DECISION

RIBBLE VALLEY BOROUGH COUNCIL
REPORT TO POLICY AND FINANCE COMMITTEE

Agenda Item No 8

meeting date: 20 MARCH 2018
title: GENERAL DATA PROTECTION REGULATION (GDPR)
submitted by: DIRECTOR OF RESOURCES
principal author: LAWSON ODDIE

1 PURPOSE

1.1 To provide members with details of the new requirements under GDPR and the implications for this council.

1.2 The report also looks at the requirements under the Data Protection Act 1998 and GDPR for members in their various roles as:

- A member of the council;
- Representative of residents of their ward;
- Representing a political party, i.e. at election time

1.3 Relevance to the Council's ambitions and priorities:

- Community Objectives – none identified
- Corporate Priorities - to continue to be a well-managed Council providing efficient services based on identified customer need.
- Other Considerations – none identified.

2 BACKGROUND

2.1 Currently, all organisations in the UK that collect, process or store personal information must comply with the Data Protection Act 1998 (DPA), or face fines of up to £500,000 in the event of a data breach.

2.2 The DPA will soon be superseded by the EU General Data Protection Regulation (GDPR), which introduces tougher fines for non-compliance and breaches, and gives people more say over what companies can do with their data. It also makes data protection rules more or less identical throughout the EU.

2.3 The EU's General Data Protection Regulation (GDPR) is the result of four years of work by the EU to bring data protection legislation into line with new, previously unforeseen ways that data is now used.

2.4 The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

3 REQUIREMENTS AND RIGHTS UNDER GDPR

3.1 Like the Data Protection Act, GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and expansive providing a wide range of personal identifiers that constitute personal data, reflecting the changes in technology and the way organisations collect information about people.

3.2 It can be assumed that any data held that falls within the scope of the Data Protection Act will also fall within the scope of GDPR. It not only applies to electronic personal data but to manual filing systems.

3.3 The data protection principles under GDPR set out the main responsibilities for organisations. The principles are similar to the current DPA principles (fair and lawful, purpose, adequacy, retention, right, security, international), with added detail at certain points and a new accountability requirement.

3.4 Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. 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.

3.5 The accountability principle requires that the organisation put in place comprehensive but proportionate governance measures. The following procedures, policies and frameworks will become a requirement under GDPR and should minimise the risk of breaches and uphold the protection of personal data:

- Information Audit
- Establish an information asset register
- Privacy Impact Assessments
- Documented procedures for Subject Access Request
- Privacy by design

3.6 GDPR also creates some new rights for individuals and strengthens some that currently exist under the Data Protection Act.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

3.7 A duty is placed on all organisations to report a data breach to the Information Commissioner's Officer (ICO) within 72 hours of the organisation becoming aware of it and to inform affected subjects as soon as possible.

3.8 The ICO will be supervisory authority for the UK. Under GDPR the ICO will have the power to spot audit organisations with little prior notice. If the ICO find that an organisation is not compliant to GDPR they have the power to fine and/or stop the organisation from processing personal data

3.9 Under the Data Protection Act the ICO could apply fines of up to £500,000. Under GDPR lesser incidents could expect fines of up to £7.9 million or 2 per cent of the organisations global turnover (whichever is greater). More serious violations could result in fines of up to £16 million or 4 per cent of turnover (whichever is greater).

4 ROLE OF THE DATA PROTECTION OFFICER UNDER GDPR

4.1 The General Data Protection Regulations state that a Data Protection Officer should be designated by local authorities to take responsibility for data protection compliance.

4.2 The role should be the first point of contact for all data protection matters and must report directly to the board (management team). There is also a requirement that they must have enough resource to perform the function to ensure the organisation is compliant with GDPR.

4.3 As part of their role, they must also provide compliance training and annual refresher training to all staff that come into contact with personal data and consistently monitor and benchmark the organisation's levels of compliance.

4.4 Highlighted under GDPR and by the ICO have been issues around potential conflicts of interest for those holding the role of Data Protection Officer. The role of Data Protection Officer at this council currently sits with the ICT Manager.

4.5 The legislation is not prescriptive on where the role should sit within the organisation. However, there is recognition that in some cases there may be conflicts of interest that make someone inappropriate for the role. It is recognised that the Data Protection Officer cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data.

4.6 As a result a potential conflict of interests has been identified for our current Data Protection Officer role (ICT Manager) and work is ongoing to identify how this conflict of interests can best be addressed.

4.7 In the changeover to GDPR there is likely to be an extensive workload for the Data Protection Officer role in ensuring our compliance. However, in the medium to longer term it is possible that this workload **may** lessen as compliance becomes more embedded in our processes. There is a potential that additional staffing resources may be needed in order for us to meet our statutory requirements.

5 IMPLICATIONS FOR MEMBERS

5.1 Councillors are likely to have three different roles:

- As a member of the council, for example, as a member of a committee.

- A representative of residents of their ward, for example, in dealing with complaints.
- They may represent a political party, particularly at election time.

5.2 For work as a member of the council, in some circumstances members may require access to personal information. In this case it is the council rather than the councillor that determines what personal information is used for and how it is processed. For example, if a member of a committee has access to files to help them in considering a matter, the councillor is carrying out the local authority's functions and so does not need to register in their own right.

5.3 When councillors represent residents of their ward, they are likely to have to register in their own right. For example, if personal information is used to timetable surgery appointments or take forward complaints made by local residents.

5.4 When acting on behalf of a political party, for instance as an office holder, councillors are entitled to rely upon the registration made by the party. When individuals campaign on behalf of political parties to be the councillor for a particular ward, they can rely on the parties' registration if the party determines how and why the personal information is processed for the purpose of their individual campaigns. If a councillor is not part of any political party but campaigning to be an independent councillor for a particular ward, they need to have their own registration.

5.5 There is a clear distinction between when a councillor is a data controller in his/her own right in their advocacy work when dealing with constituency casework, as they decide how personal data is processed/handled, and when they are carrying out their duties as a representative of the council rather than as a representative of the constituent.

5.6 Based on the above summary, there is a highly likely requirement (depending on what processes each individual member may have in place) for members to register under Data Protection for their processes in relation to their constituency casework. Further guidance is given in the attached Annex 1 *(Advice for elected and prospective councillors).* The Head of Legal and Democratic Services has previously written to all members with regard to these requirements.

5.7 As a safeguard it would be suggested that each member be registered under Data Protection for their processes, and this could be undertaken centrally by the council for all members.

5.8 There is an associated cost to such registration, currently £40 per registration. This would equate to a total annual cost of £1,600. It is a consideration of this report and for members as to:

- Whether each member should register individually with the ICO;
- Whether the council should submit registrations for all members;
- Whether the annual cost of registration should be met by members or by the council.

6 CONCLUSION

6.1 The new GDPR requirements will apply in the UK from 25 May 2018.

6.2 There is a high level of workload in the short to medium term to ensure that we are compliant with the new requirements. It is possible that this workload **may** continue longer term under GDPR. Consideration needs to be given as to how the potential conflict of interests is best addressed. This is currently being looked at by management team.

6.3 It has been highlighted that the undertakings of members in respect of constituency casework and the processing of personal data means that depending on individual circumstances, members may need to register with the ICO. It is possible for this to be done centrally if desired, but there is a charge associated with registration. A decision is needed as to whether this charge is met by the council or by each individual member.

7 RISK ASSESSMENT

7.1 The approval of this report may have the following implications

- Resources: Should the council stand the cost of each member's registration with the ICO, this would represent an annual charge of £1,600. There is also the potential that additional staffing resources may be needed in order for us to meet our statutory requirements.
- Technical, Environmental and Legal: From 25 May 2018 it will be a legal requirement to meet the GDPR. It is currently a legal requirement to meet the Data Protection Act 1998
- Political: none
- Reputation: There would be an adverse reputation risk if found in breach of the requirements of the Data Protection Act 1998 or GDPR
- Equality and Diversity: Equality and diversity issues are considered in the provision of all council services

8 RECOMMENDED THAT COMMITTEE

8.1 Consider whether the council should pay for the registration fees for all members in respect of their constituency role

8.2 Note the potential that additional staffing resources may be needed in order for us to meet our statutory requirements.

HEAD OF FINANCIAL SERVICES DIRECTOR OF RESOURCES

PF25-18/LO/AC
6 March 2018

Advice for elected and prospective councillors

Data Protection Act

Contents

Introduction

1. The Data Protection Act 1998 (DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it

2. An overview of the main provisions of the DPA can be found in The Guide to Data Protection.

3. This is part of a series of guidance, which goes into more detail than the Guide, to help data controllers to fully understand their obligations and promote good practice.

4. This guidance aims to provide elected and prospective councillors with advice on how the DPA applies to them.

The role of the councillor

5. Councillors are likely to have three different roles:

    - As a member of the council, for example, as a cabinet member or a member of a committee.

    - A representative of residents of their ward, for example, in dealing with complaints.

    - They may represent a political party, particularly at election time.

Use of personal information

6. When councillors consider using personal information, they should take into account the context in which that information was collected to decide whether their use of the information will be fair and lawful, as required by principle 1 of the DPA:

    - Where a councillor is representing an individual resident who has made a complaint, the councillor will usually have the implied consent of the resident to retain relevant personal data provided and to disclose it as appropriate. The resident will also expect that the organisations (including the local authority) who are the subject of the complaint will disclose personal data to the councillor. If

there is any uncertainty regarding the resident's wishes, it would be appropriate to make direct contact with the resident to confirm the position.

- Sensitive personal information is treated differently; for example, where consent is being relied on this should be explicit in nature. However, in the context of a complaint, councillors – and organisations making disclosures to them - will usually be able to rely on the Data Protection (Processing of Sensitive Personal Data)(Elected Representatives) Order 2002 as a condition for processing.

- Personal information held by the local authority should not be used for political purposes unless both the local authority and the individuals concerned agree. It would not be possible to use a list of the users of a particular local authority service for electioneering purposes without their consent. An example would be using a local authority list of library users to canvass for re-election on the grounds that the councillor had previously opposed the closure of local libraries.

- When campaigning for election as the representative of a political party, candidates can use personal information, such as mailing lists, legitimately held by their parties. However, personal information they hold in their role as representative of local residents, such as complaints casework, should not be used without the consent of the individual.

- When campaigning for election to an office in a political party, councillors should only use personal information controlled by the party if its rules allow this. It would be wrong, for instance, to use personal information which the candidate might have in their capacity as the local membership secretary, unless the party itself had sanctioned this.

- Candidates for election should be aware that political campaigning falls within the definition of direct marketing. Consequently, they should have regard to the requirements of the DPA (in particular section 11) and the Privacy and Electronic Communication (EC Directive) Regulations 2003 which set out specific rules that must be complied with for each type of marketing communication. For further information on this, the Information

Commissioner has produced Guidance on Political Campaigning which is available on our website.

Multi-member wards

7. In some types of local authority, councillors are elected under a multi-member system where more than one councillor represents a particular ward.

8. As a result, there may be situations where a councillor who represents a resident may need to pass on that particular individual's personal information to another councillor in the same ward. The councillor will only be allowed to disclose to the other ward councillor the personal information that is necessary:

   - to address the resident's concerns;
   - where the particular issue raises a matter which concerns other elected members in the same ward; or
   - where the resident has been made aware that this is going to take place and why it is necessary.

   If a resident objects to a use or disclosure of their information, their objection should normally be honoured.

9. The councillor should not pass on personal information which is not connected to the resident's case.

Example

A resident asks one of the councillors in a multi-member ward for help about teenagers acting in an intimidating way in the area. The councillor wishes to share the resident's complaint with the other ward councillors because it is an issue of general concern.

The councillor lets the resident know that he wants to give the details of their complaint to the other ward councillors and why he wants to do that, rather than giving a general description of the complaint to other ward councillors.

If the resident objects, then his wishes are respected and only the general nature of the complaint is shared.

Notification

10. In considering whether they need to register their processing with the Commissioner, councillors must first decide in which role they are processing personal information:

    - **As a member of the council**

    Councillors may have access to, and process, personal information in the same way as employees. In this case it is the council rather than the councillor that determines what personal information is used for and how it is processed. For example, if a member of a housing committee has access to tenancy files to consider whether the local authority should proceed with an eviction, the councillor is carrying out the local authority's functions and so does not need to register in their own right.

    - **As a representative of the residents of their ward**

    When councillors represent residents of their ward, they are likely to have to register in their own right. For example, if they use personal information to timetable surgery appointments or take forward complaints made by local residents.

    - **As a representative of a political party**

    When acting on behalf of a political party, for instance as an office holder, councillors are entitled to rely upon the registration made by the party.

    When individuals campaign on behalf of political parties to be the councillor for a particular ward, they can rely on the parties' registration if the party determines how and why the personal information is processed for the purpose of their individual campaigns.

    If a prospective councillor is not part of any political party but campaigning to be an independent councillor for a particular ward, they need to have their own registration.

11. There is an exemption from registration where the only personal information which is processed takes the form of paper records.

12. A standard form for registration by councillors has been created to simplify the procedure.

Offences

13. The DPA contains a number of criminal offences, including:

    - Failure to register when required to do so. For example, a councillor who holds computerised records of residents' details for casework purposes would commit an offence if they had not registered this use of personal information.

    - Making unauthorised disclosures of personal information. For example, a councillor who discloses personal information held by the council to their party for electioneering purposes without the council's consent could commit an offence.

    - Procuring unauthorised disclosures of personal information. For example, a councillor who obtains a copy of personal information apparently for council purposes, but in reality for their own personal use (or the use of their party), is likely to have committed an offence.

Security

14. Councillors should be aware that they need to arrange for appropriate security to protect personal information. They must take into account the nature of the information and the harm that can result. They should consider what technical and organisational measures, such as use of passwords, computer access privileges, procedures and staff training, are appropriate to keep the information safe. Councils should also take appropriate measures in the same way.

More information

15. Additional guidance is available on our guidance pages if you need further information on other parts of the DPA.

16. If you need any more information about this or any other aspect of data protection, please contact us, or visit our website at www.ico.org.uk.