PERTH AND KINROSS COUNCIL

Scrutiny Committee

9 September 2020

Data Protection Compliance 2019-20

Report by Data Protection Officer (Report No. 20/158)

PURPOSE OF REPORT

This report is the professional assessment of the Council's compliance with the General Data Protection Regulation (GDPR) by the Data Protection Officer (as is required to be provided by him in accordance with the legislation). This report relates to the year 2019-20.

1. BACKGROUND

1.1 The GDPR requires a public authority such as the Council to appoint a Data Protection Officer (DPO) and defines tasks that the person must undertake. These tasks include monitoring and reporting on compliance with the GDPR.

1.2 The Council's Data Protection Policy sets out that the DPO will present a report on the Council's data protection compliance to the Council's Senior Management and the Scrutiny Committee annually or more frequently if considered necessary.

1.3 It should be noted that responsibility for compliance with data protection legislation lies with the Council rather than the DPO.

2. EXECUTIVE SUMMARY

2.1 Given the breadth of the Council's activities and the huge number of interactions and transactions involving personal information entailed in the delivery of its services, it is unlikely that Council will ever be able to state categorically that it is fully compliant with data protection legislation. The DPO is confident, however, that the current level of compliance is reasonable and continues to gradually improve.

2.2 The DPO is satisfied that the principal pillars of GDPR compliance are all in place and are generally becoming accepted as normal practice across the Council. Where procedural failings have occurred regarding data protection, these can reasonably be attributed to a lack of training / awareness and general workload pressures.

2.3 Whilst the Council would wish to avoid any data breach, the total number of breaches recorded in the year is very small given the volume and wide range of personal data that is processed across the Council in the course of a year.

2.4 The DPO has highlighted issues arising from a lack of adequate resources, supplier intransigence, and changes to international transfers of personal data.

3. COMPLIANCE

3.1 Policy

3.1.1 The Council has a Data Protection Policy which satisfies the separate requirements of the GDPR and the Data Protection Act 2018.

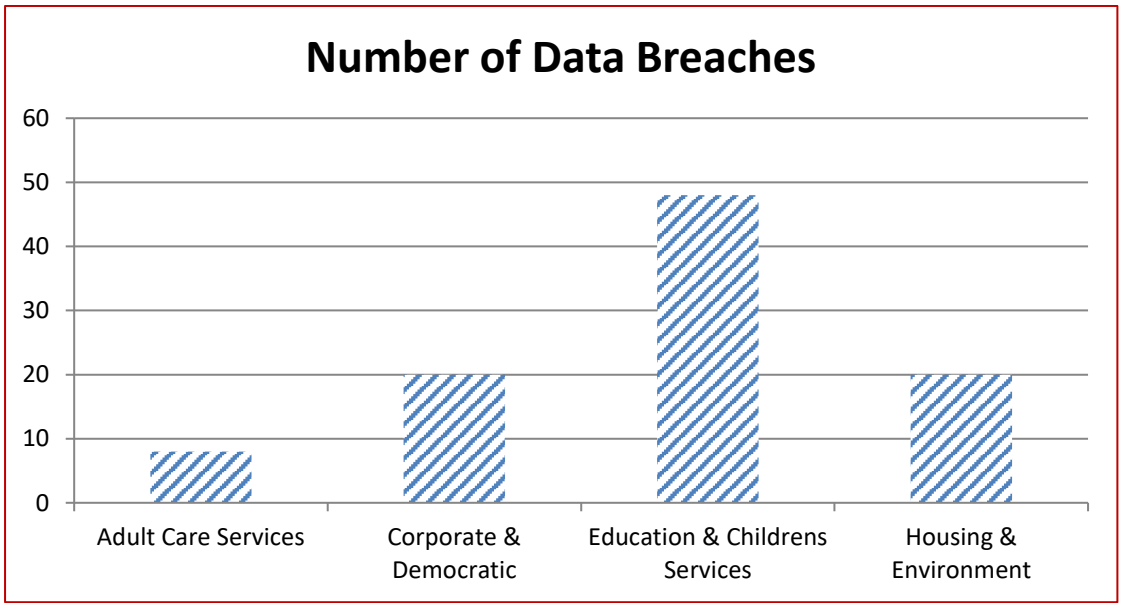
3.2 Data Breaches

3.2.1 A data breach is defined as an incident involving "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

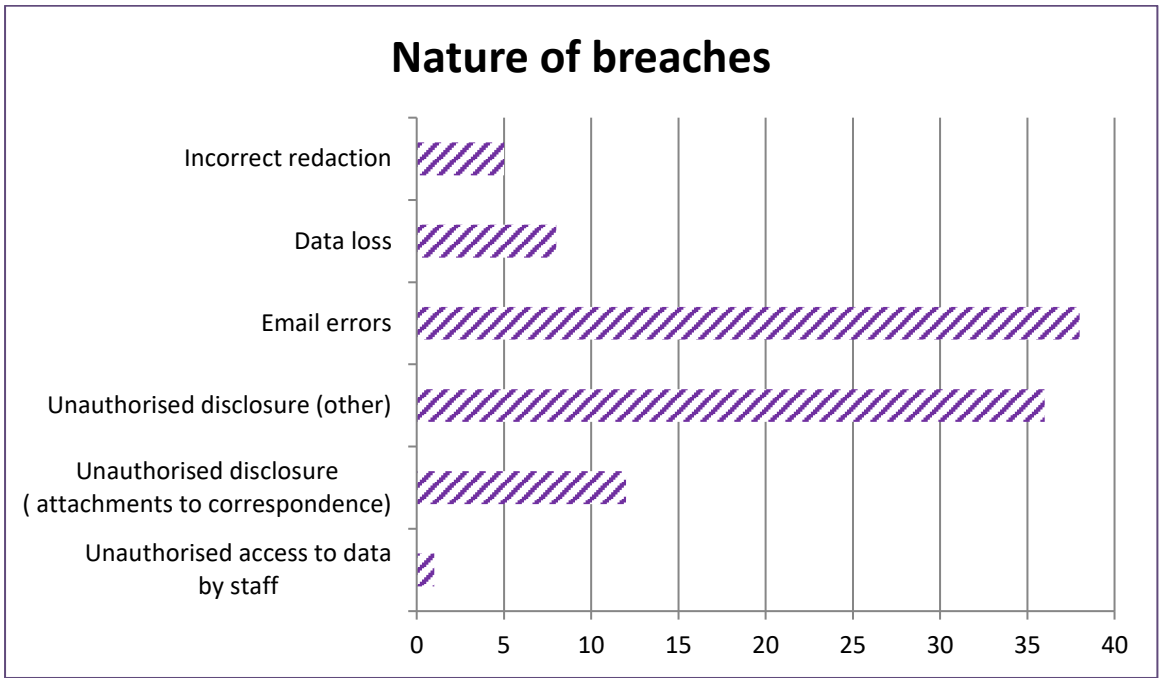
3.2.2 The Council is required to maintain a register of data breaches and, where appropriate, report them to the Information Commissioner's office.

3.2.3 Between 1 April 2019 and 31 March 2020, the Council recorded a total of 96 data breaches (compared to 89 during the previous year).

3.2.4 The split of data breaches by Service is illustrated below: -



3.2.5 The nature of the data breaches was as follows: -



3.2.6 Almost all of the breaches were reported promptly to the DPO. In a some cases, however, there were delays in providing the DPO with additional information or taking remedial action as quickly as requested by the DPO.

3.2.7 The DPO is satisfied that, in the main, where breaches have been identified, that the relevant area has been keen to engage with the DPO to amend and improve practice.

3.2.8 Of the 96 breaches, the DPO considered four of those required to be reported to the Commissioner's Office (ICO).

3.2.9 For three of the breaches reported, the ICO considered that the actions taken by the Council in response to the breaches were appropriate and did not require any further action. For the other breach, the ICO required a procedural change and the dissemination of information about the change to the relevant employees.

3.2.10 It would appear that employees across the organisation understand breaches caused by unauthorised disclosure and the DPO is confident that all significant data breaches of this type were reported during the year. The DPO is aware, however, that the other types of data breach are less well understood and will continue to provide advice and guidance about breaches and breach reporting.

3.3 **Data Subject Requests**

3.3.1 The GDPR gives data subjects a number of specific rights. Requests to exercise these rights have to be responded to within 1 month (interpreted by the Council as 28 calendar days). The DPO has responsibility for dealing with requests to exercise data subject rights received by the Council.

3.3.2 Between 1 April 2019 and 31 March 2020, the Council received 136 requests for access to personal information, of which:-

- 6 are still in progress
- 26 are on hold awaiting further information from the requester (normally proof of identity)
- 104 have been completed

3.3.3 Of the 104 requests that were processed

- 69 were completed within the statutory timescale (66%).
- 35 were late (Many of these requests were complex and involved the processing of a very large volume of information).

3.3.4 The Council received 7 other requests: -

- 1 request for erasure
- 2 requests regarding processing
- 1 request regarding access to information
- 2 requests for rectification
- 1 request to cease processing

3.3.5 The Council also received 19 complaints, either directly from the data subjects or via the ICO, about the way personal data had been handled. All of the complaints were dealt with appropriately and timeously.

3.3.6 The DPO is satisfied that data subject requests are being handled appropriately within the resources available.

3.4 **Training**

3.4.1 The DPO team has not delivered any planned LIG sessions this year, partly due to reduced demand and partly to workload. Face-to-face training has been provided when requested.

3.4.2 During the year, a number of data protection related Inside News Bulletins have been published as well as several ‘Spotlight’ slots on the Council intranet. These have been used to highlight particular issues or the availability of new guidance.

3.4.3 The DPO considers that there appears to be a good level of general awareness across the Council.

3.4.4 The DPO team planned to re-write the data protection e-Learning modules during the year, but this has not proved possible, largely due to the lack of available resources within the team.

3.4.5 The DPO considers that the lack of revised and up-to-date training material could be considered a significant weakness by the Information Commissioner's Office in the event of a reportable data breach.

3.5 **Documentation**

3.5.1 There is a statutory requirement for the Council to be able to provide evidence of its compliance with the legislation at all times. This is achieved through a number of key pieces of documentation: -

- Data Protection Impact Assessments (DPIAs)
- Details of Processing Arrangements
- Privacy Notices
- Data Sharing Agreements (DSAs)

3.5.2 Responsibility for the creation of the first three all lie with the Council; the DPO has responsibility to assist and advise in their creation and to maintain registers of the documentation.

3.5.3 During the year, the DPO team identified that Services were finding the DPIA process daunting, so revised its presentation and introduced a simpler pre-DPIA checklist to allow the identification of projects that would require a full DPIA prior to the project going live. The DPO team is aware of a backlog of incomplete DPIAs and intends to progress this as a priority during 2020-21.

3.5.4 The DPO team had intended to review the Register of Processing Activities during the year, but this has not been possible due to resource availability.

3.5.5 In general, short privacy notices appear correctly wherever personal data is collected (i.e. electronic and physical forms). It is known that the matching detailed privacy notice does not exist in many cases. The DPO team had intended to try and address this situation during the year, but this has not been possible due to resource availability both within the DPO team and within Services which are required to provide us with details of processes undertaken.

3.5.6 The DPO team continue to work on Data Sharing Agreements as and when the requirement is identified. These are specialised documents and tend to be lengthy and time-consuming pieces of work, often needing extensive consultation with the other organisations involved.

3.6 **Data Protection Officer**

3.6.1 The role of the DPO is defined in the GDPR and the legislation places particular restrictions on both the DPO and the Council in terms of roles and responsibilities. The DPO, like the other Statutory Officers within the Council, has an independent and autonomous role and the Council cannot instruct the DPO how to undertake the role.

3.6.2 During the course of the year, the understanding of this new statutory and strategic role has been gradually developed across the organisation.

3.6.3 All formal advice provided by the DPO to the Council has been accepted to date.

3.7 **DPO Resources**

3.7.1 The legislation provides that adequate resources should be made available to the DPO to enable him to fulfil his role.

3.7.2 The Data Protection Officer's team comprises 2.5 FTEs

- the Information Governance Manager, who is the DPO
- the Senior Information Governance Officer
- 0.5 FTE Information Governance Officer

Both officers can deputise for the DPO. The team is also assisted by one of the Council's solicitors.

3.7.3 The members of the DPO team are all part of the Information Governance Section and have significant other responsibilities in addition to data protection - freedom of information, information security, information and records management, and corporate complaints handling.

3.7.4 As with many other teams across the organisation, resources are an issue as reflected in the outstanding activities identified above. Much of the business is responsive, with statutory timescales and constraints attached, which often means that in terms of managing the associated risks, development activities are sacrificed.

3.7.5 The DPO considers that whilst directing resources to "urgent" work is an adequate short-term strategy, an inability to delivery training, or review practice and policy may create the potential for greater risk to the organisation in the longer term.

3.7.6 In the report for 2018-19, the DPO advised that the demands of the function could not be met within current resources but was mindful of the financial climate in which the organisation was operating. That being acknowledged, the DPO flagged the lack of resources to the Council as a risk.

3.7.7 The DPO considers that this situation has not changed and the lack of adequate resources for the DPO function remains a risk to the Council.

3.7.8 The DPO considers that the function is being exercised appropriately and as effectively as it can be in the Council within the resources available.

3.8 **Compliance Monitoring**

3.8.1 This report has been based on the information currently available to the DPO team and cannot be considered a comprehensive assessment of the Council's compliance with data protection legislation during the year.

3.8.2 It had been intended that the DPO would work with Senior Management, and the Head of Legal & Governance Services in particular, as part of the Council's wider review of the governance framework to develop a more systematic approach to obtaining assurance as regards compliance across the organisation. This has not proved possible during the year for a number of reasons, but remains an intention for 2020-21.

4. ISSUES

4.1 The DPO is aware of issues with a small number of both live and planned projects where the processing of personal data is likely to be considered unlawful without changes being made. In all these cases, the Council is dependent on suppliers acceding to the Council's wishes, but the suppliers are proving reluctant to make the necessary changes. The DPO has highlighted these issues to the relevant officers.

4.2 The impending UK exit from the EU will make a minor change to data protection legislation in the UK, but will make a significant change in data protection terms between the UK and the rest of the EU. The degree to which this will affect the Council remains unclear.

4.3 The decision of the European Court of Justice in July 2020 regarding the EU-US Privacy Shield and other international transfers of personal data will affect the Council (regardless of Brexit). Clarification and guidance about this is currently awaited from the Information Commissioner's Office.

5. CONCLUSION AND RECOMMENDATION(S)

5.1 Whilst, like all other local authorities and organisations undertaking a similar range of functions and volume of activities, the Council is not fully compliant with data protection legislation, the DPO is confident that it a reasonable degree of compliance has been achieved and that progress towards increased compliance across all Services will continue.

5.2 It is recommended that the Committee:-

(i) note the DPOs assessment of the Council's compliance with the requirements of data protection legislation;
(ii) provide appropriate challenge and comment.

Author(s)

Name	Designation	Contact Details
Donald Henderson	Data Protection Officer	x77930

Approved

Name	Designation	Date
Karen Donaldson	Interim Chief Operating Officer	11/08/2020

ANNEX

1. IMPLICATIONS, ASSESSMENTS, CONSULTATION AND COMMUNICATION

Strategic Implications	**Yes / None**
Community Plan / Single Outcome Agreement	**n/a**
Corporate Plan	**n/a**
Resource Implications	**n/a**
Financial	**n/a**
Workforce	**n/a**
Asset Management (land, property, IST)	**n/a**
Assessments	**n/a**
Equality Impact Assessment	**n/a**
Strategic Environmental Assessment	**n/a**
Sustainability (community, economic, environmental)	**n/a**
Legal and Governance	**n/a**
Risk	**n/a**
Consultation	**n/a**
Internal	**n/a**
External	**n/a**
Communication	**n/a**
Communications Plan	**n/a**

1. **Strategic Implication** N/A

2. **Resource Implications** N/A

3. **Assessments**

   - Equality Impact Assessment N/A
   - Strategic Environmental Assessment N/A
   - Sustainability N/A
   - Legal and Governance N/A
   - Risk N/A

4. **Consultation** N/A

5. **Communication** : N/A

6. **Background papers :** None

7. **Appendices :** None