DECISION

RIBBLE VALLEY BOROUGH COUNCIL
REPORT TO POLICY AND FINANCE COMMITTEE

Agenda Item No 11

meeting date: 19 JUNE 2018
title: GDPR IMPLEMENTATION PROGRESS REPORT AND DATA PROTECTION POLICY
submitted by: DIRECTOR OF RESOURCES
principal author: LAWSON ODDIE

1 PURPOSE

1.1 To provide members with details of the progress being made in the implementation of the requirements under GDPR and also to seek the associated approval of the council's new Data Protection Policy.

1.2 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2.1 The Data Protection Act 1998 (DPA) has now been superseded by the EU General Data Protection Regulation (GDPR), which introduces tougher fines for non-compliance and breaches, and gives people more say over what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.

2.2 A report was brought to the last meeting of this committee and covered

- Requirements and Rights under GDPR
- Role of the Data Protection Officer under GDPR
- Implications for Members

2.3 GDPR has also been reported to the Accounts and Audit Committee for discussion and consideration around governance issues.

3 PROGRESS ON IMPLEMENTATION OF GDPR REQUIREMENTS

3.1 There is a large amount of detailed work that has been undertaken across the council and its services in preparation for the application of GDPR from 25 May 2018. Whilst a large number of requirements have been fulfilled, there are a number of detailed actions that have yet to be completed, however good progress has been made.

3.2 It must be highlighted that once the actions being monitored below are completed, there is much ongoing monitoring and training work that will continue to take place.

3.3 Detailed across the following paragraphs is a summary of the progress that has been made at the time of writing this report.

Awareness

3.4 We are required to make sure that decision makers and key people in the organisation are aware that the law has changed to the GDPR. We also need to ensure that they appreciate the impact that GDPR is likely to have.

3.5 To date there have been regular updates provided to the Corporate Management Team on progress and any issues that have needed to be considered from a corporate perspective. There has also been an update provided to all Heads of Service at one of their meetings, in addition to one to one meetings having been held with them.

3.6 We will continue to promote GDPR through the staff newsletter and also formal training to all staff and members. Any future awareness training will need to be ongoing and refreshed annually.

3.7 There will also be ongoing general updates provided to management team and members regarding GDPR, data protection and any governance issues.

Information the Council Holds

3.8 We are required to document what personal data is held, where it came from, and who it is shared with. To do this the ICO highlight that there may be the need to undertake an information audit.

3.9 As part of this work, all Heads of Service have been met with to discuss their service's use of any personal data, how that data is stored and who such data may be shared with. The collation of all this information has led to the creation of an Information Asset Register, reflecting the findings from the meetings that have been held.

3.10 Work is ongoing to finalise and review the Information Asset Register.

Communicating Privacy Information

3.11 We are required to review the current privacy notices that we have and make any necessary changes to them in line with the GDPR.

3.12 An overarching privacy notice has been created for the council and this has been published on our website.

3.13 Individual service area privacy notices have also been created for Council Tax, Business Rates, Housing Benefits, Electoral Services and Recruitment which are all published on the council's website.

3.14 A further review will need to be undertaken of any electronic and manual forms to ensure users are correctly signposted to the relevant privacy notices.

Individuals' Rights

3.15 We are required to check our procedures to ensure that they cover all the rights that individuals have, including how personal data will be deleted, or provided electronically in a commonly used format.

3.16 We are in the process of producing procedures to follow in order to action any requests to restrict or stop the processing of a data subject's information.

3.17 We continue to consult with our many software vendors to ensure that systems are capable of performing the required functions to action the data subject's rights.

Subject Access Requests

3.18 We are required to update our subject access procedure and document our processes for being able to handle such requests within the new timescale of 30 days.

3.19 We have taken steps to ensure that all subject access requests are passed directly to the Data Protection Officer. We look to handle any subject access requests in the same manner as currently in place, but with acceleration in processing time to ensure that they are dealt with within the new timescales.

3.20 By ensuring that requests are passported directly to the Data Protection Officer we are comfortable in the ability to meet the 30 days turnaround of any requests received.

3.21 A formal policy is in the process of being produced to allow staff and members to recognise and process a subject access request.

Legal basis for Processing

3.22 We are required to look at the various types of data processing that we carry out, identify the legal basis for carrying it out, and then document it.

3.23 We have reviewed the Information Asset Register that has been created, as detailed above, in order to identify the legal basis for our processing of such data. The majority of these are 'public task' with a handful of 'legitimate interest', 'consent' or 'contract' and have been classified as such on the Information Asset Register.

- *Public task* refers to where we are carrying out a specific task in the public interest which is laid down in law, or exercising our official authority (functions, duties or powers) which are laid down by law.
- *Legitimate interest* can be our own interest or the interests of third parties and commercial interests as well as wider societal benefits. GDPR specifically mentions the use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list.
- *Consent* is where an indication of consent has been given, which must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct consent options for distinct processing operations. Consent should also be separate from other terms and conditions and should not generally be a precondition of signing up to a service.
- *Contract* is where processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.

Consent

3.24 We are required to review how we are seeking, obtaining and recording consent, and whether we need to make any changes.

3.25 The above section on legal basis for processing gives a flavour of the requirements under consent.

3.26 Again we have been reviewing our Information Asset Register and identifying those areas flagged as consent. Work here has largely focused on any mailing lists that we hold and ensuring that consent is acquired in line with the GDPR.

Children

3.27 We are required to identify potential areas that children may sign up to and put in place procedures to gather parental or guardian consent.

3.28 We don't believe that this area of GDPR impacts on our services. However, we will seek confirmation that any sign up to services are made through parental or guardian consent.

3.29 Some further investigation work is required in order to clarify that we don't offer any services directly to children without parental or guardian consent.

Data Breaches

3.30 We are required to make sure that the right procedures are in place to detect, report, and investigate a personal data breach.

3.31 We are in the process of developing a notification procedure to ensure that we can investigate and report to the ICO in a timely manner and most importantly within the statutory deadlines.

3.32 Data breach identification, notification and remediation training is to be provided to staff and members.

Data Protection by Design/Data Protection Impact Assessments

3.33 We are required to improve awareness and familiarity with the ICO guidance on Privacy Impact Assessments and work out how to implement.

3.34 As part of this work we will be highlighting to Heads of Service the importance of including the Data Protection Officer from the outset to ensure that data protection principles are integral to system design and processes put in place. This will include the undertaking of full privacy impact assessments.

3.35 Further training has yet to be undertaken in this area; however, there are no imminent new systems or fundamental changes anticipated.

3.36 A review is to be undertaken of all contracts where personal data may be shared with or processed by the contractor.

3.37 We are to review security policies, procedures and information governance arrangements to ensure that they reflect business objectives and to support good information risk management.

Data Protection Officer

3.38 We are required to designate a Data Protection Officer, or someone to take responsibility for data protection compliance and assess where this role will sit within the organisation's structure and governance arrangements.

3.39 At your last meeting we highlighted a potential conflict of interest in that our ICT Manager acts as our Data Protection Officer role. There have been general concerns raised by the ICO to all organisations where key ICT staff act in the role of Data Protection Officer and are involved in the decision of how and where data is stored.

3.40 Following consideration by Corporate Management Team such risks have been fully considered and it has been agreed that the Data Protection Officer role will remain with the ICT Manager, particularly as a result of the skills set that were identified as being needed for such a role. This also echoes a number of comments made at the meeting of Accounts and Audit Committee, where governance and GDPR has also been discussed.

International

3.41 The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

3.42 The council does not process or store personal data outside the European Union. Should the need arise for the council to process or store personal data outside the European Union in the future, we would ensure that all necessary safeguards are in place.

4 DATA PROTECTION POLICY

4.1 As part of our compliance work with the GDPR, we have undertaken a full review of our Data Protection Policy.

4.2 This has been substantially changed from our existing policy and therefore does not contain any 'tracked changes', essentially having been re-written.

4.3 This report also seeks committee approval of the policy which is attached at Annex 1.

5 CONCLUSION

5.1 We must now meet the new GDPR requirements.

5.2 Some work is continuing on some elements of compliance, and there will be ongoing work needed around training, involvement in system implementations and relevant monitoring work.

5.3 As part of the compliance work that has been undertaken to date, the Data Protection Policy has been re-written and is attached at Annex 1 for consideration and approval by members.

6 RECOMMENDED THAT COMMITTEE

6.1 Consider and approve the new Data Protection Policy as attached at Annex 1.

HEAD OF FINANCIAL SERVICES DIRECTOR OF RESOURCES
PF35-18/LO/AC

ANNEX 1

RIBBLE VALLEY BOROUGH COUNCIL

Ribble Valley
Borough Council
www.ribblevalley.gov.uk

Data Protection Policy

June 2018

Document Review Record

Version	Date Reviewed	Reviewed By	Details of any Changes Made
1	23 May 2018	Stuart Haworth	Draft new policy
2			

Contents

The Policy

Ribble Valley Borough Council is committed to a policy of protecting the rights and privacy of the individuals we provide services to and individuals we have contact with, in accordance with current Data Protection legislation.

The General Data Protection Regulation (GDPR) environment demands higher transparency and accountability in how organisations manage and use personal data. It also gives new and stronger rights for individuals to understand and control their personal information.

In order to provide services to the residents of the Ribble Valley and to perform its statutory duties Ribble Valley Borough Council needs to collect and process personal information for various purposes such as, but not limited to:

- The administration and collection of Council Tax and National Non Domestic Rates
- The assessment, administration and payment of Housing Benefit and Council Tax Support
- The collection of refuse
- The administration of the Electoral Register and management of Elections
- The recruitment and payment of staff
- The processing and determination of planning applications
- Supporting community events and groups

To comply with current Data Protection legislation and other legal obligations Ribble Valley Borough Council must ensure that all personal information is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

This policy applies to all staff. Any breach of this policy or any current Data Protection legislation will be considered an offence and the Council's disciplinary procedures will be invoked.

Contractors, agencies and individuals working with Ribble Valley Borough Council and who have access to personal information, will be expected to read and comply with this policy. It is the responsibility of each service area when engaging with external bodies that a signed contract is in place which includes an agreement to abide by this policy.

This policy applies to all situations where the Council processes (collects, stores, uses) personal data about living individuals. It includes personal information stored in various formats including but not limited to:

- Electronically
- On paper
- CCTV
- Photographs
- Audio

We will regularly review and update this policy to comply with changes in Data Protection legislation and to reflect changes in our services.

Personal Data

"Personal Data" is data about a living individual who can be identified from that information or from that information and other information in the possession of the Council.

"Sensitive Personal Data" is information relating to the racial or ethnic origin of an individual, his or her political opinions, religious beliefs, trade union membership, sexual life, physical or mental health or condition, or criminal offences or record.

GDPR

The new EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 (including the UK regardless of its decision to leave the EU) and impacts every organisation which holds or processes personal data. It introduces new responsibilities, including the need to demonstrate compliance, more stringent enforcement and substantially increased penalties than the Data Protection Act (DPA) which it supersedes.

Ribble Valley Borough Council's Responsibilities

Under current Data Protection legislation (including GDPR) Ribble Valley Borough Council is classed as a 'data controller' – this means that the Council is responsible for controlling the use and processing of the personal data that it collects. As a data controller the Council must register it's data processing activities with the Information Commissioners Office (ICO), we have the following registrations:

- Ribble Valley Borough Council – registration number Z6400958
- Electoral Registration Officer Ribble Valley Borough Council – registration number Z5797531

The Council is required to appoint a Data Protection Officer (DPO). The DPO has the following responsibilities:

- To educate the organisation and employees on data protection compliance legislation
- To train staff on how to process data securely
- Conduct spot-checks and audits to ensure compliance with data protection legislation
- Address non-compliance, or potential security breaches
- Act as the primary contact between the Council and Information Commissioners Office (ICO)
- Keep detailed records of all data

Corporate Management Team and Heads of Service, with the help of the Data Protection Officer, are responsible for developing and encouraging robust information handling practices that comply with the eight key data protection principles.

Compliance with data protection legislation is the responsibility of all members of staff and Elected Members who come into contact with personal information.

Data Protection Principles

Data protection legislation places responsibility on every controller to process all personal data in accordance with the following eight data protection principles:

1. **Process personal data fairly and lawfully**
   Ribble Valley Borough Council will make all reasonable efforts to
   a. collect and process personal data for legitimate purposes
   b. not use personal data in ways that would have an unjustified adverse effect on the data subject
   c. be transparent about the intended use of the data collected
   d. handle personal data in ways that the data subject would reasonably expect
   e. ensure that the data is not used in any unlawful ways
2. **Process the personal data for the specific and lawful purpose for which it was collected**
   Ribble Valley Borough Council will ensure that personal data is processed only for the purpose that it was collected or a purpose that is compatible with the original purpose.
3. **Ensure that the information is adequate, relevant and not excessive for the purpose for which it was collected**
   Ribble Valley Borough Council will only collect personal data that is necessary for the purpose for which it is processed. Any irrelevant data supplied by an individual will be securely destroyed.
4. **Keep personal information accurate and up to date**.
   Ribble Valley Borough Council will make every effort to ensure that information collected is kept accurate and up to date. Any notifications received from the data subject of a change or inaccuracy with the data held will be rectified in a timely fashion.
5. **Ensure that personal information is kept no longer than is necessary for the purpose for which it was collected**.
   Ribble Valley Borough Council will not keep personal data for longer than is necessary of the purpose for which it was collected. The retention period is either dictated by law or by the Council's retention policies. Once personal data is no longer required it will be destroyed securely and confidentially.
6. **Personal data is processed in accordance with the rights of the data subject under data protection legislation**
   Data subjects have various rights under Data Protection legislation including:
   a. The right to be informed how their personal data is processed and who it may be shared with
   b. The right to access the personal information we hold about them
   c. The right to have their personal information rectified if inaccurate or incomplete
   d. The right to have their personal information erased under certain circumstances
   e. The right to restrict the processing of their personal information under certain circumstances

f. The right to request their personal data in a structured, commonly used, machine readable format

g. The right to object to the processing of their personal data

h. The right not to be subject to a decision where it is solely based on automated processing

Ribble Valley Borough Council will only process personal information in accordance with the data subject's rights

7. **Ensure technical and organisational measures are in place to prevent**
    a. **Unauthorised or unlawful processing of personal data**
    b. **Accidental loss, destruction or damage to personal data**

    All members of staff are responsible for ensuring that any personal data that they hold or process is kept securely and is not disclosed to any authorised third parties.

    Ribble Valley Borough Council will have in place security measures to ensure that personal data is only accessible to those who have a valid reason to access it and to safeguard the data from accidental destruction, theft or loss. Where there is a requirement to take personal data off-site, appropriate procedures and controls will be adopted to ensure the safety of that data.

8. **Ensure that no personal data is transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**.
    Ribble Valley Borough Council will not transfer data to such countries or territories.

Subject Access Request (SAR)

An individual has the right to request a copy of the personal information we hold about them.

Under current Data Protection legislation a fee cannot be charged to comply with the request unless the request is 'manifestly unfounded or excessive' and the Council as the data controller must respond within 30 days to the request.

Disclosure of Data.

Ribble Valley Borough Council must ensure that personal data is not disclosed to unauthorised third parties. All staff and Elected Members should exercise caution when asked to disclose personal data held by the Council to a third party.

Personal data may be legitimately disclosed where one of the following conditions apply:

- The data subject has given their consent for the sharing of the data with the third party
- The Council is legally obliged to disclose the data
- Current data protection legislation permits the disclosure

Data Security

The Council will process personal data in accordance with its Information Security Policy (and other related policies and procedures). To ensure the security of personal data, Ribble Valley Borough Council has in place appropriate physical, technical, procedural and organisational measures in place. All Council employees and Elected Members are required to comply with this policy and the associated Information Security Policy.

Training

Data protection training is crucial so that all staff understand their responsibilities in relation to data protection. Failure to comply with Data Protection legislation could lead to fines being imposed on the Council or the Council being instructed to stop processing personal information.

It is the Council's policy that all employees who come into contact with personal data are required to complete the applicable training yearly. Heads of Service will be responsible for ensuring that their staff attend and complete the training.

There may be a requirement for some post holders to undertake further data protection training where appropriate dependant on their role within the organisation.

Our Commitment to Data Protection

The Council will ensure that staff who handle personal information will be trained to an appropriate level in the use and control of personal data.

The Council will implement a process to ensure all staff handling personal information know when and how to report any actual or suspected data breach(es), and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner.

The Council will monitor and review its processing activities to ensure these are consistent with current Data Protection legislation.

The Council will ensure that new or altered data processing will be assessed for its impact on the privacy of the data subject and the appropriate privacy notices are updated to reflect the change.

Changes to this policy

This policy will be regularly reviewed and updated to reflect changes in Data Protection legislation and changes in our services and procedures.