An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Audit of Political Parties in Ireland

A report by the Data Protection Commission following data protection audits conducted under Article 58(1)(b) of the GDPR

December 2021

Contents

Foreword

In 2021, the Data Protection Commission (DPC) decided to audit certain data processing activities by all of Ireland's political parties for the first time. It did so in circumstances where it supports the view that trust in democracy should not be eroded by poor and opaque personal-data processing practices. Against the backdrop of media stories that began circulating in April, the DPC opened data protection audits in May in respect of all twenty-six registered political parties in Ireland. The audits were conducted under Article 58(1)(b) of the GDPR which empowers each data protection supervisory authority to carry out investigations in the form of data protection audits.

The DPC audits of political parties examined the following issues:

1. The designation of data protection officers
2. The use of Registers of Electors and Marked Electoral Registers
3. Party Membership/Volunteers Databases
4. Databases of Electors/Voters
5. Data Protection Impact Assessments
6. Market Research/Opinion Polling

From the DPC's perspective, carrying out twenty-six audits across all political parties has been a particularly useful exercise and it has given us the opportunity to examine, at first hand, how political parties process personal data, not only in relation to their own membership and supporters, but also more widely in relation to the personal data of the electorate in cases where political parties use data from the Register of Electors and/or the Marked Electoral Register. The audits did not look at broader issues of spend on political advertising (as this is outside of the remit of the DPC) and nor did it examine if any targeted advertising to voters on social media is carried out.

For all political parties that were audited by the DPC this year, this exercise presented them with an opportunity to reflect on, to review, and

to reconsider several aspects of their data processing operations in the context of replying to the DPC's audit questionnaires.

The level of engagement between the political parties and the DPC during the course of the audits and the detailed responses submitted to our questionnaires indicates that there is a high level of data protection awareness in political parties. From the DPC's perspective, we were pleased to note that in the course of many of the data protection audits the top officials of the parties, such as the General Secretary or equivalent, involved themselves in the audit process. This demonstrates the seriousness with which the audits were embraced by the political parties and their desire to get things right from a data protection perspective.

The data protection audits established that, for the most part, processing of personal data by political parties occurs in respect of the processing of the personal data of party members and volunteers rather than data of voters.

The DPC notes that there are no particularly concerning findings to report from its twenty-six audits. As in any other sector, there is always room for improvement in relation to the protection of personal data in the course of data processing. For the most part, the greatest volume of personal data that is processed by political parties relates to data held by the parties in relation to party members, supporters and activists. And the majority of our audit recommendations were made to political parties in relation to that category of data processing – see Chapter 3.

Aside from the aforementioned party membership data, the number of political parties that use data from the Register of Electors and/or the Marked Electoral Register was found to be relatively low: only six of the twenty-six parties currently use (or have used in the past) Register of Electors data while only four parties use (or have used in the past) Marked Electoral Register data.

The extent to which personal data is processed by political parties in the context of conducting market research or opinion polling was examined in depth. The audits found that seven political parties have conducted

market research or opinion polling through the deployment of resources from their own membership, supporters or activists. However, of the seven parties, only one processed personal data in the context of its market research/opinion polling activities. The full details of the audit findings concerning this subject are set out in Chapter Six below. Arising from those findings, the DPC notes that from the perspective of data protection and the processing of personal data, no significant concerns arise in relation to market research or polling activities by political parties.

Chapter 4 of this report reveals the DPC's audit findings with regard to databases of electors/voters. The media stories that first broke in April 2021 with regard to data processing by political parties were dominated by reference to Sinn Féin's Abú database. Chapter 4 below focusses exclusively on the Abú database because Sinn Féin is the only political party that keeps a bespoke database that encompasses electors/voters data from all constituencies across the State. The Abú database combines data from Registers of Electors and Marked Electoral Registers with data obtained from party canvassing activities. As outlined below, the DPC made a number of recommendations to Sinn Féin with regard to the operation of the Abú database. Apart from our recommendations, the DPC is acutely aware that two matters of significant seriousness from a data protection perspective were at play when the media stories first emerged in April:

- Data processing activity in relation to the Abú database commenced in September 2019 but a data protection impact assessment was not conducted by Sinn Féin until April 2021.
- The privacy policy for the Abú database was first published on the Sinn Féin website in April 2021. Prior to its publication, no information was made available to electors/voters in any format to comply with the transparency requirements in the GDPR.

The DPC notes that Sinn Féin took action in relation to both of these matters in April 2021 (prior to the commencement of the DPC audits).

A key question for consideration is whether there is a lawful basis for a political party to create a central database of electors/voters as Sinn Féin

has done by combining data from Registers of Electors, Marked Electoral Registers and from the Party's own canvassing activities. As set out in some detail in Chapter 4 below, several legislative provisions come into play when the question of the legal basis for the keeping and using of a database of electors/voters is considered. Taking all of those provisions into consideration, it is the view of the DPC that there is an arguable case in favour of the existence of the required legal basis therein. The primary legal basis for data processing must be identified in Article 6 of the GDPR and, where special categories of personal data are processed (such as data revealing political opinions) Article 9 must additionally be complied with. The cumulative effect of Sections 39, 48, 59 and 175 of the Data Protection Act, 2018 is that, in relation to political parties, they may process personal data of data subjects in the course of their electoral activities in the State. According to Section 39(4) electoral activities *"includes the dissemination of information, including information as to a person's activities and policies, that might reasonably be of interest to voters."* This gives a wide breadth to the meaning of electoral activities and does not restrict activities purely to the period in the run-up to a notified election and, as pointed out by the sponsoring Minister for Justice in a Seanad debate on the Data Protection Bill, 2018, it includes canvassing (see Chapter 4 below). Accordingly, the DPC is satisfied that the Oireachtas, in framing the Data Protection Act, 2018 has provided political parties with sufficient legal scope to process the personal data of the electorate for its electoral activities in the State, [for the purposes of the requirements set out in Articles 6(1)(e) and 9(2)(d) or (g) GDPR, as applicable] and this includes canvassing and the processing of personal data associated with canvassing activities.

Centralised databases containing vast amounts of personal data do, of course, present their own risks. Data controllers must consider in such cases a whole range of security risks that may arise such as hacking, unauthorised accesses, accidental destruction, and physical or technical incidents leading to data loss. On the other hand, a centralised database that is established in a professional manner with robust access controls can be more secure than subsets of a database being held less securely by individual elected representatives. Political parties play a central role in

a democracy and they must not be inhibited in the performance of that role. Equally, strong protections must be put in place to ensure that the personal data of the electorate is used by political parties in a lawful manner and that they apply robust measures to mitigate against the security risks referred to above, such as unauthorised disclosure of, or access to that personal data.

These are issues that could be considered further by the Oireachtas in the context of forthcoming debates on the Electoral Reform Bill 2020. This will present the Oireachtas with a further opportunity to consider, if it wishes to do so, whether specific limitations should be placed on the creation by political parties of centralised databases of voters/electors using a combination of data from the Register of Electors, Marked Electoral Registers and canvassing activities. Subject to compliance with all GDPR principles, the DPC has not identified any such specific limitations currently in the law.

In conclusion, therefore, this report highlights all the key themes and the main recommendations from across the twenty-six audit reports. With over eighty recommendations made in total, this has been an invaluable undertaking not only for all the political parties but also for the DPC in terms of giving us insight into the data processing operations of Ireland's political parties. We thank the political parties for their cooperation throughout. We welcome the useful contribution of the media in drawing attention to these issues earlier this year.

Introduction

Background

In April 2021 the Data Protection Commission (DPC) became aware of a number of reports in the media, in particular in the *Irish Independent*, regarding the alleged storing by the political party, Sinn Féin, of personal information of millions of voters listed by the Party on an internal party database. Further articles emerged in the media in June 2021 with regard to members of some political parties allegedly posing as market researchers in conducting political opinion polls.

Against this backdrop and conscious of the public interest aroused by these media reports, the DPC decided to carry out data protection audits of all registered political parties in Ireland with regard to the processing by them of personal data of the electorate. The DPC considered it important to conduct these audits to establish the extent to which personal data, if any, of voters is processed by political parties in the manner alleged in the media reports and to establish whether the political parties concerned are carrying out that processing in a manner that is compliant with data protection legislation.

Scope of the Audits

The audits were conducted by Authorised Officers of the DPC beginning with two questionnaires.

Questionnaire 1, which issued on 25 May 2021, aimed to examine the processing of personal data since 25 May, 2018[1] by each political party as a data controller in respect of matters such as:

- Consideration of the designation of a Data Protection Officer
- The carrying out of Data Protection Impact Assessments

[1] The date of coming into legal effect of the GDPR.

- The provision of transparent information to data subjects (such as by means of data protection notices)
- The keeping of databases of party members and databases of voters/electors

Questionnaire 2, which issued on 18 June 2021 aimed to examine the processing of personal data since 25 May, 2018 by each political party as a data controller in respect of:

- Market Research/Opinion Polling

The data protection audits were scoped to examine the matters outlined above only. In that regard, it is important to note that other day-to-day data processing activities carried out by the political parties were not examined in these audits such as, for example, the processing of the personal data of party employees, or the processing of personal data by the deployment of CCTV cameras on party offices, etc.

In addition, it is important to note that the data protection audits were confined to the data processing activities of political parties only (as distinct from politicians or candidates for elective office). Therefore, any data processing activities conducted by individuals such as TDs, Senators or County Councillors (who are data controllers in their own right when processing personal data of data subjects) did not fall into the scope of the audits of political parties.

Political Parties Audited

Data Protection audits were conducted in respect of the following twenty-six registered political parties[2]:

Aontú	Direct Democracy Ireland
Éirigí For A New Republic	Fianna Fáil

[2] Political parties are registered with the Registrar of Political Parties in accordance with Section 25 of the Electoral Act 1992 (as amended).

Fine Gael	Fís Nua
Green Party	Housing Rights & Reform Alliance
Human Dignity Alliance	Identity Ireland
Independents 4 Change	Irish Freedom Party
Kerry Independent Alliance	Party for Animal Welfare
People Before Profit	Renua Ireland
Sinn Féin	Social Democrats
Solidarity	The Communist Party of Ireland
The Labour Party	The National Party
The Right To Change Party	The Workers' Party
United People	Workers and Unemployed Action

Methodology

Phase 1: A questionnaire consisting of seventy-six questions across six sections was issued to all political parties. The breakdown of sections was as follows:

- Section 1: General Questions about the Party and whether it uses the Register of Electors and the Marked Register of Electors.
- Section 2: Data Protection Officer Designation.
- Section 3: Data Protection Impact Assessments.
- Section 4: Party Membership/Volunteers Database.
- Section 5: Database of Electors/Voters.

- Section 6: The Provision of Transparent Information to Data Subjects (in respect of databases of party members/volunteers and electors/voters).

Phase 2: A questionnaire consisting of ten questions concerning market research/opinion polling was issued to all political parties.

Inspection Phase: Having reviewed the replies received from the political parties to the aforementioned questionnaires, the DPC decided to carry out inspections of four political parties. Authorised Officers of the DPC carried out inspections during the months of July and August 2021 at Fianna Fáil, Green Party, Fine Gael (conducted virtually) and Sinn Féin.

Report Phase: The DPC prepared draft audit reports containing recommendations which it commenced issuing to the political parties in October 2021. Submissions were invited from each party. Having carefully considered the submissions received, the DPC prepared a final audit report for each political party and issued them on 10 December 2021. With the exception of three political parties, namely Direct Democracy, Fís Nua and Kerry Independent Alliance, the audit reports contained recommendations from the DPC to the parties for actions to be taken by the parties.

Final Phase: Currently, the onus lies on the political parties to implement the recommendations contained in the audit reports. The DPC will continue its engagement with the political parties over the coming months to ensure that all of the recommendations that contain a specific time-span for implementation are fully implemented on time.

Purpose of This Report

Given the public interest in the matters highlighted by the media between April and June 2021, the DPC considers it appropriate to produce and publish this report to highlight the key findings of its data protection audits and to outline the key recommendations made by the DPC to the

political parties concerned[3]. This report draws from the contents of the audit reports that were issued to the twenty-six registered political parties in the State following the completion of the data protection audits conducted by the DPC in 2021. Set out in this report are the key themes that emerged over the course of those audits and the main recommendations made by the DPC to the political parties concerned.

[3] Section 149(4) of the Data Protection Act, 2018 refers.

Chapter One: Designation of Data Protection Officer

GDPR Requirements

During the course of the data protection audits, with regard to its examination of the designation of data protection officers by the political parties, the DPC focussed its attention on Article 37(1) and Article 37(7) of the GDPR.

Article 37(1) of the GDPR is as follows:

The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

Article 37(7) of the GDPR is as follows:

The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 37(1)(c) above refers to the processing on a large scale of special categories of data pursuant to Article 9 of the GDPR. Personal data revealing political opinions is a special category of personal data. Accordingly, the requirement in Article 37(1) to designate a data protection officer applies to political parties that process, on a large scale, personal data revealing political opinions.

Large Scale Processing

The DPC has considered this matter with a view to determining firstly, what personal data political parties are processing which reveals political opinions and, secondly, the extent to which that data processing is carried out on a large scale. The data protection audits have provided the DPC with the opportunity to examine at first-hand the various categories of personal data processed by political parties. In that regard, the DPC has drawn the following conclusions:

- Register of Electors data does not reveal the political opinions of the individual voters listed on the register. It is a list of persons who were entitled to be registered as electors on a qualifying date. It contains no information about their political opinions.
- Marked Electoral Register data does not reveal the political opinions of the individuals listed as having voted. It provides a list of those who voted on a particular election day. It contains no information about their political opinions or about which candidate(s) they cast their vote for.
- Party Membership/Volunteers Databases which contain personal information in respect of members or volunteers of a political party do reveal the political opinions of the individuals listed thereon in relation to their support for the political party concerned.
- Electors/Voters Databases which contain personal information in respect of the electorate and which indicate the likely voting intentions of the electorate (e.g. on the basis of information recorded during canvassing campaigns) do reveal the opinions of the individuals listed thereon in relation to their level of support for the political party concerned.

In light of the above conclusions, the DPC has considered the extent to which the political parties process, on a large scale, personal data revealing political opinions. Neither the GDPR nor the Data Protection Act 2018 prescribe a figure to quantify the term 'on a large scale' for such data processing. The DPC has, therefore, decided to guide where that figure should be set with the benefit of information obtained from the political

parties. During the audit process, the political parties informed the DPC of the number of records on their party membership/volunteers databases and, in the case of Sinn Féin, on its Electors/Voters database. It is not intended to reveal in this report the details of party membership numbers as given to the DPC by the political parties. We can state, however, that a number of small political parties do not process any data revealing political opinions; a number of other small political parties process such data in very small numbers (in some cases less than one hundred records); while at the other end of the scale a limited number of political parties process thousands of records on their membership databases. Having considered all of the information obtained during the course of twenty-six data protection audits, the DPC has determined that the appropriate threshold that should be met in order for a political party in Ireland to be considered to process personal data revealing political opinions on a large scale is **30,000** records of data subjects (individuals).

Therefore, on the basis of that determination, political parties in Ireland who process personal data revealing political opinions in respect of more than 30,000 individuals are required by Article 37(1) of the GDPR to designate a data protection officer. While there is no requirement on other political parties to do so, it is open to them to designate a data protection officer if they so wish.

Issues That Arose in the Audits Concerning Data Protection Officer Designations

In the context of the data protection audits, the following issues arose with regard to political parties that are required to designate a data protection officer:

- Fianna Fáil first designated a data protection officer in April 2018 prior to the GDPR coming into effect. However, it was three months late in communicating the contact details to the DPC.
- Sinn Féin first designated a data protection officer in April 2021 (almost three years late). It published the contact details and communicated them to the DPC at that time.

Recommendations have been made to both parties to communicate the contact details of newly appointed data protection officers to the DPC without delay in future.

Several other political parties that do not meet the 30,000 threshold referred to above have also designated data protection officers and in some cases there was a delay in communicating the contact details to the DPC. Similar recommendations to the above concerning the need to avoid delays in notifying the DPC have been made to those political parties in the event that they choose to designate data protection officers in the future.

Chapter Two: The Use of Registers of Electors and Marked Electoral Registers

Register of Electors

Section 13 of the Electoral Act, 1992 provides the statutory basis for the preparation and publication in every year of a register by reference to registration areas consisting of administrative counties and county boroughs of persons who were entitled to be registered as electors on the qualifying date.

Section 175 of the Data Protection Act, 2018 amended the Electoral Act, 1992 by the insertion of the following subsection in Section 13:

"(3C) In addition to any other electoral purpose for which the information contained in the register prepared under section 13, including a draft register or the supplement to the register prepared under section 15 or an electors list published under section 16, being information which is excluded from the edited register, may be used, that information may be used – (a) by a specified person (within the meaning of section 39 of the Data Protection Act 2018), for the purpose of communicating with a data subject in accordance with section 39 of that Act, or (b) by an elected representative (within the meaning of section 40 of the Data Protection Act 2018) for the purposes of section 40 of that Act."

A "specified person" means a political party, a member of either House of the Oireachtas, the European Parliament or a local authority, or a candidate for election to the office of President of Ireland, or for membership of either House of the Oireachtas, the European Parliament or a local authority.

An "elected representative" means a member of either House of the Oireachtas, a member of the European Parliament, or a member of a local authority.

In summary, there is a statutory basis for a political party, being a "specified person" to use information contained on the Register of Electors for the purpose of communicating with data subjects in the

course of electoral activities (which includes the dissemination of information) (per section 39 of the Data Protection Act 2018).

Marked Electoral Register

Section 131 of the Electoral Act, 1992 provides the statutory basis for all documents sent by a returning officer to the Clerk of the Dáil to be open for public inspection. It makes provision for the Clerk of the Dáil to supply copies of or extracts from the said documents to any person demanding the same on payment of such fees not exceeding the reasonable cost of copying.

The Marked Electoral Register shows whether an individual voted or not at a particular election. At a polling station, the presiding officer 'marks' the register of electors in respect of each individual who casts their vote. The election Returning Officer subsequently supplies to the Clerk of the Dáil a copy of the 'marked' registers used at each polling station.

To give practical effect to the requirement in Section 131 of the Electoral Act, 1992 for the Clerk of the Dáil to supply copies of or extracts to any person demanding them, the Public Bills Office of the Houses of the Oireachtas Service requires persons who seek a copy of the Marked Electoral Register to sign a statutory declaration "Regarding Intended Usage of Marked Electoral Register." This requires the requester to declare, among other things, that they are aware of their obligations pursuant to Section 13A(3) of the Electoral Act 1992 and that they are aware of their obligations pursuant to the GDPR and the Data Protection Act 2018. Sanction regarding the fees to be charged for providing the Marked Electoral Register to requesters is granted by the Minister for Public Expenditure and Reform. The fees sanctioned in respect of the Marked Electoral Register for the 2020 General Election were as follows: €57.00 for a three seater constituency, €75.00 for a four seater constituency and €93.00 for a five seater constituency. Multiple constituencies were chargeable at multiples of the same rates and all forty constituencies were charged at €3,090.00.

In summary, as there is a statutory basis for any person to obtain a copy of the Marked Electoral Registers for general elections on payment of a

fee and on signing a statutory declaration, it is therefore open to any person, including a person acting as a representative of a political party, to obtain copies of the Marked Electoral Register by this means.

Similar provisions are laid down in respect of providing a statutory basis for individuals to obtain from local authorities a copy of the Marked Electoral Registers for Local Elections (Regulation 94 of S.I. No. 297 of 1995 – Local Elections Regulations, 1995 refers).

Neither of the aforementioned legislative provisions set down limitations as to the uses that those who receive copies may put the Marked Electoral Registers. [The Clerk of the Dáil (in the case of General Elections) or the Returning Officer (in the case of Local Elections) is required to retain the documents for six months from the date of the poll and to destroy them thereafter].

Political Party Users of Registers of Electors

The DPC data protection audits found that the following political parties either keep a copy of Registers of Electors at present or have done so in the past:

Fianna Fáil (none retained at present); Fine Gael; Sinn Féin; Social Democrats; The Workers' Party; Workers and Unemployed Action.

Recommendation. In the case of one of the above political parties, Workers and Unemployed Action, the DPC made a recommendation concerning Register of Electors data that the Party set a retention period and implement procedures for the keeping of personal data for no longer than is necessary in order to meet the requirements of the principle of storage limitation in Article 5(1)(e) of the GDPR.

The other political parties that use Register of Electors data had retention policies and procedures in place.

In the case of Social Democrats and Workers and Unemployed Action the audit made the following recommendation:

Recommendation: The DPC recommends that Social Democrats/Workers and Unemployed Action update its privacy policy to include information concerning the processing of personal data that it undertakes in relation to the information contained on the Register of Electors. This work should be completed by the end of 2021 and the Data Protection Commission should be notified accordingly.

Political Party Users of Marked Electoral Registers

The DPC data protection audits found that the following political parties either keep a copy of Marked Electoral Registers at present or have done so in the past:

Fianna Fáil; Fine Gael; Green Party; Sinn Féin.

In the case of Fianna Fáil, the audit made the following recommendation in relation to its published privacy policy:

Recommendation: In the event that Fianna Fáil acquires copies of any future Marked Electoral Register, the DPC recommends that Fianna Fáil update its privacy policy at that point to include information concerning the processing of personal data that it will undertake in relation to the information contained on the Marked Electoral Register.

In the case of Fine Gael, the audit made the following recommendation in relation to its published privacy policy:

Recommendation: The DPC recommends that Fine Gael's Privacy Policy should include information concerning the processing of personal data that it undertakes in relation to the information contained on the Register of Electors and on the Marked Electoral Register. This work should be completed by the end of Q1 of 2022 and the DPC should be notified accordingly.

In the case of the Green Party, the audit made the following recommendation in relation to its published privacy policy:

Recommendation: The DPC recommends that the Green Party update its privacy policy to include information concerning the processing of personal data that it undertakes in relation to the information contained on the Marked Electoral Register. This work should be completed by the end 2021 and the DPC should be notified accordingly.

Further Discussion

See Chapter 4 "Database of Electors/Voters" below for further discussion on the matter of the use of electoral register data.

Chapter Three: Party Membership/Volunteers Databases

Overview

The data protection audits established that, for the most part, processing of personal data by political parties occurs in respect of the processing of the personal data of party members and volunteers rather than data of voters.

Of the twenty-six political parties audited, twenty-three of them keep and process computerised records in relation to their membership and volunteers. Depending on the size of the parties, the records may be kept on a specially designed bespoke database or a relational database, in the case of the larger parties in particular, or they may be kept in a spreadsheet format (such as Excel) in the case of some of the smaller parties.

The situation in relation to the processing of the remaining three political parties is as follows:

- *Direct Democracy Ireland* and *Kerry Independent Alliance*: Neither party keeps computerised or manual records of membership at present.
- *Fís Nua*: Keeps completed membership forms only in manual format.
- The DPC made no recommendations to these three political parties concerning the processing of personal data of party members or volunteers or in relation to any of the other issues examined by the audits.

As stated in Chapter One above, the processing of party membership data reveals personal data concerning the political opinions of the members concerned and, accordingly, this is deemed to be processing of special category personal data pursuant to Article 9 of the GDPR. The level of such data processing varies in line with the size of the political parties concerned with some small parties processing membership data in very

small numbers (in some cases less than one hundred records) while a few political parties process thousands of records on their membership databases.

Issues of Concern With Regard to Membership Databases

The primary issues of concern that emerged in relation to the membership databases were as follows:

- Information to members concerning the processing of their personal data
- Logging of 'edit' and 'read only' accesses to the databases and auditing of the audit trails
- Setting of retention periods for membership data
- Minimisation of the fields of data collected in relation to members
- Documenting of backup policies governing databases and servers

Information To Members Concerning The Processing Of Their Personal Data

The provision of transparent information to data subjects is one of the key cornerstones of the GDPR. Article 12 refers to the requirement for data controllers to provide information to data subjects in a concise, transparent, intelligible and easily accessible form using clear and plain language. Article 13 sets out the range of information that a data controller is required to provide to data subjects where personal data related to those data subjects are collected from the data subjects themselves – such as in the case of members of a political party who provide the party concerned with their own data for membership purposes. Article 13(1) of the GDPR requires, in such circumstances, that data subjects be provided with such key information as the identity and contact details of the controller; the contact details of the data protection officer, where applicable; the purposes of the processing for which the

personal data are intended as well as the legal basis for the processing; the recipients of the personal data. To ensure fair and transparent processing Article 13(2) requires that the data controller provide the data subject with the following information: the period for which the personal data will be stored; the existence of the rights of access, rectification or erasure, restriction of processing, to object to processing; and the right to lodge a complaint with a supervisory authority.

The data protection audits of political parties found several instances where insufficient information had been given to the Party membership that would meet the requirements of Articles 13(1) and 13(2). Recommendations were made to the following political parties with regard to transparent information concerning membership data: Éirigí For A New Republic, Fianna Fáil, Fine Gael, Housing Rights & Reform Alliance, Human Dignity Alliance, Identity Ireland, Independents 4 Change, Irish Freedom Party, Party For Animal Welfare, Renua Ireland, Social Democrats, Solidarity, The Communist Party, The Labour Party, The National Party, The Right To Change Party, The Workers' Party, United People and Workers and Unemployed Action.

The recommendations to these political parties were along the following lines (or a variation thereof where a data protection notice was already in place):

Recommendation. The DPC recommends that the Party devise a comprehensive data protection notice as a matter of priority for circulation to all individuals whose personal data is kept on the Party membership database. The notice should provide all the information stipulated in Articles 13(1) and 13(2) of the GDPR in a concise, transparent, intelligible and easily accessible form, using clear and plain language – as is required by Article 12 of the GDPR. This should be completed and distributed to Party members by the end of 2021 and the DPC should be notified accordingly.

Logging Of 'Edit' and 'Read Only' Accesses to Party Membership Databases and Auditing of the Audit Trails

In terms of computerised databases, it is essential that there is inbuilt technical capability to log all access activity – this includes not only 'edit' accesses but also 'read only' accesses. The existence of technical audit trails or access logs on computerised systems are of little value, however, if they are not audited routinely. The practice of "auditing the audit trails" is a key governance measure that assists a data controller to comply with the requirements of Article 24(1) of the GDPR to implement appropriate technical and organisational measures for ensuring that the processing of personal data for which it is responsible is performed in compliance with the GDPR and to demonstrate such compliance. In the absence of proactive and regular auditing of audit trails, unauthorised accesses could occur without any prospect of being detected. This lack of oversight may present a security vulnerability.

The principle of integrity and confidentiality that is set out in Article 5(1)(f) of the GDPR requires that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Article 32(1) obliges the data controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The matter of a lack of 'auditing of the audit trails' on party membership databases emerged as a common issue of concern during these data protection audits. Recommendations were issued to the following political parties with regard to this particular issue:

Aontú, Fianna Fáil, Green Party, Independents 4 Change, Irish Freedom Party, Party for Animal Welfare, People Before Profit, The Labour Party, The Workers' Party and United People.

The DPC's recommendations to these political parties were along the following lines, or similar:

Recommendation. The DPC recommends that the Party implements a robust procedure to ensure that the logs of all accesses, 'read only' and 'edit', are regularly audited to ensure that unauthorised accesses are detected without delay and that reports of auditing activity are submitted to the senior management of the organisation on a regular basis. A progress report on the implementation of this recommendation should be sent by the Party to the DPC by the end of Q1 of 2022.

Setting of Retention Periods for Membership Databases

The 'storage limitation' principle in Article 5(1)(e) of the GDPR requires that personal data is not kept for longer than is necessary. To comply with this principle, data controllers are advised to adopt and implement a data retention policy in respect of all personal data records under its control. It is a matter for the data controller to determine the appropriate period for which personal records should be retained taking account of its business needs as well as statutory obligations that may apply to certain personal data records. However, keeping personal data records indefinitely is not acceptable from the perspective of the 'storage limitation' principle.

Issues of concern that arose during the course of the data protection audits included the retention of the data of lapsed members or others who leave the Party concerned as well as the absence, in some cases, of an overall data retention policy. Recommendations were made to the following political parties with regard to data retention in relation to membership data: Éirigí For A New Republic, Human Dignity Alliance, Irish Freedom Party, Party For Animal Welfare, The Labour Party, The National Party, The Right To Change Party and Workers and Unemployed Action.

The recommendations to these political parties were along the following lines, or similar:

Recommendation. The DPC recommends that the Party devise a policy and implement procedures to ensure that the principle of storage limitation in Article 5(1)(e) of the GDPR is complied with in relation to membership data generally and, in particular, concerning the personal data of lapsed members or other members who leave the Party. This work should be completed by the end of Q1 of 2022 and the DPC should be notified accordingly.

The following two recommendations were made to Fianna Fáil:

Recommendation: The DPC recommends that Fianna Fáil establish a process to communicate with its non-voting membership periodically to establish whether those members wish to continue to have their personal data retained on the membership database and then update the database accordingly. It should send a progress report to the Data Protection Commission on the implementation of this recommendation by the end of Q1 of 2022.

Recommendation: The DPC recommends that Fianna Fáil complete its work on devising, adopting and implementing a data retention policy that takes full account of the requirements of the 'storage limitation' principle of Article 5(1)(e) of the GDPR. It should aim to complete this task by the end of Q1 of 2022 at the latest and it should notify the DPC on completion.

Minimisation of the fields of data collected in relation to members

The principle of 'data minimisation' that is set out in Article 5(1)(c) of the GDPR requires that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. With regard to a membership database for a political party this means, in practical terms, that the party collect only the minimum fields of data. For example, data fields such as 'job title', 'current employer', or

'your interests' are unnecessary for the purposes of becoming a member of a political party.

Recommendations were made to two political parties during the audits with regard to the application of the principle of 'data minimisation.'

Recommendations. In the case of Aontú, which is currently developing a new membership database system, the DPC recommended that the fields of personal data that will be collected in relation to Party members be kept to the minimum necessary for the business needs of the organisation.

In the case of the Green Party, the DPC recommended that it critically review the current data fields on its membership database to satisfy itself that each field is necessary for the business needs of the Party. Where it identifies any data fields that are not necessary, it should delete the data collected from the existing membership using those data fields. This work should be completed by the end of Q1 of 2022 and the DPC should be notified accordingly.

Documenting of backup policies governing databases and servers

An issue examined by the audits in relation to the security of the membership database concerned the backup policies in place and how the reliability of the backup dataset is tested. Of the political parties that have membership databases, two parties came to attention on the grounds that neither one had a documented process governing their backup service and measures were not in place to regularly test and assess the effectiveness of their backups. The parties concerned in that regard were People Before Profit and Sinn Féin.

The recommendations made to these political parties were along the following lines:

Recommendation. The DPC recommends that the Party documents appropriate backup policies which govern both the database and the servers upon which the personal data resides. This work should be completed by the end of Q1 of 2022 and the DPC should be notified accordingly. It also recommends that the Party periodically test and assess the effectiveness of the backup measures in place.

The above recommendation made to Sinn Féin applies also to the Abú database discussed below in Chapter 4.

Chapter Four: Databases of Electors/Voters

Introduction

Of the twenty-six registered political parties audited by the DPC only one of them, Sinn Féin, keeps a database that encompasses electors/voters data from all constituencies across the State. As mentioned in Chapter One above, a handful of political parties use Register of Electors data or Marked Electoral Register data. However, with the exception of Sinn Féin, none of those political parties has created a bespoke database combining data from Registers of Electors and Marked Electoral Registers with data obtained from party canvassing activities.

Overview of Sinn Féin's Abú Database

Sinn Féin informed the audit that it maintains a database of electors/voters, called Abú Canvass Aid that was established in September 2019. Abú is a specially designed, bespoke relational database that was designed to identify supporters in order to get out the vote on election day. The system contains data from the register of electors and the marked electoral register and is supplemented by canvass information.

During the course of the audit, the Authorised Officers established that Abú does not contain records of individuals in Northern Ireland or elsewhere and it is not used by officers or offices of Sinn Féin in Northern Ireland.

Sinn Féin informed the audit that the Abú database is kept for electoral activities in the State and that it is used primarily in the run-up to elections and on polling day. The purpose of its use is to record a canvasser's opinion of an individual's likelihood to vote for Sinn Féin, with a view to ultimately increasing turnout of voters and convincing voters to support Sinn Féin. It is a canvass aid used to create the material necessary to conduct and record a door-to-door canvass and other electoral activity based upon the register, with the ultimate objective of mobilising voters on election day. It allows Sinn Féin to best direct scarce canvassing resources in areas of constituencies.

The sources of the data on Abú are, according to Sinn Féin, as follows:

- Register of Electors data is obtained from the relevant city or county council.
- Marked Register data is obtained from the Registrar of Dáil Éireann or the local authority (depending on the election)
- Canvass data is received from canvassing activities.

The data fields on the Abú database consist of all the fields on the Register of Electors and Marked Register datasets, Canvass data and Get Out The Vote (GOTV) Canvass data (further described below).

The Register of Electors dataset contains voter number (assigned at polling district level); first name of voter; surname; type of voter (i.e. whether a voter is eligible to vote in Dáil or European or Local elections); house name; house number; townland; qualifier (this is the secondary address field, normally the name of the town, area or district); postcode (used exclusively for Dublin); Eircode; polling district; electoral division; electoral area; polling station; and Dáil constituency.

Using the Marked Register data set, each voter is marked on the Abú database as either (i) having voted; or (ii) not voted; or (iii) N/A; for each of the following elections: 2016 General Election, 2019 Local Election and 2020 General Election. Sinn Féin does this by scanning the marked registers and running them through an algorithm that tries to determine if the name has been crossed out or not on the Marked Register. This is then assigned either a value of having voted or not voted for the given register. In subsequent years, where voters are on the register now who were not on the register at the time of the relevant election, they are marked N/A.

Canvass Data, which is derived primarily from door-to-door canvassing, is recorded against the voter record as follows:

- Hard Support: This is where a canvasser has a high degree of confidence that the voter canvassed is likely to vote for Sinn Féin.
- Soft Support: This is where a canvasser is confident that the voter canvassed is likely to vote for Sinn Féin, but not as certain as a Hard Supporter.

- Transfer: This is where a canvasser believes that a voter will give a high preference to Sinn Féin, but not a first preference.
- Strong Opposition: This is where a canvasser believes that a voter will not vote for Sinn Féin and is unlikely to do so in the future.
- Unknown: This is where a canvasser has not formed an opinion on a voter, but has spoken to at least one voter in that household.
- Not In: This is to record that a household was canvassed but there was no opportunity to engage a voter.

GOTV Canvass Data is collected on polling day itself. These are canvasses of those recorded as likely Sinn Féin voters only and is designed to get them out to vote. The fields are used to track progress throughout polling day and to deploy resources where needed to maximise voter turnout. The information is recorded against the voter record as follows:

- Already Voted: This indicates that a voter has told the canvasser that they have already voted.
- Committed to vote later: This indicates that a voter has told the canvasser that they will vote later.
- Will not vote: This indicates that a voter has told the canvasser that they do not intend to vote.
- Not In: This is to record that the household was canvassed but there was no opportunity to engage the voter.
- Confirmed Opposition: This is to correct the recording of a voter who was recorded as a supporter but is actually not one.

The Abú database currently holds the Register of Electors data for the years 2016, 2019, 2020 and 2021. It also currently holds the Marked Electoral Register data for the General Elections held in 2016 and in 2020 and for the Local Elections held in 2019. Canvass Data and GOTV Canvass Data is also currently held on the Abú database in respect of the by-elections held in 2019, the 2020 General Election and the 2021 Dublin Bay South by-election.

Having inspected the Abú database, the Authorised Officers noted that the total number of eligible voters that are marked as to their political opinions is currently approximately 5.85% of the overall number of voters on the database. In other words, data in respect of approximately 94.15% of the eligible voters shown on the Abú database is combined Register of Electors and Marked Electoral Register data without any indicators as to the political opinions of those electors/voters.

Sinn Féin informed the audit that the only element of personal data that reveals political opinions are the canvassers' assessments of how likely an individual voter is to vote for Sinn Féin contained within canvass returns.

The Authorised Officers established that the Abú database is not used to keep a record of representations made by constituents or members of the public on political or personal matters and they were told that it is not a database of comments made or of actions to be done.

Access to the database is strictly limited to trained users. Access is determined centrally by the database administrator. Access is controlled by geographical determinations and can be established on the basis of constituency through to townland (street) level on a granular basis.

With regard to data retention, following the next general election, the personal data relating to the 2016 register and marked register will be disposed of. As no 2014 local election data is stored, the next local elections in 2024 will be added to the data field and the 2019 data will be disposed of after the 2029 local elections. The maximum retention period is ten years, though this may be shorter in the case of early general elections.

Physical security for the Abú database is provided by the hosting provider, Linode. The data is stored on a server in Frankfurt, Germany.

The Abú Database - Lawfulness of Processing

The audit asked Sinn Féin to identify the legal basis under Article 6(1) of the GDPR that it relies on for keeping a database of electors/voters. In

response Sinn Féin referred to "Public Interest – Article 6(1)(e) of the GDPR."

From what follows below, it can be seen that several legislative provisions come into play when the question of the legal basis for the keeping and using of a database of electors/voters is considered.

First, there is Article 6(1)(e) of the GDPR, referred to by Sinn Féin, which reads as follows:

"Processing shall be lawful only if and to the extent that at least one of the following applies:….processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

Second, there is Article 6(4) of the GDPR which reads as follows:

"Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

Third, there is Recital 45 of the GDPR which reads as follows:

"Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official

authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing……"

Fourth, there is Section 39 of the Data Protection Act, 2018 which is headed *"Communication with data subjects by political parties, candidates for and holders of certain elective political offices."* Section 39(1) reads as follows:

"A specified person may, in the course of that person's electoral activities in the State, use the personal data of a data subject for communicating in writing (including by way of newsletter or circular) with the data subject."

Section 39(2) reads as follows: *"Communicating in accordance with subsection (1) shall, for the purposes of Article 6(1)(e), be considered to be the performance of a task carried out in the public interest."*

According to Section 39(3) 'specified person' means a political party, a member of either House of the Oireachtas, the European Parliament or a local authority, or a candidate for election to the office of President of Ireland, or for membership of either House of the Oireachtas, the European Parliament or a local authority. "Electoral activities" according to Section 39(4) includes the dissemination of information, including information as to a person's activities and policies that might reasonably be of interest to voters.

Fifth, there is Article 9 of the GDPR which classifies personal data revealing political opinions as a special category of personal data.

Sixth, there is Recital 56 of the GDPR which is as follows:

"Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted

for the reasons of public interest, provided that appropriate safeguards are established."

Seventh, there is Section 48 of the Data Protection Act, 2018 which is headed *"Processing of personal data revealing political opinions for electoral activities and functions of Referendum Commission."* It reads as follows:

"Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of personal data revealing political opinions shall be lawful where the processing is carried out – (a) in the course of electoral activities in the State for the purpose of compiling data on peoples' political opinions by (i) a political party, or (ii) a candidate for election to, or a holder of, elective political office in the State."

During the Report Stage Seanad debate on the then Data Protection Bill 2018 on 22 March 2018 the sponsoring Minister for Justice, Charlie Flanagan T.D. elaborated on the meaning of "electoral activity" as set out in Section 43 of the Bill (now Section 48 of the 2018 Act):

"Section 43 is important because it allows for something of a special status for the conducting of political activity, which as both Senators have said is important in the context of our democracy. We are traversing the terrain between Cambridge Analytica on the one hand and Cambridge Road, Rathmines, on the other. We need to address the balance here.

Senator McDowell is of the view that the section as currently constructed is too narrow and that in many ways it could well curtail or restrict what he, and I am sure all of us here present, would regard as lawful political activity. I remind Members that the revised text of section 43 refers to "electoral activity" rather than "election activity". Undoubtedly electoral activity is considerably broader in context than what might be described as a narrower election activity, lest Members be of the view that this provision would only apply within a certain timeframe, namely, during an election campaign, once an election has been announced or after these Houses have been dissolved. That is not the case. Electoral activity is considerably broader and, to my mind, will cover the issues as raised by Senator McDowell in terms of flexibility, or in terms of the processing of data for political activity. It will not just apply during the timeframe of an election campaign but perhaps at any stage in the context

of our political deliberations. I feel that the element of flexibility in the revised text will meet the concern of Senator McDowell. It is broader, and it does denote a greater level of flexibility."

At another point in the same Seanad debate, the Minister for Justice stated:

I will take this opportunity to point out that section 43 provides a legal basis for elected representatives, Members of this House and members of other institutions, whether members of political parties or not, to engage in data processing for electoral activities, including canvassing.

In a Dáil debate on 16 May, 2018 the Minister for Justice stated:

I stand over the important changes that we have made, in particular to section 38, and I am anxious to be of assistance to Deputy Thomas Byrne. In that regard, electoral activity must be clearly understood in a broad sense to be more than just activity within the confines of the three weeks, 28 days or whatever. In support of this point, I will point out that we do not have fixed-term parliaments. As such, all of the activities of elected representatives and candidates are undertaken with an eye on the next election. Suffice it for me to draw on our earlier debate when Deputy O'Callaghan gave way to Deputy Byrne on the matter of the digital age of consent. Regardless of when an election takes place, electoral activity continues. I say this to be of assistance to Deputy Byrne and to assure him that I am keen to go as far as I can on the objective of his amendments within the strictures of the GDPR and without introducing new elements of uncertainty in the matter of political activities. I take the Deputy's point about political activities and I like the phrase "political activities", but if we are to introduce new definitions or phrases without an appropriate level of definition, we will get into uncertainty and difficulty. "Electoral activities" is known in law to be the work that we do on a continual basis. I am sure that Deputies Daly and Wallace also do that work, although they might not like it to be termed as such.

For its part, Sinn Féin informed the audit that it has implemented several "suitable and specific measures" envisaged by Section 48 of the Data Protection Act, 2018 and, in that regard, it referred specifically to having implemented the following measures:

- limitations on access to the personal data undergoing processing
- strict time limits for the erasure of personal data
- specific targeted training for those involved in processing operations
- logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased
- encryption of the personal data

Eighth, there is Section 59 of the Data Protection Act, 2018 which is as follows:

"The right of a data subject to object at any time to the processing of personal data concerning him or her under Article 21 shall not apply to processing carried out – (a) in the course of electoral activities in the State by – (i) a political party, or (ii) a candidate for election to, or a holder of, elective political office in the State, and (b) by the Referendum Commission in the performance of its functions."

Ninth, there is Section 175 of the Data Protection Act, 2018 which provides for the lawfulness of obtaining personal data from the register of electors. It amends Section 13A of the Electoral Act 1992 by the insertion of the following subsection after subsection (3B):

"(3C) In addition to any other electoral purpose for which the information contained in the register prepared under section 13, including a draft register or the supplement to the register prepared under section 15 or an electors list published under section 16, being information which is excluded from the edited register, may be used, that information may be used –

(a) by a specified person (within the meaning of section 39 of the Data Protection Act 2018), for the purpose of communicating with a data subject in accordance with section 39 of that Act, or

(b) *by an elected representative (within the meaning of section 40 of the Data Protection Act 2018) for the purposes of section 40 of that Act.*"

Taking all of the above into account, the Authorised Officers did not consider it necessary to make any recommendations to Sinn Féin in relation to the legal basis of its Abú database.

Information To Electors/Voters Concerning The Processing Of Their Personal Data

As stated in Chapter 3 above, the provision of transparent information to data subjects is one of the key cornerstones of the GDPR. Article 12 refers to the requirement for data controllers to provide information to data subjects in a concise, transparent, intelligible and easily accessible form using clear and plain language. Article 13 sets out the range of information that a data controller is required to provide to data subjects where personal data related to those data subjects are collected from the data subjects themselves – such as in the case of members of the public who are canvassed at their doorstep by political party activists and who provide the political party concerned with information about their voting intentions. Article 14 of the GDPR sets out the range of information that a data controller is required to provide where personal data have not been obtained from the data subject – such as in the case of electors/voters whose data from the Register of Electors or Marked Electoral Register is processed by a political party on a bespoke database. Article 14(1) of the GDPR requires, in such circumstances, that data subjects be provided with such key information as the identity and contact details of the controller; the contact details of the data protection officer, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the categories of personal data concerned; the recipients of the personal data; the period for which the personal data will be stored; the existence of the rights of access, rectification or erasure, restriction of processing, to object to processing; and the right to lodge a complaint with a supervisory authority.

Sinn Féin informed the audit that its bespoke privacy policy for Abú can be found on its website www.sinnfein.ie/privacy-abu. It stated that additionally, physical election communication contains clear signposting to Sinn Féin's privacy policies and canvassers and candidates are made aware of this in advance of every campaign. It explained that all electoral

canvass material includes a reference to this policy and provides citizens with clear signposts on how to access it. Sinn Féin provided the audit with sample literature used in the Dublin Bay South By-Election in 2021.

Following an examination of the privacy policy and the sample election literature, the Authorised Officers concluded that the privacy policy contained the key transparency information requirements of the GDPR. However, they noted that the sample canvassing literature made no reference to the Abú database or to the fact that canvassing information with regard to prospective voters to whom the leaflet is handed out may be processed on the Abú database.

It was established by the audit that the privacy policy relating to the Abú database was published on 22 April 2021. In simple terms, therefore, prior to the publication of the privacy policy for the Abú database on 22 April, 2021 no information was made available to electors/voters in any format to comply with the transparency requirements of the GDPR.

The following recommendation[4] was made to Sinn Féin:

Recommendation. The DPC recommends that from now on Sinn Féin proactively draw voters/electors attention to the existence of the Abú database and the associated privacy policy by way of notice on all canvassing and electioneering literature. This should continue as standard practice for as long as the Abú database continues to exist.

Data Collection Relating to Social Media Channels

During the audit, the Authorised Officers sought to examine the processing undertaken by Sinn Féin through its social media channels, as well as to determine whether Sinn Féin was processing personal data obtained through these channels in other contexts, including whether it

[4] Sinn Féin in response to the draft audit report provided an example of a revised canvassing notice that will be used going forward which includes the URLs for its privacy page and Abú privacy policy.

was being used to enrich the Abú or party membership databases. These matters were probed in detail during the inspection phase of the audit.

No evidence was found during the audit that suggests that Sinn Féin has been using its social media presence, or its activities on social media platforms, to obtain or otherwise process personal data to enrich either the Abú or the party membership databases.

Other Recommendations

The DPC also made the following recommendations to Sinn Féin with regard to the Abú database:

Recommendation: The DPC recommends that Sinn Féin ensures that it implements robust and appropriate measures by the end of Q1 of 2022 (and notifies the DPC when implemented) to detect and alert it to anomalous and unauthorised activity on its servers and databases, as well as to regularly monitor and audit the server and database logs in addition to its application-level activity monitoring that currently takes place, and that reports of auditing activity be submitted to the senior management of the organisation on a regular basis.

Recommendation: The DPC recommends that Sinn Féin ensures that any envisaged activity relating to software development, script development and related testing is governed by an associated policy which is guided by relevant standards, industry best practice and guidance, so as to ensure that such actions are carried out in a routine, repeatable and expected manner. The DPC should be notified when the policy is introduced.

Recommendation: With regard to database fields and tables that are present in the database but are no longer in use, not intended to be used, or where potential usage has not yet been decided, the DPC recommends that Sinn Féin remove those tables and fields from the Abú database in line with the principle of data minimisation in Article 5(1)(c) of the GDPR. This work should be completed by the end of Q1 of 2022 and the DPC should be notified accordingly.

Chapter Five: Data Protection Impact Assessments

GDPR Requirements

Article 35(1) of the GDPR is as follows:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

In November 2018 the DPC published a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment (DPIA).

The audits of political parties sought to establish:

- Whether each political party carried out risk assessments that gave rise to an identified need to conduct a DPIA.
- Where DPIAs have not been conducted since 25 May 2018, whether the parties concerned considered the DPC's published list of types of data processing operations which require a DPIA.

Audit Findings

Sinn Féin confirmed that it carried out a data protection impact assessment (DPIA) in relation to the Abú database in April 2021. It stated that the data protection officer was consulted at length when the DPIA was being carried out.

Sinn Féin confirmed that the data processing activity in relation to the Abú database commenced in September 2019.

The Authorised Officers noted that data processing activity in respect of the Abú database commenced in September 2019 (i.e. after the GDPR had

come into effect) and that the DPIA was conducted in April 2021 (i.e. after the processing had commenced).

The following recommendation was made to Sinn Féin:

Recommendation. The DPC recommends that in future Sinn Féin undertake all data protection impact assessments prior to the commencement of the processing operations concerned in order to meet the requirements of Article 35(1) of the GDPR.

The audit established that Fine Gael and the Green Party have also carried out DPIAs. Fine Gael provided a list of eleven data processing activities for which it had undertaken DPIAs while the Green Party confirmed that one DPIA had been undertaken on a proposed CRM specification. In respect of those parties, the Authorised Officers did not consider it necessary to make any recommendations to either one.

A number of other political parties informed the audit that they had carried out risk assessments (e.g. in some cases as part of their GDPR readiness work in 2018) and had concluded that none of their processing activities gave rise to the need to conduct a DPIA.

On the other hand, however, due to the absence of evidence of any form of risk assessment having been carried out, the Authorised Officers found it necessary in the case of some other political parties to draw attention to the fact that the data controller has obligations under Article 24 of the GDPR to implement appropriate measures to ensure and to be able to demonstrate that data processing is performed in accordance with the GDPR. Recital 74 of the GDPR states that those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. Furthermore, Article 32 of the GDPR concerning security of data processing and Recital 83 also highlight the need to evaluate the risks inherent in data processing in order to maintain security. In addition, the principle of 'accountability' in Article 5(2) of the GDPR requires that the data controller

be responsible for and be able to demonstrate compliance with the data protection principles in Article 5(1). Given all of these requirements, the carrying out of risk assessments are, at a very minimum, necessary in order for a data controller such as a political party to meet its data security obligations, its Article 24 responsibilities and to meet the requirements of the principle of accountability.

A recommendation along the following lines was issued to Housing Rights & Reform Alliance, Human Dignity Alliance, Identity Ireland, Independents 4 Change, Party for Animal Welfare, Renua Ireland, The National Party, and The Right To Change Party:

Recommendation. The DPC recommends that the Party carry out risk assessments in accordance with its responsibilities under Articles 24 and 32 of the GDPR and that it fully document the risk assessments and the measures taken to address the risks in order to meet its accountability obligations under Article 5(2) of the GDPR. All of this work should be completed by the end of Q1 of 2022 and the DPC should be notified accordingly.

Chapter Six: Market Research/Opinion Polling

As stated at the beginning of this report, a number of articles emerged in the media in June 2021 with regard to members of some political parties allegedly posing as market researchers in conducting political opinion polls. The DPC was concerned to establish the extent, if any, to which the personal data of members of the public was processed by any political parties that may have engaged in the alleged activity concerning opinion polling. Normally, opinion polling is conducted on an anonymised basis and cannot be attributable to individual electors. If however, for example, personal data of the electorate was collected by a political party under false pretences by means of opinion polling activity and could be attributed to particular voters in records kept by the party, this would undoubtedly raise data protection concerns in relation to the lawful basis for such activity and it would undermine the transparency requirements of the data protection legislation. In that regard, therefore, in Phase 2 of the audits of political parties a questionnaire consisting of ten questions concerning market research/opinion polling was issued to all political parties.

The audit sought to establish in the first instance whether political parties use party members, volunteers, activists or supporters to conduct market research or opinion polling or if they had done so in the past. The following seven political parties indicated that they have done so in the past and below we have outlined in respect of each one a description of their activities in that regard: Aontú, Fianna Fáil, Fine Gael, Green Party, Renua Ireland, Sinn Féin and Solidarity. The audit then examined the extent to which any of the political parties concerned processed personal data in the course of their market research or opinion polling activities. The DPC considered it necessary to seek this information in order to establish whether there was an appropriate lawful basis for the collection and processing of personal data, if any, and to establish the extent to which the transparency requirements were met. The audit findings are set out hereunder.

Aontú

Aontú confirmed that it had conducted surveys in the past, from 15 April, 2021 to the 20 April, 2021. Four survey pages were set up on the Aontú website and four Facebook posts were created on an Aontú branded Facebook page. These posts were boosted, that is turned into paid advertisements with a budget of about €40, and people who clicked on them were directed to surveys on the main Aontú website. The advertisements and surveys were aimed at the Co. Meath area, predominantly about living in Co. Meath. Personal data was collected i.e. names, email addresses, ages and gender. Aontú confirmed that personally identifying information was removed and the survey results were pseudonymised and aggregated into graphs. Afterwards all individual names, ages, gender information and email addresses were deleted. Responses to questions were retained on a secure MySQL database with no web access routes beyond the hosting control panel. The survey pages were deleted after the surveys were completed. Very few responses to the surveys were received overall.

As personal data was processed by Aontú during the course of these surveys, the Authorised Officers made the following recommendation:

Recommendation. The DPC recommends that in the event that Aontú carries out further online surveys in the future that it avoid the requirement for participants to submit personal data so as to ensure full compliance with the principle of data minimisation in Article 5(1)(c) of the GDPR.

Fianna Fáil

Fianna Fáil informed the audit that it does not use Party members, volunteers, activists, or supporters to conduct market research or opinion polling and has not done so for over fourteen years. It said that its polling methodology has never involved the processing of personal data. It explained that when such activity was conducted, individuals were sent to

locations in a constituency where they would ask people if they wished to complete a sample ballot paper. This was totally anonymous. It said that Fianna Fáil developed a constituency polling methodology and model in the mid-1990s. This was undertaken by Party members, on a voluntary basis, and was co-ordinated by Party HQ. Sometime late in the 1990s/early 2000s, the Party moved to external providers to undertake this research. Between 2004 and 2007, the external provider was supplemented by the reintroduction of the member/volunteer polling model. This ended in 2007. Fianna Fáil confirmed that personal data of members of the public or the addresses of those polled were not gathered during the conducting of such activities. It confirmed that individuals did not carry register of electors or marked electoral register information with them at the time of carrying out the task.

The Authorised Officers were satisfied that as the polling activities referred to above did not involve the processing of personal data, no data protection issues arose for consideration by them and it was not necessary for them to make any recommendations to Fianna Fáil in relation to this matter.

Fine Gael

Fine Gael informed the audit that it does not use Party members, volunteers or activists to carry out market research or opinion polling but it has done so in the past (occasionally from the late 1990s up to 2014/2015). It explained that when it was done, volunteers called door-to-door and invited members of the public to take part in a survey, presenting those who agreed with a questionnaire. Typically the questionnaire would have asked participants about their voting intentions, by party, and also asked them to complete a mock ballot paper, listing all likely election candidates. Some demographic information was recorded, for analysis purposes. On occasion, attitudes to various national or local issues might have been recorded.

The total sample varied, depending on the area being polled, but typically varied from 300 to 500, collected using thirty or fifty clusters of ten, as appropriate. Those carrying out the surveys were given a starting point for each cluster and were asked to collect ten samples in the immediate area.

Completed questionnaires were returned and the results were then analysed. Fine Gael stated that no personal data was collected or stored (e.g. name, address) other than information regarding gender and age group of respondents, and the answers to the specific questions included in the questionnaire.

It stated that, in general terms, the findings were used to inform the Party's electoral strategy in a given area, i.e. the number of candidates to run, etc. Feedback may have been analysed according to age or gender to see if there were any significant variations in attitudes. Fine Gael stated that those carrying out these tasks did not carry register of electors or marked electoral register information with them, they did not record names or addresses of participants, and that participants were selected randomly.

Fine Gael stated that typically opinion polls were carried out in the period before an election campaign, all anonymised responses were stored securely at the Party HQ, and were generally destroyed within a short period of time.

Fine Gael also confirmed that members of the public who were approached to take part in polling activities were not informed that the polling was conducted by either members/volunteers/activists/supporters of Fine Gael or by non-Party members on behalf of Fine Gael.

The Authorised Officers were satisfied that as the polling activities referred to above did not involve the processing of personal data, no data protection issues arose for consideration by them and it was not necessary for them to make any recommendations to Fine Gael in relation to this matter.

Green Party

The Green Party informed the audit that it does not currently conduct market research or opinion polling. Over ten years ago some local polling was undertaken by Party activists with members of the public by telephone. The call recipients were not asked what their name or address was or the names of others living at the household. They were asked about their voting intentions for the next elections, their age, gender and

issues in the constituency. Volunteers and supporters acting on behalf of the Party did not give the name of a false or genuine polling company name when conducting the polling. If the call recipient asked who the caller was representing, the activists stated that they were conducting opinion polling on behalf of the Green Party. The Party stated that personal data was not gathered, that information collected from the polling phase was aggregated for statistical purposes and that the hardcopy response sheets from the phone calling phase of the research were destroyed.

It was confirmed to the Authorised Officers by the Green Party that a number of constituency level polls were done along the lines outlined above in the period from 2005 to 2007 but it was not done in all constituencies as the Party did not have the capacity to do so at that time. The Party was unable to confirm whether the polling activity was confined to general elections only. It was confirmed that polling is not done nowadays by the Green Party using professional polling companies or otherwise.

The Authorised Officers were satisfied that as the polling activities referred to above did not involve the processing of personal data, no data protection issues arose for consideration by them and it was not necessary for them to make any recommendations to the Green Party in relation to this matter.

Renua Ireland

Renua Ireland confirmed to the audit that it had used members, volunteers, activists or supporters to conduct market research or opinion polling in the past. It stated that an opinion poll was completed using Google forms. Members were emailed a link and replies were anonymous. Renua Ireland stated that personal data of members of the public was not gathered during such activities and that the only information that was required was gender and whether the person lived in an urban or rural area. The Party confirmed that it is not in possession of data gathered during such activities and that those who conducted the activities did not use either the register of electors or the marked electoral register when so doing.

The Authorised Officers were satisfied that as the polling activities referred to above did not involve the processing of personal data, no data protection issues arose for consideration by them and it was not necessary for them to make any recommendations to the Green Party in relation to this matter.

Sinn Féin

Sinn Féin confirmed to the audit that it conducted opinion polling using party members or supporters. It stated that Sinn Féin supporters conducted polling without revealing that the polling was being conducted by Sinn Féin and that, on occasion, activists did misrepresent, either verbally or by the use of misleading branding, that polling was being conducted otherwise than by Sinn Féin supporters, on behalf of Sinn Féin. It stated that the practice generally ceased in mid-2018 as part of a general increase in awareness in data practices brought on by the advent of GDPR and that for a short period of time thereafter Sinn Féin conducted a very limited number of self-administered private polls without the use of misleading branding.

Sinn Féin stated that these polling practices did not involve the collection of any personal data. Polls were conducted on the basis of blank sample ballot papers being provided at the doorstep to those being polled. No register of electors data or other data was used to identify individuals. Some general demographic data was collected, not from the person polled, but rather was an assessment of the pollster. Pollsters did not poll in their own areas and only polled areas where they were unlikely to know any of the persons being polled. At no point was the identity of the persons whose views were being polled known to Sinn Féin. It stated that the value of the data lay not in individual information about data subjects, but rather in understanding large-scale trends. The sample ballot papers were destroyed once the results were collated. Sinn Féin stated that there is not and never has been any database containing individual preferences

or any information from individual sample ballot papers in respect of those anonymous polls.

During the audit, it was confirmed to the Authorised Officers that the polling activity occurred in the context of general election campaigns only and that over a period of over ten years approximately twenty such polls were carried out for all constituencies. In terms of the demographic data recorded, Sinn Féin said that this was gender data and an estimate of the age profile (e.g. between 18 and 35) of the persons being polled. The sample ballot paper contained the names of election candidates from the previous election as well as the names of likely new candidates. Sinn Féin stated that the polling exercises were not connected in any way to canvassing activities.

The Authorised Officers were satisfied that as the polling activities referred to above did not involve the processing of personal data, no data protection issues arose for consideration by them and it was not necessary for them to make any recommendations to Sinn Féin in relation to this matter.

Solidarity

Solidarity informed the audit that the party does not conduct market research or opinion polling as a standard practice. However, on a few occasions over the last decade it conducted local polls during the final weeks of election periods. Solidarity members conducted opinion polling to gauge expected support for its candidates and others. The polling was conducted at local shopping areas and/or door to door. In each case no personal data was collected. Solidarity members did not use the register of electors when conducting opinion polls and names, addresses or other personal identifiable data was not processed. Each individual was asked how they intend to vote, the issues that most affect them (and their voting preference) and which local area/polling district/estate they live in. That information was then used to produce anticipated voting patterns per

local areas and utilised to inform Party candidates and local teams where they should focus their activity in the final days of the campaign.

The Authorised Officers were satisfied that as the polling activities referred to above did not involve the processing of personal data, no data protection issues arose for consideration by them and it was not necessary for them to make any recommendations to Solidarity in relation to this matter.

Conclusion

As described above, while seven political parties have conducted market research or opinion polling through the deployment of resources from their own membership, supporters or activists, only one political party, Aontú, processed personal data in the context of its market research/opinion polling activities. In the case of Aontú, as the surveys were conducted in an overt manner, those who participated in them were aware at the time of participation that they were providing their personal data and their views on the matters being surveyed to Aontú.

In relation to the market research or opinion polling activities carried out by the other six political parties, the DPC is satisfied from the results of the data protection audits that no personal data was processed by the political parties concerned. On that basis, therefore, no data protection concerns arise for further consideration by the DPC.

Finally, it would be inappropriate for the DPC to comment on any other matters relating to the conduct of the market research/opinion polling.

ENDS

An Coimisiún um Chosaint Sonraí
Data Protection Commission