[108] M. P. Margot James, *Public Bill Committee, Data Protection Bill* 22 (13 Mar. 2018).
[109] *See* Privacy International, *supra* n. 86.
[110] UK Information Commissioner, *Data Protection Bill*, House of Commons Public Bill Committee – Information Commissioner's further written evidence at 10.
[111] DPA, ss 40(1)–(3).
[112] DPA, s. 40(4).
[113] An elected representative is defined for the purposes of s. 40 as 'a member of the national or European parliaments or of a local authority': DPA, s. 40(5).
[114] DPA, s. 40(3).

Requests or representations may be made on behalf of a data subject where the data subject has consented to the making of such a request or representation or where 'by reason of his or her physical or mental incapacity or age, he or she is unable to make a request or representation'.[115] The Act does not provide any further guidance on when a data subject is unable to make the request or representation. Elsewhere in the DPA, a 'child' is defined for the purposes of the application of the GDPR in the State as a person under the age of eighteen years[116] and it may be the case that a similar approach would be taken to the age-related aspect of section 40. Physical and mental incapacity raise further questions. In a world of telephones and digital communication, at what point does a physical incapacity render a person unable to make a request or representation? In respect of mental incapacity, the DPA does not identify the applicable standard to determine whether a person is unable to make a representation. When the Assisted Decision Making (Capacity) Act 2015 (ADMCA) comes into force in 2022, the statutory standard for capacity set out in this Act will apply. This requires that a person's capacity be assessed on the basis of his or her ability to understand, at the time the decision has to be made (in this case, the decision to make the request or representation), the nature and consequences of the decision in the context of the available choices at the time.[117] The ADMCA also requires that decisions made for a person who lacks capacity must be in accordance with the principles set out in section 8. These include that the decision, in this case the request or representation, must 'give effect, as far as practicable, to the past and present will and preferences of the relevant person, in so far as that will and those preferences are reasonably ascertainable'.[118] The legal obligation in this respect is on the person making the request or representation on behalf of the person lacking capacity rather than on the elected representative to whom the request is made.

Section 40 does not place any restrictions on the categories of persons who may make a request or representation to an elected representative on behalf of a data subject. Clearly parents or guardians would have legal authority to make a request on behalf of a child. For adults, it is not clear what, if any, legal basis there is for a third party to make a representation (unless s/he has been appointed and given powers in this regard under the Powers of Attorney Act 1996 or has been appointed to act on behalf of a person admitted to wardship). Thus, the legal basis

---

115 DPA, s. 40(2).

116 DPA, s. 29.

117 ADMCA, s. 3(1). A person lacks capacity if s/he is unable to understand the information relevant to the decision; retain the information for long enough to make a decision; use or weigh the information as part of making the decision; or communicate his or her decision: ADMCA, s. 3(2). The ADMCA also requires that a person 'shall not be deemed to be unable to make a decision unless all practicable steps' have been taken to help him or her: ADMCA, s. 8(3).

118 ADMCA, s. 8 (7).

for this aspect of s.40 is uncertain. This problem will continue after the ADMCA comes into force. Under the ADMCA, the only circumstances in which a person will be legally authorized to act on behalf of a person lacking decision-making capacity (including making requests or representations) will be where s/he has a power of attorney granting this power or has been appointed by the court to act as Decision-Making Representative for the person with specific powers in this regard.

Section 40(4) is concerned with the position under the GDPR of entities who process personal data in response to representations made by elected representatives. Section 40(4) makes it lawful for any person to disclose to an elected representative or to a person acting on his or her behalf, personal data and special categories of personal data of a data subject who has made a request or representation, or on whose behalf a request or representation has been made, in order to enable that elected representative to respond to that request or representation. Such data may only be disclosed to the extent that it is necessary and proportionate to enable the elected representative to deal with a request or representation. The making of such disclosures is also subject to 'suitable and specific measures' being taken to safeguard the fundamental rights and freedoms of the data subject.[119]

In contrast to section 39, section 40 does not identify which of the lawful basis for the processing of personal data it relies upon. While section 40(2) references obtaining the consent of the data subject, the consent in question is consent to the making of a representation on behalf of a data subject rather than consent to the processing of personal data. The activities permitted by section 40 are not stated to constitute the performance of a task carried out in the public interest for the purposes of Article 6(1)(e) or as 'necessary for reasons of substantial public interest' for the purposes of Article 9(2)(g). Assuming consent is not obtained, the only possible basis for the processing of personal data under section 40 would appear to be that of the legitimate interests of the data controller (Article 6(1)(f)). As identified above, this calls for a balancing test in which the legitimate interests of the controller must be balanced against the interests or fundamental rights and freedoms of the data subject.[120] In the case of processing of personal data under section 40(1), the legitimate interests in question are those of the elected representative whereas under section 40(4) the legitimate interests are those of the third party e.g. the service provider. While elected representatives have a legitimate interest in representing their constituents and third parties such as service providers have a legitimate interest in engaging with those who make representations on behalf of service users, it is not clear that the interferences with the privacy and

[119] *See* the discussion of 'suitable and specific measures' at text to *infra* n. 123.
[120] *See* text to *supra* n. 57.

autonomy of data subjects that such processing may entail would be overridden by the interests of the data controllers concerned. Moreover the legitimate interests of the data controller is only available as a ground for the lawful processing of ordinary personal data and cannot be used as the basis of the processing of special categories of data such as data relating to health. It is not clear that the processing of special categories of data under section 40 would meet any of the conditions for the processing of special categories of personal data provided for in Article 9.

The DPA UK also provides for both the processing of personal data by elected representatives and the processing of personal data by third parties resulting from requests made by individuals to elected representatives, although there is no direct equivalent to section 40. In the first place, provision is made in DPA UK for the processing of special categories of personal data[121] by elected representatives where this is done in connection with the discharge of the elected representative's functions and in response to requests from individuals.[122] The processing must be 'necessary for the purposes of or in connection with, the action reasonably taken by the elected representative in response to [the] request'.[123] A request may be made to an elected representative by someone other than the data subject and without the consent of the data subject in the following four situations: where in the circumstances, consent to the processing cannot be given by the data subject; where in the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing; where obtaining the consent of the data subject would prejudice the action taken by the elected representative; and finally where the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

Secondly, provision is made in DPA UK for the disclosure of special categories of personal data by data controllers to elected representatives in circumstances where the elected representative communicates with the controller in response to receiving a request from the individual.[124] The personal data must be relevant to the subject matter of the communication, and the disclosure must be necessary for the purpose of responding to that communication.[125]

The scope provided by DPA UK to persons other than the data subject to make requests to elected representatives is broader than in the Irish DPA. It is not clear from DPA UK the circumstances in which it might be said that the consent

[121] The processing by elected representatives of ordinary personal data would presumably fall within the scope of Art. 6(1)(e) of the GDPR on the basis that it is 'an activity that supports or promotes democratic engagement' as provided for in s. 8(e).
[122] DPA UK, s. 10(3) and Sch. 1, Part 2, para. 23.
[123] DPA UK, Sch. 1, Pt 2, para. 23(1)(b).
[124] DPA UK, s. 10(3) and Sch. 1, Part 2, para. 24.
[125] *Ibid*.

of the data subject 'cannot be given' or that the elected representative 'cannot reasonably be expected to' obtain consent or that the data subject can be said to have withheld consent unreasonably. On the other hand, the statutory language of DPA UK more closely reflects the language of the GDPR. The processing of special categories of personal data by elected representatives is expressly designated in DPA UK as being on 'grounds of substantial public interest' thus clearly bringing such processing within the scope of Article 9(2)(g). In contrast, the processing of personal data by elected representatives under section40 of DPA is not so designated thus casting doubts on its legality. Moreover unlike the Irish measure the requirement of necessity, which is a central feature of both Articles 6 and 9, features prominently in DPA UK.

3.2[b][iii] Section 48: Processing of Personal Data Revealing Political Opinions

Section 48 of the Act has its origins in Article 9(2)(d) of the GDPR. It states that subject to suitable and specific measures[126] being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of personal data revealing political opinions[127] shall be lawful where it is carried out in the course of its electoral activities in the State for the purpose of compiling data on peoples' political opinions by a political party, or a candidate for election to, or a holder of, elective political office in the State.[128]

While section 48 to some extent mirrors Article 9(2)(d) of the GDPR, there are some significant differences. On the one hand, the scope of section 48 is more limited than that of Article 9(2)(d) in that the former is confined to the processing of personal data revealing political opinions whereas Article 9(2)(d) applies in respect of processing of any of the special categories of data. On the other hand, the GDPR requirement 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' is omitted from section 48 and nor does section 48 reference the requirement of Article 9(2)(d) that the personal data must not be disclosed outside the body processing it without the consent of the data subjects. These omissions would appear to broaden the scope of section 48 beyond what is permitted by Article 9(2)(d). The equivalent provision under the DPA UK also

---

126 *See* the discussion of 'suitable and specific measures' *infra*.

127 Neither the GDPR (from which the term is taken) nor the DPA provide a definition of what constitutes a political opinion.

128 The exemption also applies to the Referendum Commission in the performance of its functions: DPA, s. 48(b). The Referendum Commission is a statutory body established under the Referendum Act 1998 as am by the Referendum Act 2001 and has the function of explaining to the public what a referendum proposal means; ensuring people know a referendum is being held; and, encouraging people to vote.

fails to limit its application to members or former members and thus also appears to exceed the scope of the GDPR.[129] However, the DPA UK contains important protections in that it provides for exceptions to the processing of personal data revealing political opinion where it is likely to cause substantial damage or substantial distress to a person[130] and where the data subject has given reasonable notice in writing to the controller requiring the controller not to process the personal data and the notice period has ended.[131]

3.2[b][iv] Section 36: Suitable and Specific Measures

The application of the exemptions in both section 40(4) and section 48 depend on the taking of 'suitable and specific measures' to safeguard the fundamental rights and freedoms of data subjects. Section 36(1) of the DPA sets out the measures to be deployed in circumstances where the DPA (or any regulations made under the DPA) requires that suitable and specific measures be taken. Such measures 'may include, in particular' a set of measures listed in section 36(1) which range from the relatively undemanding, such as the provision of specific targeted training for those involved in processing operations, through to requiring that the explicit consent of the data subject be obtained for the processing. Section 36(2) enables, but does not mandate, the introduction of regulations to specify safeguarding measures additional to those provided for in section 36(1) and to specify that the adoption of any measures is mandatory.[132] Examples of additional safeguarding measures include: measures relating to governance structures and to processes or procedures for risk assessment purposes, and organizational measures..[133]

In the absence of relevant regulations being introduced under section 36(2), the processing of personal data under section 40(4) by third parties in response to requests or representations from elected representatives and under section 48 of personal data revealing political opinion may be undertaken on the basis of safeguards as undemanding as the putting in place of training for those involved in the processing operations. It is questionable whether this meets the requirement in Article 9(2)(g) of the GDPR that processing of special categories of personal data

---

[129] DPA UK, Sch. 1, Pt 2, para. 22.
[130] *Ibid.*, para. 22(2).
[131] *Ibid.*, para. 22(3).
[132] In making regulations under s. 36(2), regard must be had to the public interest and to the need for the protection of individuals with regard to the processing of their personal data and to matters such as the nature, scope, context and purposes of the processing, the risks arising for the rights and freedoms of individuals, and the likelihood and the severity of the risks for the individuals concerned. To date the only measure introduced is the Data Protection Act 2018 (s. 36(2)) (Health Research) Regulations 2018 (S.I. No. 314 of 2018): *see* further Donnelly & McDonagh, *supra* n. 41.
[133] DPA UK, s. 36(3).

be carried out 'with appropriate safeguards'. An amendment to section 36 proposed during the course of the parliamentary debate sought to make the adoption of certain of the safeguards referenced in section 36 mandatory.[134] In opposing this amendment, which was ultimately defeated, the Minister responsible for the Bill stated that it 'would place a high burden on elected representatives making representations on behalf of constituents'.[135] The making of representations on behalf of constituents as well as the seeking of information and services on their behalf were referred to by the Minister as 'part of the routine work we do' and he concluded by noting that '[w]hile it is important that there is compliance with the legislation and the GDPR as we enter this new era, it is also important that we do not make matters so burdensome and onerous as to become unworkable'.[136] The light touch requirements in the DPA can be contrasted with a more rigorous approach in DPA UK. Here a, substantial public interest condition will only be met where the controller has an appropriate policy document in place which inter alia explains the controller's procedures for securing compliance with the data protection principles and as regards the controller's policies as regards the retention and erasure of personal data including giving an indication of how long such personal data is likely to be retained [137] and provided that a record is made of the processing.[138]

4 CONCLUSION

Given the wide range of political cultures across the EU, the task of developing pan-EU data protection measures applicable to the operations of political parties was inevitably going to prove challenging. The mixed messages emanating from the GDPR with respect to the processing of personal data by political parties have been compounded by the level of flexibility afforded by the GDPR to Member States to set their own rules through national legislation. While respecting different cultures and traditions, this also has the effect, to borrow from the old saying, of leaving the fox in charge of the henhouse.

The analysis of the Irish DPA conducted in this article found that Irish legislators have afforded themselves a good deal of latitude in processing data for political purposes. In some situations, arguably in the case of section 39 which allows political parties to process personal data in the course of their electoral

---

134 Amendment proposed by Deputy Claire Daly, Select Committee on Justice and Equality (2 May 2018).
135 Deputy Charles Flanagan, *Select Committee on Justice and Equality* (2 May 2018).
136 *Ibid*.
137 DPA UK, Sch. 1, Pt 4, para. 39.
138 *Ibid*., para. 41.

activities for the purpose of communicating with data subjects, this might simply be described as a generous interpretation of the GDPR requirements (although as noted, this may well run into difficulties under the ePrivacy Directive/ Regulation).[139] In others, however, the DPA approach to data processing by political parties seems to directly contravene the GDPR. This is the case with section 40 which allows for the processing of special categories of personal data in the context of a request or representation to an elected representative without a clear basis in the GDPR and with section 48 which fails to limit the processing of personal data revealing political opinions for electoral activities to data that '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' as is required under Article 9(2)(d) of the GDPR.

It is also important to remember that domestic legislation on the processing of personal data must also comply with the requirements of the CFEU. While Article 52(1) of the CFEU permits the placing of limitations on the rights protected by the CFEU, it requires that these satisfy the proportionality assessment outlined in Article 52.[140] It is difficult to see that the kind of wide-ranging processing exemptions adopted in the DPA would fulfil these requirements. It is interesting to note that the granting of powers to political parties under national legislation to process the personal data of citizens is already under attack at domestic level on human rights grounds: the Spanish Constitutional Court has declared unconstitutional a provision of the Spanish Data Protection Act which permitted political parties to collect personal data concerning the political preferences of citizens.[141]

In drawing broader conclusions from the discussion of the Irish approach, it is important to remember the specifics of Irish political culture with its very strong emphasis on local and constituency politics. The comparison with this aspect of the DPA UK suggests a somewhat more rigorous approach, although in the UK too the political parties are generally facilitated in what they may do and aspects of that legislation too would seem to be inconsistent with the GDPR. A more in-depth study of Member States is required before definitive conclusions can be reached but in light of the UK approach and of the issues which have already been raised in some other Member States,[142] it might reasonably be presumed that many Member States share Ireland's liberal approach to data processing by political parties.

---

139 *See* text to *supra* n. 105.
140 *See* text to *supra* n. 62.
141 Constitutional Court of Spain, Office of the President, Press Release No 76/2019, https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/PressReleaseNo.76.2019.pdf.
142 *See* text to *supra* n. 83.

While other measures have been taken to address the problems associated with attempts to influence the outcome of elections by manipulating personal data,[143] data protection law remains central to this endeavour. The importance of data protection law in this context has been highlighted by the EDPB in the following terms:

> Compliance with data protection rules, including in the context of electoral activities and political campaigns, is essential to protect democracy. It is also a means to preserve the trust and confidence of citizens and the integrity of elections.[144]

In light of this, it is necessary to work towards striking a better balance between the values at stake. Closer engagement with the issue of political parties by the EDPB would seem to be an obvious place to begin. As noted in the Introduction, this issue was neglected by the A29WP. However, in the wake of Cambridge Analytica, it is no longer defensible to ignore the importance of data protection in the political context. Guidance from the EDPB would provide a more nuanced engagement with the issues at stake and thus allow for a more fine-grained response which bridges the space between the 'one size fits all' approach in the GDPR and the wide-ranging discretion of the flexibilities afforded to Member States.

---

[143] *See* e.g. the announcement by the European Council in Mar. 2019 of the adoption of rules aimed at preventing European political parties from misusing personal data in EP elections through the amendment of Regulation 1141/2014 on the statute and funding of European political parties and European political foundations, https://www.consilium.europa.eu/en/press/press-releases/2019/03/19/ep-elections-eu-adopts-new-rules-to-prevent-misuse-of-personal-data-by-european-political-parties/.

[144] EDPB, *supra* n. 5, at 3.