RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

OVERVIEW & SCRUTINY COMMITTEE

8th APRIL 2019

UPDATE REPORT ON THE COUNCIL'S INFORMATION MANAGEMENT ARRANGEMENTS

REPORT OF: DIRECTOR OF FINANCE AND DIGITAL SERVICES

Author(s): Louise Evans, Data Protection & Improvement Officer

1. PURPOSE OF THE REPORT

1.1 The purpose of this report is to provide the Committee with an update on the Councils Information Management arrangements.

2. RECOMMENDATIONS

2.1 It is recommended that the Committee:

i. Acknowledge the change to the Councils information governance structure in relation to the role of Senior Information Risk Owner (SIRO).

ii. Acknowledge the changes to the legal framework that governs the use of personal data and the associated risks with non-compliance.

iii. Form a view on the adequacy of the Councils Information Management arrangements and that the fundamental requirements of the General Data Protection Regulation have been met.

3. BACKGROUND

3.1 Overview & Scrutiny Committee on the 14th November 2017 received a report that provided an overview of the Information Management function and governance arrangements within the Council. Members were satisfied with the adequacy of arrangements reported and agreed to receive further updates in relation to Information Management.

3.2 The report specifically dealt with the following key points:

- Definition of Information Management
- Legal Drivers
- Enforcement Action
- Information Governance Structure/Arrangement
  - Senior Information Risk Owner (SIRO)
  - Information Asset Owners
  - Information Management Board
  - Information Management Working Group
- Information Management Priorities
- Information Management Arrangements (security incidents / events, subject access requests)
- Wales Audit Office Review.

4. INFORMATION MANAGEMENT - UPDATE ON CHANGES, WORK & PROGRESS

4.1 This report provides an update on any changes, work and progress around the Councils Information Management arrangements for the period 1st April 2018 – 31st March 2019.

5. INFORMATION GOVERNANCE STRUCTURE

5.1 The Council's information governance structure remains unchanged with the exception of the role of SIRO that was designated to the Director of Finance & Digital in March 2019.

5.2 An illustration of the Councils information governance structure is provided in Appendix I.

6. LEGAL DRIVERS

6.1 The effective management of information places significant demands on the Council. In particular, there is a wide ranging, dynamic and complex legal landscape in which the Council has to operate within. 2018/19 saw the biggest change in data protection laws in over 20 years with the introduction of the new EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18).

6.2 The GDPR replaced the EU's 1995 Data Protection Directive and all Member State law based on it, including the UK's Data Protection Act 1998 (DPA98).

6.3 The DPA18 modifies the EU GDPR by filling in sections of the Regulation that were left to individual Member States to interpret an implement.

6.4 The GDPR's key information handling principles are similar to that of the DPA98 but with added detail and enhanced mandatory requirements. It places greater obligations on how organisations handle personal information and introduces a new accountability principle that requires organisations to demonstrate and evidence compliance with the regulations.
The GDPR is fully retrospective, in that it applies to information collected prior to the Regulation coming into force.

7. ENFORCEMENT ACTION

7.1 Failure to manage personal data appropriately can lead to reputational loss and considerable financial penalties. In particular, the Information Commissioner's Office (ICO), who oversees and enforces the GDPR in the UK, has a wide range of enforcement powers to change the behaviour of organisations who are found to breach the GDPR. These enforcement powers, in particular in relation to monetary penalty notices are significantly higher than that under the previous regime (DPA98).

7.2 GDPR enforcement powers include but are not limited to:

- **Monetary penalty notices:**
  - Tier 1: Administration / organisational non-compliance (e.g. failing to keep records of processing activities, appoint a Data Protection Officer, register with the ICO etc.). Up to €10M or 2% organisations global turnover.
  - Tier 2: Infringements (e.g. breaches of the data protection principles such as data loss, inappropriate disclosure etc.). Up to €20M or 4% organisations global turnover
- **Serve enforcement notices** (and 'stop now' orders) - where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law.
- **Serve assessment notices** to conduct compulsory audits to assess whether organisations processing of personal data follows good practice.

7.3 The GDPR also gives individuals the right to compensation for material and/or non-material damage resulting from an infringement.

8. KEY CHANGES / REQUIREMENTS OF THE GDPR

8.1 The following outlines a number of key changes / requirements of the GDPR. Failure to comply with these requirements can potentially result in enforcement action as outlined in 7.2 above (Tier 1 fine for administration/organisational non-compliance).

8.2 Records of processing activities (Data Protection Register)

The GDPR contains explicit provisions requiring organisations to document their data processing activities. Organisations must maintain records on several things including the purpose for which the information is being processed, the lawful basis for processing, description of the categories of individuals whose information is being processed and a description of the categories of personal data etc.

Records must be kept up to date and reflect the organisations current processing activities. Records must also be made available to the ICO upon request.

8.3 Transparency / Right to be informed

The transparency requirements of the GDPR requires organisations to be open, honest and transparent with people about how their personal data will be used. The GDPR sets out what information should be provided to people when organisations process personal data, this includes the purpose for which the information is being processed, lawful basis, categories of personal data, source of the data, retention period for the data and existence of data subject rights etc.

8.4 **Contractual Obligations – Commissioned/Traded Services**

Where the Council uses a third party to process personal data on its behalf the GDPR requires a written contract that contains specific data protection clauses (regardless of the contract value).

Where the Council jointly processes personal data with another organisation the GDPR requires an arrangement.

These data protection clauses/arrangements are important so that both parties (Council and third party) understand their responsibilities and liabilities for personal data and to evidence and govern the working relationship. It helps the Council demonstrate compliance with the GDPR.

8.5 **Personal Data Breach**

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO). This must be done within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk to the rights and freedoms of individuals (who are the subject of the breach), the organisation must also inform those individuals without undue delay.

Organisations are required to have robust breach detection, investigation and internal reporting procedures in place to facilitate decision-making about whether or not it needs to report a breach to the ICO and notify the affected individuals.

Organisations must keep a record of any personal data breaches, regardless of whether the ICO and/or individuals are notified.

8.6 **Right of access / Subject Access Request (SAR)**

The GDPR gives rights to individuals to access their personal data (commonly referred to as subject access).

The Council must respond to all requests without undue delay and no later than one month from receipt (previously 40 calendar days).

The Council is no longer able to charge for the request (previously £10 under the DPA1998).

The Council could face enforcement action for failing to respond to SAR's within the statutory timeframe and/or failing to provide all of the information covered by the request (unless and appropriate exemption applies).

8.7 **Data Protection Officer**

The GDPR introduces a duty for all public authorities to appoint a Data Protection Officer (DPO).

The DPO's role is to assist an the organisation in monitoring internal compliance, provide information and advice on data protection obligations and act as a point of contact for data subjects and the supervisory authority.

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

9. PROGRESS MADE AGAINST THE KEY REQUIREMENTS OF THE GDPR

9.1 The following outlines the significant progress made by the Council in meeting the key requirements placed upon it by the GDPR, as per the actions specified in the GDPR Project Delivery Plan that was endorsed by Cabinet on the 22nd March 2018:

9.2 **Records of processing activities (Data Protection Register)**

During 2018/19 a Council-wide data mapping exercise was undertaken to identify and document what personal data was held and processed by the Council and how it was used (why, what, when, how etc.).

The detailed information gathered as part of the exercise formed the baseline of the Councils Data Protection Register that supports the Council in evidencing compliance with the accountability requirements of the GDPR. To date over 100 entries have been created within the Register covering approximately 90% of processing activity within the Council.

Work continues to further develop and enhance the register and to ensure that the information contained within it remains accurate and up-to-date and reflects the Council's current position. To support this, the service is implementing an information management system that will host the register enabling better reporting, monitoring and tracking of data and processing activities thus further supporting compliance with the accountability requirements of the GDPR.

9.3 **Transparency / Right to be informed**

The Council has adopted a layered approach to the provision of privacy information. This approach supports the Council is meeting the transparency requirements of the GDPR:

i. Corporate Privacy Notice (Layer 1)

The Corporate Privacy Notice consists of a series of webpages published on the Councils website under the data protection pages:

- **How we use your personal information** - introductory page about the way the Council uses your personal information and the ways in which we protect your privacy.

- **How we use your personal information (Frequently Asked Questions)** - answer to commonly asked questions about the Council's use of personal information.

- **Your information rights** - provides information on your information rights including your right to access the personal information the Council holds about you.

- **Concerns or complaints about the way the Council is handling your personal information** – in the event that an individual may be dissatisfied with how their personal information has/is being handled by the Council, this page provides information on how an individual may raise a concern or make a complaint (links to the Councils Complaints and Concerns Policy).

ii. Service Privacy Notice (Layer 2)

In support of the Corporate Privacy Notice, it is important that individuals are provided with detailed information about how their personal information is used when receiving specific services. These are referred to as 'Service Privacy Notices'**.**

To date over 90 service privacy notices been developed and published on the Councils website via the following link: Service Privacy Notice.

iii. Short Privacy Notice (Layer 3)

The short privacy notice is typically found for example on an application or data capture form and is the first piece of privacy information the individuals sees or is provided with. It should directly link or signpost to wider/more detailed privacy information such as the service and/or corporate privacy notice.

Significant work has been undertaken to review all applications, data capture forms and correspondence templates in use within the Council (paper and electronic), to ensure that a short privacy statement is included that links/signposts to the corporate and/or service specific notices. This work will continue during 2019/20 to maximise opportunities for promoting privacy information.

9.4 **Contractual Obligations – Commissioned/Traded Services**

GDPR complaint contracts/agreements have developed and approved by the Council's Data Protection Officer and Head of Legal in consultation with Procurement.

Over 1200 current/active contracts over the value of £15k have been identified (via the e-tender Wales Contract Register system) and reviewed by Procurement, relevant Service/Contract Managers and the Data Protection Officer to establish whether personal data is processed (as part of the contract). Where personal data is processed, contract

variations have been issued in relation to 860+ contracts. These are now considered GDPR complaint.

Reviewing contracts will continue to be a key priority / work-stream for the Council 2019/20, focussing specifically on contracts under the value of £15k.

9.5 **Personal Data Breach**

The Council has a robust and well established incident management process in place that has been reviewed, updated and approved by the IM Board to reflect the new requirements of the GDPR in relation to personal data breach notification:

- The procedure for reporting information security incidents and events requires all employees, elected Members, contractors and third party suppliers with access to council information, systems and assets (regardless of the format in which they are held), to report any potential, suspected or actual information security incident or event to the appropriate person and the ICT Service Desk as soon as becoming aware of a potential occurrence.

- The procedure for investigating information security incidents and events sets out the process for the management of a reported information security incident or event including breaches of personal data. The procedure aims to contain and recover of any compromised information, assess the harm or risk posed to individuals by the incident, notifying the affected individuals and/or relevant authorities where necessary and determining the mitigation needed to prevent further occurrence of similar incidents.

9.6 **Right of access / Subject Access Request (SAR)**

The Council's Data Protection policy sets out the Council's commitment to ensuring individuals can freely exercise their information rights, including the right of access. This commitment is also reflected in the Council's corporate privacy notice that includes a specific section on information rights and how they may be exercised.

The Council has robust and well established procedures for the handling of subject access requests. These procedures have been reviewed, updated and approved by the IM Board to reflect the new requirements of the GDPR in relation to verbal requests, time scale for response and removal of fee etc:

- The Subject Access Procedure (for all staff) sets out the Council's procedure for handling SAR's which every Council employee must follow. These procedures have been updated to reflect the new requirements of the GDPR as outlined above. The procedure ensures that all staff know how to recognise a subject access request and that any requests received are routed to the Information Management Team where they are centrally logged and monitored.

- The Subject Access Procedure for SAR Co-ordinators and Service Managers provides the procedure for handling subject access requests within the Council and offers practical advice about identifying all of the information covered by the request,

redaction and guidance on the limited circumstances in which personal data is exempt from subject access.

9.7 **Data Protection Officer**

The Data Protection & Improvement Officer was formally designated 'Data Protection Officer' for the Council by Cabinet on the 22nd March 2018.

10. EQUALITY AND DIVERSITY IMPLICATIONS

10.1 There are no equality and diversity implications as a result of the recommendations set out in the report

11. CONSULTATION

11.1 There are no consultation implications as a result of the recommendations set out in the report

12. FINANCIAL IMPLICATIONS

12.1 There are no adverse financial implications as a result of the recommendations set out in the report.

13. LEGAL IMPLICATIONS

13.1 The legal implications for non-compliance with the key requirements of the GDPR are set out within section 7 of this report.

14. LINKS TO THE CORPORATE AND NATIONAL PRIORITIES AND THE WELL-BEING OF FUTURE GENERATIONS ACT.

14.1 There are no links to corporate and national priorities and the Well-being of Future Generations Act.

LOCAL GOVERNMENT ACT 1972

AS AMENDED BY

THE LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985

RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

OVERVIEW & SCRUTINY COMMITTEE

8th April 2019

REPORT OF THE DIRECTOR OF FINANCE AND DIGITAL SERVICES

Author: Louise Evans, Data Protection & Improvement Officer

Item: **UPDATE REPORT ON THE COUNCIL'S INFORMATION MANAGEMENT ARRANGEMENTS**

Background Papers

General Data Protection Regulation 2018
Data Protection Act 2018
Overview and Scrutiny Committee – 14 November 2017

Other information:

Officer to contact: Louise Evans (Alison.l.evans2@rctcbc.gov.uk)

APPENDIX I

ILLUSTRATION: INFORMATION GOVERNANCE STRUCTURE