Constituency Office - Best Practice in the Workplace

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Introduction

An Elected Representative (a member of the Oireachtas, the European Parliament or a local authority) is the data controller for all of the personal data that their office handles, and is responsible for ensuring that the processing of personal data by their office is carried out in compliance with the data protection legal frameworks.[1] This data can include the personal information of staff or voluntary workers, information held for electoral campaigning purposes, and information acquired in the course of constituency casework. Elected representatives, and those who assist them in their work, should be aware of their responsibilities when processing personal data and put in place procedures to ensure that they adhere to the principles of data protection in the course of their work.

The implementation of good data protection practices in the office requires a clear understanding of the personal data held and why that data is held and processed. An elected representative, as a data controller, should also look at how they and their staff process data and identify how this can be improved. Finally, focussing on communications to others about how and why their personal data is processed will assist the elected representative in meeting their obligations to be accountable and transparent as a data controller.

Understand your data

The key to achieving data protection compliance as a data controller is in understanding why the personal data of individuals is obtained and processed and knowing exactly what that data is. It is recommended that an inventory is made of all personal data hold and examined under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?

[1] From 25 May 2018 the key legislative frameworks are the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679); the Data Protection Act 2018; the "Law Enforcement Directive" (Directive (EU) 2016/680) which has been transposed into Irish law by way of the Data Protection Act 2018; the Data Protection Acts 1988 and 2003; the 2011 "e-Privacy Regulations" (S.I. No. 336 of 2011 – the European Communities (Electronic Communications Networks And Services) (Privacy And Electronic Communications) Regulations 2011)

- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

This is the first step towards compliance with the accountability principle, which requires data controllers to demonstrate the ways in which they comply with data protection principles when transacting business. The inventory will also enable controllers to amend incorrect data or track any third-party disclosures.

Data Security

The data protection legal frameworks require data controllers to implement appropriate technical or organisational measures to protect the data that they hold and process. This includes protection against unauthorised access or unlawful processing and any accidental loss destruction or damage. It is the responsibility of all data controllers to put such measures in place using a risk-based approach and taking into account the nature and scope of their data processing operations.

Elected representatives should carry out a risk based approach to data protection. This means that they should implement appropriate and protective measures which correspond to the level of risk of the data processing activities. For example, elected representatives, as data controllers, are required to ensure a level of data security appropriate to the risk and implement risk-based measures for ensuring compliance with the GDPR's general obligations. Risk-based measures could include some of those as outlined in Section 36(1) of the DPA 2018 such as pseudonymisation, encryption and limitation on access. A risk based approach to data protection requires consideration of the following:

1. To identify the potential harm associated with a processing activity.
2. To evaluate the severity of harm that could result.
3. Assess the likelihood of the event by analysing the vulnerabilities of their systems and operations as well as the nature of the threats.

Example 1

A constituency volunteer misplaces a paper list of party members scheduled to carry out canvassing activities. The list contains the members' names, the streets they are to canvass and the dates and times that they are scheduled to do so. As the only personal data contained in the list are the names of the members, this is not likely to represent a serious risk. If the list had identified that they are members of the party, this would present a more severe risk, as information revealing a person's political opinions is a special category of data.

Example 2

A laptop belonging to an elected representative is stolen from their car. This laptop contains folders of information on constituents related to representations made on their behalf, including medical data obtained from hospitals and personal data pertaining to Local Authority housing applications. If the laptop is password locked and the files are protected by encryption software, this should not present a serious risk to the data subjects, as it is unlikely that any third party will be able to access the data. However, if the laptop is not equipped with adequate security measures, this will present a more serious risk as there is a much greater likelihood of the data subjects' sensitive data being accessed by a third party and potentially used to harm them.

Breach reporting

Elected representatives, as data controllers, should be mindful of their obligation to report breaches of personal data to the Data Protection Commission, and to report the breach to the individual(s) concerned where the breach is likely to result in a high risk to their rights and freedoms. Further guidance on this is available on the Commission's website.

In most offices, personal data will be stored and processed using computers and other information technology solutions. There is a range of security measures available for the protection of electronic data, including password protecting files and using encryption on laptops and portable storage devices. It is also important to ensure that any anti-malware software that is used is kept up to date.

On occasion, constituency staff members and campaign volunteers may process personal data using their own devices (laptops, mobile phones etc.). Elected Representatives as Data controllers should be aware of the devices that may be used to process data and put in place clear policies and guidelines around any such usage.

Where personal data is kept in hard copy, paper files there is a range of measures that may be taken to protect it. This can include keeping files in locked rooms or cabinets, ensuring that data is securely disposed of or shredded when no longer needed, and ensuring that the minimum amount of personal data is taken away from the office.

Access controls are a key organisational measure to protect personal data. In general, staff members should only have access to the personal data that they require to carry out their tasks. Policies and procedures can be put in place whether electronic or paper files are used, to govern access to personal data and to document when access is made and by whom.

Training and awareness raising are fundamental to ensuring that staff members implement good data protection practices in the office. This will assist in maintaining a culture of respect for the personal data of constituents and others that may be processed, as well as helping to prevent any data protection breaches. It may be deemed appropriate to arrange specific data protection training for staff, but also ensuring that staff are properly trained in the use of any software that they may use to process data will reduce the risk. It is recommended that a data protection policy be put in place and made available to all staff.

Accountability and Transparency

The data protection legislative frameworks require data controllers to process data transparently and to be accountable to both the individual data subjects whose data they process, and the Data Protection Commission.

The key to the transparent processing of personal data is the timely provision of information to individuals whose data is processed about what is going to happen to their information. Where personal data is obtained from an individual, they must be provided with the following information at a minimum:

(a) The identity and contact details of the controller
(b) The contact details of the data protection officer, if applicable
(c) The purposes of the processing for which the personal data are intended as well as the legal basis for processing
(d) The period for which the personal data will be stored
(e) The existence of their right to access and rectification or erasure of personal data

Where staff members are engaging with members of the public, for example compiling mailing lists at public meetings, they should be in a position to provide this information. If a website is used to provide information to constituents, and especially if the site is used to obtain any personal data through forms or portals, a privacy notice should be put in place to ensure that individuals are adequately informed.

Subject Access Requests

The data protection legislative frameworks provide individuals with the right to obtain information as to whether their data is processed by a data controller and to access the data in question. When an individual exercises this right, it is referred to as a *data subject access request*, and all data controllers should have procedures in place for facilitating such requests.

When a request for information about, or access to, data is received, it must be responded to without undue delay and at the latest within one month (30 days). There is no fee applicable for the provision of any copies of data that may be requested.

It is important that data controllers and their staff are able to recognise and respond to access requests that may be received through any of their public channels of communication. Where an access request is not responded to or they are unsatisfied with the response, the data subject may make a complaint to the Data Protection Commission.

When a request has been received, the controller can take whatever steps they deem necessary to verify the identity of the individual and may ask them to specify the particular data or range of data that they wish to access. Implementing good office management practices will assist in responding to access requests as it will be easier to identify all of the relevant data in a timely manner.

The right of access to personal data may be restricted in certain circumstances. Section 60 of the Data Protection Act 2018 outlines the exemptions that may be applied to restrict the exercise of their rights by a data subject, including the right of access. The rights of the data subject are restricted to the extent that the restrictions are necessary and proportionate –

1) to safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State,
2) for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties,
3) for the administration of any tax, duty or other money due or owing to the State or a local authority in any case in which the non-application of the restrictions concerned would be likely to prejudice the aforementioned administration,
4) in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure,
5) for the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim, or
6) for the purposes of estimating the amount of liability of a controller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the commercial interests of the controller in relation to the claim.[2]

The right of access may also be restricted where the personal data relating to the data subject consist of an expression of opinion about the data subject by another

[2] Section 60(3)(a) Data Protection Act 2018

person given in confidence or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving the information.[3]

These exemptions to the right of access should be interpreted narrowly and applied on a case-by-case basis. Where it is deemed necessary and proportionate to restrict the right of access based on one of the grounds outlined above, the data subject should be notified of this in writing within one month of the receipt of their request. The data subject should also be informed of their right to complain to the Data Protection Commission about the restriction of access to their personal data.

December 2018

[3] Section 60(3)(b) Data Protection Act 2018