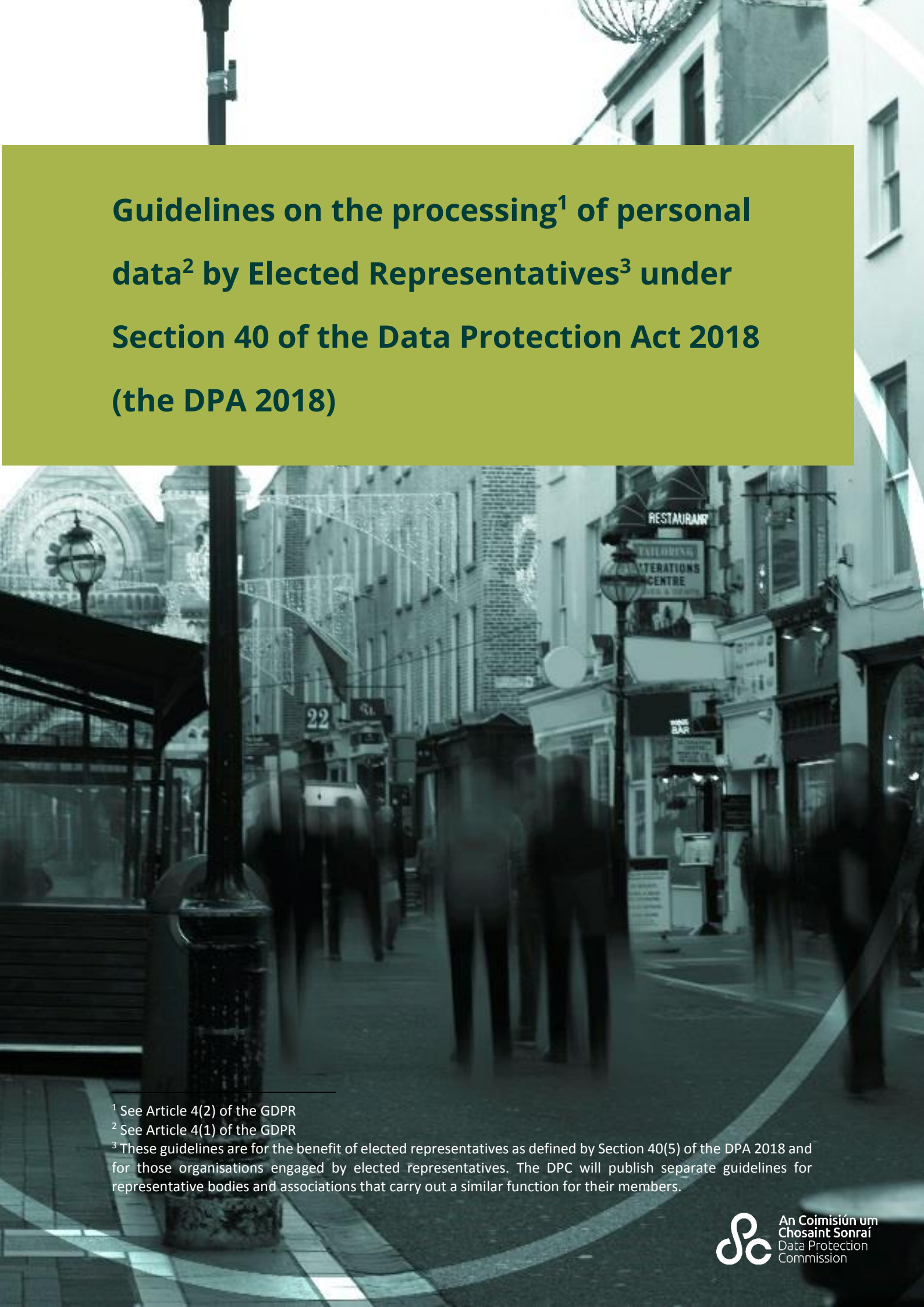
Guidelines on the processing[1] of personal data[2] by Elected Representatives[3] under Section 40 of the Data Protection Act 2018 (the DPA 2018)



[1] See Article 4(2) of the GDPR
[2] See Article 4(1) of the GDPR
[3] These guidelines are for the benefit of elected representatives as defined by Section 40(5) of the DPA 2018 and for those organisations engaged by elected representatives. The DPC will publish separate guidelines for representative bodies and associations that carry out a similar function for their members.

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Introduction

Elected representatives may, during the course of their activities, be asked to make representations to, and on behalf of, an individual (a data subject). This is a normal and important democratic function which typically occurs in relation to access to services or to information about the provision of services. When people contact their elected representative wanting representations to be made on their behalf, they are asking for assistance and expect that the elected representative will be able to respond effectively and efficiently to their concerns. However, there is also a responsibility on elected representatives to protect the personal data of their constituents, particularly where processing involves special categories of personal data[4]. Section 40 of the DPA 2018 finds a balance between these two positions, intention of which is to provide "a robust legal basis for the making of representations by Members of the Houses of the Oireachtas and members of Local Authorities"[5].

Sections 40(1) and (2) of the DPA 2018 provide an elected representative[6] with a legislative basis for the processing of the personal data (including special categories of personal data) of individual constituents in order to perform their functions[7]. The processing of personal data by an elected representative is permitted under Section 40 where:

[4] Special categories of data are defined in Article 9(1) of the GDPR.
[5] Minister for Justice and Equality, Deputy Charles Flanagan, Select Committee on Justice and Equality debate, Thursday, 3 May 2018.
[6] See Section 40(5) – Member of the Houses of the Oireachtas, European Parliament or a local authority.
[7] It should be noted that an elected representative could also rely upon consent (and explicit consent if involving special categories of data) as a separate legal basis under Article 6 (and a condition under Article 9) of the GDPR to process personal data on behalf of the data subject.

(i) the elected representative either receives a request or representation directly from the data subject, or where

(ii) the elected representative receives a request or representation from another person on behalf of the data subject and the elected representative is able to demonstrate that they are compliant with the principles of data protection[8].

These guidelines set out the obligations on elected representatives in relation to the making of such representations on behalf of the data subject and their responsibilities in relation to personal information that comes into their possession and control. They also set out the obligations placed upon organisations (public and private data controllers) that process representations made on behalf of individuals by elected representatives.

Lawfulness, Fairness and Transparency

In advance of any processing of personal data, an elected representative should ensure that the individual who makes a request for representation is made aware, *inter alia*, of the nature and possible extent of the processing of personal data which may take place on foot of such an engagement[9]. An elected representative as a data controller is obligated, at a minimum, to meet their transparency responsibilities set out in the GDPR[10]. For further guidance please note the following publication on transparency issued by the Article 29 Working Party (WP29) which has been endorsed by the European Data Protection Board (the EDPB)[11]:

[8] See Article 5 (1) of the GDPR for the principles: (a) Lawfulness, fairness and transparency, (b) purpose limitation, (c) data minimisation (d) accuracy (e) storage limitation (f) integrity and confidentiality and Article 5(2) Accountability. These principles apply to all processing activities carried out by data controllers.

[9] For example if there is a possibility that personal data in relation to a representation may be made public either through, for instance the availability of minutes of public meetings or public webcasts by a public authority it is important that the individual in made aware and is cognisant of this possibility in advance of the processing.

[10] See for instance as provided for in Articles 12, 13 and 14.

[11] The EDPB has endorsed the guidance provided on the GDPR provided by WP29.

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Recommendation

Elected representatives should use privacy notices whenever they collect personal information about people and have a privacy notice on their website. It is recommended that a specific privacy notice is drafted in relation to public representations on behalf of individuals. These notices should satisfactorily address the requirements set out in Articles 12, 13, 14 & 30 (where relevant) of the GDPR and also should be clear, accessible and informative to help people to understand what will be done with their personal information.

Under Article 40(1) and Article 40(2) an elected representative will need to be satisfied that they are, at all times, acting upon a request from the data subject. In many instances, the permission of the individual can be implied from a relevant action or request[12]. For example, the raising of the matter by an individual will create an expectation that their personal data will be further processed by the elected representative and other relevant organisations. In such cases they will expect the elected representative will process any personal information provided and recipient organisations will disclose their personal information to the elected representative where this is necessary to provide an appropriate response. However, there may be circumstances where the processing will go beyond the expectation of the individual particularly where there is uncertainty over their wishes or where there is a possibility of unexpected and/or sensitive personal information being processed as part of the request. For instance, an individual may ask for assistance from an elected representative in terms of trying to access specific public health services. However, the elected representative then uses this

[12] Provided that the elected representative satisfactorily meets his/her transparency requirements in relation to this particular processing activity See Articles 12 – 14 of the GDPR.

request and the personal details obtained to advocate on a national level for improved provisions of public health services. In cases like this it could be appropriate for the elected representative to revert to the individual to ensure they are aware of the nature of their request, the personal data involved, the processing that is likely to take place on foot of such a request, the publicity this request could generate and that the individual is happy to proceed on that basis.[13] Elected representatives should be particularly vigilant when the request for representation involves the possible disclosure or release of special categories of the data concerning the individual[14]. In general, an elected representative should obtain the explicit consent of an individual to receive and process this type of personal data[15].

The responsibilities of an elected representative are amplified if the request has come indirectly to them. Section 40(1), in conjunction with Section 40(2) of the DPA 2018 requires, where the request or representation is received from another person on behalf of the individual concerned, that the elected representative ensures the said request/representation is valid and lawful. Therefore the elected representative will need to satisfy themselves that the conditions of consent (as outlined in Article 7 of the GDPR) are met and that the individual has the authority to make a request on behalf of the data subject. For example, they may need to take reasonable steps to establish that an individual has appropriate legal standing to manage the affairs of an individual, such as guardianship or enduring power of attorney[16].

[13] An organisation in receipt of a representation of this nature must include measures to ensure that the rights and freedoms of a data subject are protected – see Section 40(4) of the DPA 2018

[14] An organisation which controls and holds the personal information in respect of the request would need to implement appropriate safeguards before considering disclosing personal information of this nature to the elected representative see Section 40(4) and Section 36 of the DPA 2018.

[15] An organisation that intends to disclose this type of data will be required to implement specific safeguards, including the receipt of undertakings from the elected representative that the individual has explicitly consented to the disclosure of this data.

[16] The provisions of the Assisted Decision-Making (Capacity) Act 2015 will also be very relevant.

For further information on consent, please note the following guidelines of the WP29 endorsed by the European Data Protection Board[17]:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

There may be specific circumstances where an elected representative is unable to ascertain those wishes from the individual in advance of making a representation and sound judgement will be important in such situations in deciding how to proceed [18]. Ultimately, it will be a matter for the elected representative to justify their decisions in making a representation where they have not fully ascertained the wishes of the individual in advance of the processing. In general, it will only be permissible to act in such a manner in exceptional circumstances; particularly where an individual cannot give (or be expected to give) consent. An elected representative would need to justify the processing of personal data on this basis by setting out and recording the steps taken to ascertain those wishes before proceeding. This will assist them when making a representation to an organisation. In addition, it may be appropriate for an elected representative to seek alternative assurances to confirm the bona fides of the request and, where relevant, to confirm that a signed consent will be provided by the individual following the making of the representation[19].

[17] Formerly known as the Article 29 Working Party.
[18] For instance, a representation may be time sensitive and require immediate action.
[19] For example, they could seek a formal declaration or undertaking from a person who is making a request on behalf of the individual

Recommendation

It will be a matter for the elected representative to demonstrate their compliance with Section 40 of the DPA 2018 and clearly, a signed and appropriately detailed written request from a data subject/constituent is the optimum approach to take. However, there may be instances where this proves impractical or may create unreasonable barriers for elected representatives to carry out their duties on behalf of their constituents in an effective manner. For example, an individual may make their request verbally to the elected representative. It is recommended that a sufficiently detailed and contemporaneous record is made and kept by an elected representative in respect of all requests made by data subjects or indirectly by another individual on behalf of the data subject. Such a record will be a useful document to assist an elected representative in demonstrating their compliance with Section 40 of the DPA 2018 and the GDPR.

Purpose Limitation

An elected representative should be clear about the purpose for which the personal data is processed when a request for representation is made by an individual. An individual contacting an elected representative may not want their details used for any other purposes other than their stated request.

Recommendation

An elected representative should not assume that an individual who makes a request for a representation automatically wishes to have their email address used for political canvassing.[1] It is important therefore that information obtained through constituency casework (including requests for representation) should be appropriately categorised and distinguished from personal information obtained and processed on foot of a different lawful basis. Privacy notifications should reflect the different processing activities engaged by elected representatives.

Data Minimisation

It is important for an elected representative to ensure that they process and hold personal information that is relevant and limited to what is required to make an effective representation on behalf of the individual. They should consider how much of the information it is necessary to give to the organisation in order for them to make an adequate representation. In short, they should only process the personal data necessary to achieve the objective sought. In many instances, it may be possible to withhold some of the information and still adequately represent the individual. Any unnecessary personal information should be returned to the individual or deleted if is not required for the stated purpose of the request.

Accuracy

Processing of inaccurate or incomplete information has the potential to cause distress or embarrassment for an individual. Particular care is required when personal information is obtained from another person or organisation rather than directly from the data subject or when the relevant information is sensitive. Elected representatives should be very attentive to the accuracy of the data and ensure that correspondence is not sent to the wrong address. Individuals have a right to correct inaccurate information without undue delay as per Article 16 of the GDPR.

Recommendation

It is advisable that a procedure is implemented to ensure the personal data remains accurate. It is also important to ensure that assumptions as to the accuracy of data are avoided and that contact details of an individual and the facts of the issue are up to date with the individual concerned. For example an individual may request an additional representation on foot of a previous request with the same elected representation. In such instances the elected represented should never assume the information previously received remains the same and they should seek an update as to the facts of the matter.

Storage Limitation

Neither the GDPR or the DPA 2018 prescribes a period of retention for personal information collected via a public representation. The purpose(s) of the request will be determinative in settling on an appropriate retention period and this decision rests with the data controller.[20] In general, personal data should be processed for as long as is necessary to meet the purpose of the request. Elected representatives should be clear about the criteria they use to determine the retention period for personal information obtained under such a request and include this information in their privacy notice.

Integrity and Confidentiality

Elected representatives have discretion to decide what security measures to apply in any given circumstance. However, they must apply appropriate security standards which can vary according to the nature of the data concerned and the

[20] Regard may also be had to other statutory obligations imposed on a data controller.

harm that may ensue if inadequately protected. In particular, they should think carefully about the security arrangements for sensitive personal data and how they intend to impose limitations to access.[21]

Recommendation

Technical and organisational measures, such as use of passwords, computer access privileges, procedures and staff training are appropriate to keep the information safe. In particular provisions should be put in place for anyone who can access personal data, including staff, volunteers and third party services providers (such as cloud hosting service providers) and these should be formalised in contracts and confidentiality agreements.

[21] Section 40(3) of the DPA 2018 mandates elected representatives to impose limitations on access to special categories data to prevent unauthorised disclosure and processing.

Disclosure of Personal Data by an Organisation on foot of a Section 40 request

Section 40(4) establishes a legal basis permitting organisations to respond to and process personal data on foot of a representation received from an elected representative.[22] As a data controller, those organisations will also need to comply with the principle of accountability by demonstrating their compliance with all other principles of data protection.[23] It is therefore a matter for each organisation to determine how to implement best practice standards which meet the provisions of Sections 40(4) and 36 of the DPA 2018. However, it is also important those standards are not overly burdensome whereby an elected representative is impeded to such a degree that they are unable to carry out this important democratic function on behalf of individuals in an effective manner**.**

The DPC advises that where a public representative makes a written representation on behalf of a constituent on foot of Section 40, the organisation can generally assume that the constituent has given their permission for the release of personal data necessary to respond to the representation. In other words the organisation may accept the *bona fides* of elected representatives who state they are acting on behalf of a member of the public. As the organisation is accountable for the personal data it has chosen to release, it should be satisfied that it is reasonable to assume that the individual whose personal data is released would have no objection to such a release through a public representative. In

[22] Section 40(4) For the purpose referred to in *subsection (1)* and to the extent that disclosure is necessary and proportionate to enable an elected representative to deal with a request or representation referred to in that subsection, subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of the data subject, it shall be lawful for a person to disclose to the representative or a person acting on his or her behalf personal data and special categories of personal data of a data subject who makes the request or representation, or on whose behalf the request or representation is made, as the case may be, to enable that representative respond to that request or representation.

[23] See Article 5 of the GDPR

most cases, this is unlikely to be an issue especially in relation to the many representations made on behalf of individuals who simply wish to know when a particular service will be provided.

If the elected member makes a verbal representation to the organisation on behalf of a data subject it is advisable that the member of staff of the organisation makes a contemporaneous record of the details of the representation, including the identity of the elected representative and data subject, the time & date and other relevant particulars concerning the nature of the request. This should be completed before assessing whether to comply with the request. If the elected member is physically present when making a verbal representation it may also be appropriate to ask them to sign a short form which confirms the relevant details and purpose of the request.

Ultimately, it will be a matter for the organisation to decide whether to accede to a request on the basis that their own suitable and specific measures (which have been implemented to safeguard an individual's fundamental rights and freedoms) have been met. However, those organisations should be cognisant of the wishes of their customer or citizen when making a determination.

Appropriate policies and privacy notices should be drafted and published which outline how an organisation will manage and process personal data following the receipt of a request. In this regard the organisation, as a data controller, must also ensure they meet their responsibilities under Articles 12, 13, 14 and 30 of the GDPR. Accessible policies and privacy notices will assist organisations, data subjects and elected representatives alike in understanding what is required and entailed in making and replying to a representation. These documents will also prove useful in ensuring the representation is expediently acted upon.

Reliance upon Section 40(4) as a legal basis to disclose data on foot of a representation is dependent upon certain conditions being met advance:

Necessary and Proportionate

The principle of data minimisation requires that the minimum amount of data should be processed to achieve a given purpose, and where possible the processing of personal data should be entirely avoided. This means that where an elected member requests the release of a constituent's data, the disclosure should be limited to information strictly necessary to answer the question raised by the constituent. If the constituent's question can be answered without the need to disclose their personal data, this would be preferable. The disclosure must also be deemed proportionate in its impact upon the fundamental rights and freedoms of the individual concerned. When making the initial request to their elected member to raise a query on their behalf, the constituent and elected representative may not have considered the potential implications of the disclosure of their personal data (including special categories of data). Organisations should assess whether there could be a potentially negative impact for an individual arising on foot of a representation and subsequently implement appropriate measures which may mitigate those risks. For instance, the request could involve particularly sensitive data which is historical in nature and whilst this data is important in terms of the representation the individual concerned may not appreciate this. In such circumstances it would be advisable to seek further assurances that the disclosure of data is permissible.

*S*uitable and Specific Measures

While it will be reasonable to assume that the elected member is making a request for disclosure of personal data in good faith having been requested to do so by

the data subject, upon receipt of a request an organisation must implement suitable and specific measures to ensure that individual's rights and freedoms are protected[24]. The type of measures chosen will be very much contingent on the nature of the representation and the personal data at issue[25].

An organisation may wish to satisfy itself that the individual who has sought the representation via the elected member is fully aware of the implications that follow the processing of their personal data on foot of such a request and that they consent for the organisation to process personal data on that basis. However, the organisation must also be mindful of the nature and purpose of the request. For instance, some representations may be time sensitive and the insistence on receipt of explicit consent by an organisation may prove problematic for the elected representative to carry out their role in an effective manner. Clearly, there is an onus placed upon the elected representative to provide sufficient details as to the nature of the request but an organisation should also apply a common sense approach when considering such requests. For example, it will be unnecessary in most situations for an organisation to insist on explicit consent when in receipt of a written representation of an elected representative, particularly when this would inevitably lead to a delay such that the objective of the request could not be met and particularly when the personal information at issue is non-sensitive[26].The written request itself should be sufficient for the organisation to proceed on that basis[27].

[24] See Section 36 of the DPA 2018

[25] Clearly, where the personal data at issue is of a more sensitive nature (i.e. special categories of data, or data pertaining to the investigation or prosecution of an offence) additional and perhaps more stringent safeguards may need to be considered and imposed.

[26] For instance, an elected representative receives a request from a constituent who is in prison asking for assistance to attend the funeral of a relative. When the elected representative contacts the prison he is told that it could not provide any personal information without his constituent's explicit consent despite the fact that the constituent had contacted his elected public representative requesting assistance. Delay in obtaining confirmation of explicit consent could easily result in it being too late for that individual to attend the funeral.

[27] The written request (or verbal request) will however need to provide and set out relevant information and assurances.

If an organisation is concerned that the elected representative or individual (or both) may not be fully appreciative of the nature and sensitivity of the personal data at issue it may be appropriate that the elected member, individual or both are contacted directly, informed of the position and asked to review their request on that basis. Alternatively, if the request involves information of a highly sensitive nature, that personal data could be withheld from the documentation which is provided on foot of the disclosure.

It may be prudent for the organisation to inform an elected representative of any concerns they may have regarding a disclosure and seek further assurances from them the representative as well as the individual. Additional measures may also be introduced in order for an organisation to satisfy itself as to the appropriateness of disclosing personal data where the representation has been made on behalf of the data subject by another individual due to their incapacity or age. This could occur where the constituent makes enquiries about the provision of services to their relative and where it is not clear that their relative supports, or is even aware of, the representation being made.

Other examples of where measures will be required is when access is sought to information which would involve disclosure of personal data in relation to others (e.g. it may be wrong to release the names of the top ten individuals on a waiting list without their consent) or where the representation is made in the context of the constituent's involvement in a dispute with third parties. In general it is not permissible to process the personal data of third parties under Section 40 of the DPA 2018. It will only be permissible in very narrow circumstances to process personal data relating to a person who has not been involved in the request for

representation or subsequent discussions and where it can be shown that any of the following conditions apply

- the third party involved cannot give explicit consent; or
- the elected representative ''cannot reasonably be expected to obtain'' the third party's explicit consent; seeking the third party's explicit consent would ''prejudice the action taken by the elected representative''; or
- the processing is necessary in somebody else's interest and explicit consent has been ''unreasonably withheld'' by the third party; and
- the balance favours the disclosure of the personal data on the basis of the public interest.

Special Categories of Data

Particular care is required where the personal information being released qualifies as special categories of data under the DPA 2018 (i.e. information about the health of an individual). Representations made under Section 40 of the DPA 2018 may appropriately justify the processing of special categories of personal data relating to the data subject's health or personal circumstances.[28] However, suitable and specific measures that take on board the provisions of the Data Protection Health Regulations should be considered[29]. These regulations provide that health data relating to an individual should not be made available to the individual, in response to an access request, if that would be likely to cause serious harm to the physical or mental health of the data subject. A person who is not a healthcare professional should not disclose health data to an individual without first consulting that individual's own doctor, or some other suitably qualified health professional. Similarly, if it is considered appropriate to disclose such

[28] Provided the processing is necessary.
[29] See the Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989) and the Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83 of 1989) which remain in force as per Section 68 of the Act.

personal data to an elected representative it may be appropriate to include a warning pertaining the sensitive nature of the data[30].

Where a representation involves the processing and disclosure of Article 10 data to an elected representative it will, in general, be expected that the organisation has obtained sufficient assurances from the elected representative that the individual has explicitly consented to the request[31].

Section 40(4) of the DPA 2018

Section 40(4) does not compel a data controller to accede to a request or representation from an elected representative. Rather, it provides a legal basis to permit an organisation in receipt of a representation to process and disclose personal data. It should remove unnecessary bureaucracy and delay in managing requests. All stakeholders therefore need to apply a common sense and transparent approach. For instance, a letter of request with the relevant information and assurances from the elected representative should suffice for the release of relevant personal data in most cases. It is in the interest of elected representatives to provide relevant information to the organisation concerning the representation as the absence of appropriate details and information may delay or impede a reply.[32] It is also in the interests of an organisation to set out and publish clear protocols in respect of their application of Section 40(4). This will help manage expectations for all stakeholders in advance of receiving a representation. If an organisation refuses to act (or partially acts) on foot of a representation made by an elected representative they should be in a position to adequately explain their decision to the elected representative (and to the

[30] If an elected representative is provided special categories of personal data of an individual on foot of a representation they will also need to ensure that they apply sufficient safeguards as per Article 40(3) when processing this data.

[31] Please note the provisions of Article 10 of the GDPR and Section 55 of the DPA 2018.

individual) on the basis of Section 40 rather than citing data protection requirements as a general ground for refusal.[33]

Recommendation

Elected representatives and organisations should develop clear procedures and policies to give further effect to Section 40 of the DPA 2018. They should also publish these for the purposes of transparency. A code of conduct may be an effective tool to frame the processing activities relating to public representations. It could lead to the development of a collective and consistent approach to this particular processing activity. A code provides an opportunity to establish a set of rules that contribute to the proper application of the GDPR in a practical and transparent manner and which take on board the nuances of a particular processing activity. Adherence to an approved code under Article 40 of the GPDR is a useful method to demonstrate compliance with the provisions of the GDPR (and the DPA 2018).

If an organisation can demonstrate it has complied with Section 40(4) (and the GDPR and associated principles of data protection) by implementing and applying suitable and specific safeguards it should be confident that it has discharged it obligations in a compliant manner under the DPA 2018.

December 2018

[33] In situations where the information provided by an organisation is not clear as to the reason for the refusal or delay to act, an individual may decide to make a subject access request to obtain their personal information, which they then give to their elected representative. This would clearly not be in the interests of any stakeholder and against the spirit of the legislation.