Appendix 3

# Assurance review of Information Governance

**Update From:** Paul Mountford, - Performance, Innovation and Commissioning Specialist

**1.0 Context**

1.1 The European General Data Protection Regulation (GDPR) came into effect on 25 May 2018 aiming to reform and standardise data protection arrangements across EU member states. On the same date the regulation was incorporated into UK law as the Data Protection Act 2018.

1.2 The Performance, Innovation and Commissioning Specialist is the Council's Data Protection Officer. The Data Protection Officer has special responsibilities under the regulation in that they should work independently, report to the highest management level and have adequate resources to enable the Council meet its GDPR obligations.

1.3 The Council complies with its obligation to appoint a Data Protection Officer under the terms of the regulation. The Data Protection Officer has direct access to the Chief Executive. The Data Protection Officer maintains the necessary statutory records and provides advice and guidance to the Council, for example, regarding the completion of Data Protection (Privacy) Impact Assessments and submits periodic progress reports to the Information Governance Board.

1.4 This update sets out, with specific reference to the audit review carried out in January and February 2019, the ongoing work to establish the GDPR framework across the Council.

1.5 The audit review found the Council to have adequate and effective governance, risk and control processes, leading to a Reasonable assurance.

**2.0 Audit Review - Action Points - IMPORTANT**

2.1 In achieving a reasonable assurance three important action points were identified. In brief these were identified as:

- The action plan be updated to include timescales, resources and ownership of tasks
- Development and publication of documentation regarding the joint processing arrangements, and
- The documentation and application of retention timescales to digital and non-digital records.

2.2 In order to ensure that it fulfilled its obligations, the Council initiated a GDPR compliance project which was then subsumed as a work stream within the Council's wider Customer Connect programme. A project plan was prepared and implemented. The issues raised in the assurance review indicate that, notwithstanding the substantial preparations made to date, further work is required, in particular regarding updates to the Record of Processing Activity, data sharing arrangements and drafting of procedural guidance in order to comply with the new data protection Accountability principle, which requires the production of detailed policy and procedural guidance in order to demonstrate compliance with the Regulation.

2.3 The Customer Connect Programme action plan has been updated to include timescales, resources and ownership of tasks. This provides an understanding of the resources required and timescales involved in order to complete work on the GDPR compliance framework.

2.4 The Council's Record of Processing Activity identifies 13 organisations which act as Joint Processors of information. In line with the assurance review joint processor agreements will be developed and implemented where joint processing activity with other organisations is in place. The Council's Record of Processing Activity will be amended in accordance with these arrangements. Corrections will be made to the Council's Record of Processing Activity where no such joint processing arrangements occur.

2.5 The Council has a data retention policy and schedule. In accordance with the assurance review the means by which document retention timescales are applied to digital and non-digital records will be documented. Local procedure notes held and implemented will be summarised in the Council's Record of Processing Activity.

**3.0 Audit Review - Action Points - ROUTINE**

3.1 In achieving a reasonable assurance nine routine action points were identified. In brief these were identified as:

- GDPR refresher training be undertaken and tailored to the requirements of new staff roles
- A procedure for periodic review of the Council's Record of Processing Activity (RoPA) developed and established
- Identify and list the specific information systems (e.g. Capita) and/or locations where personal data is held
- Update the current Council Data Protection and Data Breach policies
- Consolidate, refresh and republish the Data Protection SharePoint Site
- Update, amend and re-publish the Council's Corporate Privacy Notice
- A procedure for determining the three Legitimate Interest tests is developed and established
- A record of consent be maintained by the Data Protection Officer and periodically reviewed and confirmed that consent is still given, and
- An overarching Data Protection Impact Assessment framework be established.

3.2 GDPR awareness is included as part of the induction process for new staff and a mandatory e-Learning course, available from the Council's SharePoint site, must be completed by all staff. Given the significant business transformation currently being undertaken by the Council, GDPR refresher training will be tailored to the requirements of new staff roles once the restructure has taken effect.

3.3 The Council maintains an Information Asset Register and from this a detailed data map - Record of Processing Activity - has been compiled. In accordance with the audit review a procedure for the periodic review of the Record of Processing Activity will include an updated information data audit in consultation with Information Asset Owners identified in the Information Asset Register.

3.4 The Council's main information systems - Capita Revenues and Benefits and iTrent have been updated to include new GDPR compliance modules. In accordance with the audit review a full assessment will be undertaken to identify outstanding ICT compliance regarding the Council's information systems and records. Tasks

identified will be added to the overall Customer Connect Programme project plan with the timescales and resources required to complete any identified residual tasks.

3.5 The Council's Data Protection Policy has been updated to include details relating to data subject access rights, the lawful basis upon which data will be collected, data protection by default and design and the role of the Data Protection Officer. In addition the way in which the ICT incident management policy and the data breach policy interact, has been described in the respective policies.

3.6 There is a Council SharePoint site containing a comprehensive set of GDPR related policies, procedures and on-line training materials. In line with the audit review, draft copies and working papers will be removed. The site, once signed off, will be published on the Council's SharePoint Homepage.

3.7 The Council has published a set of privacy notices on its website and SharePoint site. The corporate Privacy notice has been amended making reference to the Council's data retention policy and schedule. The Privacy Notice for staff has been amended to record all of the data subject access rights.

3.8 The Council has determined the lawful bases upon which it collects and processes personal information and recorded this in the Council's Record of Processing Activity. Three instances where Legitimate Interest is the lawful basis for data collection have been identified in the Record of Processing Activity relating to appraisal, awards and honours. GDPR requires that legitimate interest be established by the application of three 'tests'. In accordance with the audit review a link to the location of the Assessment of Legitimate interests will be entered in to the Record of Processing Activity.

3.9 There is a Consent Protocol and form and the Council has designed its processes to ensure that the need to obtain consent is kept to a minimum. The Council's Record of Processing Activity identifies 8 instances where consent must be obtained from customers and/or staff in order for the Council to collect and process their personal data. In line with the audit review recommendation a record of Consent will be developed, drafted and published through the Data Protection SharePoint site. The protocol will include all arrangements for withdrawing consent.

3.10 The GDPR makes privacy by design a legal requirement and requires organisations to undertake a Data Protection (Privacy) Impact Assessment (DPIA) when changes are made to systems which may impact upon the security, collection and/or processing of data. The Council has documented a Data Protection Impact Assessment procedure and has conducted impact assessments relating to a number of projects. The process has been incorporated into the Business and Service Redesign programme under the Customer Connect Programme.

**4.0 Audit Review - Action Points - OPERATIONAL**

4.1 In achieving a reasonable assurance one operational action point was identified:

- Consideration be given as to whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

4.2 The Council's approach to data subject access requests is noted in the Data Protection Policy and data subject rights are outlined in the Council's advisory guidance note, Exercising Information Access Rights. There is a subject access request procedure. This utilises a multi-purpose form which can be used to fulfil any or all of the data subject access rights. Any Subject Access Requests received are detailed in a log to record receipt of and action taken with the requests. The Council in developing the 'Single Customer View' and Customer Accounts are developing procedures and processes to enable residents and customers to access the information held about them online.

## 5.0 High Level Action Plan

| Action | Tasks | Implementation Date | Status | Owner |
|---|---|---|---|---|
| The action plan be updated to include timescales, resources and ownership of tasks | | 03/05/19 | COMPLETE | Data Protection Officer |
| Development and publication of documentation regarding the joint processing arrangements | Include links to specific Data Sharing Agreements and GDPR compliance statements. RoPA to be updated to include arrangements for data sharing with processors and/or joint processors. RoPA updated to include security arrangements for data at rest. Update Data Sharing register to identify security arrangements for data in transit. | 27/09/19 | IN PROGRESS | Data Protection Officer |
| The documentation and application of retention timescales to digital and non-digital records | Records Retention Policy to include local procedure notes to evidence specific arrangements for disposal summarised with RoPA. | 27/09/19 | IN PROGRESS | Data Protection Officer |
| GDPR refresher training be undertaken and tailored to the requirements of new staff roles | Current e-learning package to be reviewed in light of new staff roles - notably Customer Contact and Case Management roles. Consult and seek recommendations from Corporate Learning & Development Team. Resources to be made available. | 20/12/19 | TO COMMENCE | Data Protection Officer |

| Action | Tasks | Implementation Date | Status | Owner |
|---|---|---|---|---|
| A procedure for periodic review of the Council's Record of Processing Activity (RoPA) developed and established | IAR Framework and protocol to be developed with identified Information Asset Owners listed in current IAR. | 27/09/19 | IN PROGRESS | Data Protection Officer |
| Identify and list the specific information systems (e.g. Capita) and/or locations where personal data is held | Working with Shared Infrastructure Manager in ICT update RoPA accordingly to identify GDPR compliant systems. Working with Shared Infrastructure Manager assess any outstanding ICT compliance work regarding information systems. Include any actions as part of overall project plan (see Rec 1) to include timescales and resource requirement. | 27/09/19 | IN PROGRESS | Data Protection Officer |
| Update the current Council Data Protection and Data Breach policies | Data Protection Policy to be updated. Include links to ICT Incident Management Policy and arrangements as part of data breach reporting protocol and procedures. | 03/05/19 | COMPLETE | Data Protection Officer |
| Update, amend and re-publish the Council's Corporate Privacy Notice | Corporate Privacy Notice to be amended to make reference to Council's Records Retention procedures. Staff Privacy Notice to be updates to include subject access rights. | 28/06/19 | COMPLETE | Data Protection Officer |

| Action | Tasks | Implementation Date | Status | Owner |
|---|---|---|---|---|
| A procedure for determining the three Legitimate Interest tests is developed and established | Legitimate Interest assessment documents to be added to Information Governance Framework and Data Protection SharePoint. RoPA to be updated with relevant links. | 27/09/19 | IN PROGRESS | Data Protection Officer |
| A record of consent be maintained by the Data Protection Officer and periodically reviewed and confirmed that consent is still given | Record (log) of Consent Protocol to be developed and added to Data Protection SharePoint – reference to document within overall Data Protection Policy. Record of Consent to include details of Consent 'Owners' with reference in IAR and RoPA. Consent procedures to clearly detail arrangements for withdrawal of consent. | 27/09/19 | IN PROGRESS | Data Protection Officer |
| An overarching Data Protection Impact Assessment framework be established | Data (Privacy) Protection Impact Assessment template is being used and completed in line with Service Redesign Programme. DPIA Framework to be established with specific references and links through RoPA and Data Protection SharePoint. | 27/09/19 | IN PROGRESS | Data Protection Officer |

## Background Documents Available

| Name of Background document | Where it is available |
|---|---|
| General Data Protection Regulation - 06/12/2017 | Audit Committee - Minute AUD/37 |
| General Data Protection Regulation - 05/12/2018 | Audit Committee - Minute AUD/31 |
| Internal Audit Progress Report 2018/19 - 09/04/2019 | Audit Committee - Minute AUD/55 |