PERTH AND KINROSS COUNCIL

Scrutiny Committee

12 June 2019

Data Protection Compliance 2018-19

Report by Data Protection Officer (Report No. 19/179)

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 2018-19.

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 local government activities and the many millions of interactions and transactions involving personal information that is involved in the delivery of public services, it is unlikely that Council will ever be able to state categorically that it is fully compliant. The DPO is assured however that the current level of compliance is reasonable and like most other organisations, Perth and Kinross Council is continuing to work towards full compliance insofar as is reasonably practicable.

2.2 The Council is reasonably compliant with data protection legislation.

2.3 The DPO is satisfied that the principal pillars of GDPR compliance are all in place and are gradually 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.

2.4 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.

2.5 Of the small numbers of breaches, 13 were reported to the Information Commissioner by the DPO. As the GDPR has been implemented and practice embedded, experience would suggest that 4 of those did not require to be so. Anecdotal evidence suggests that DPOs have in the early days "erred on the side of caution" and as a consequence, initial over-reporting has been a common issue across many organisations.

2.6 The organisation does not have a programme of mandatory training per se but has acknowledged that awareness training should be essential for all employees. Tailored training was designed and delivered for areas which were deemed particularly high risk because of the volume and nature of the sensitive personal information which required to be proceed (education/social care services etc.) The DPO is concerned however at the level of uptake in respect of generic training for all employees and has advised that the organisation should take steps to address this and ensure that employees complete and renew their training on an annual basis.

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.

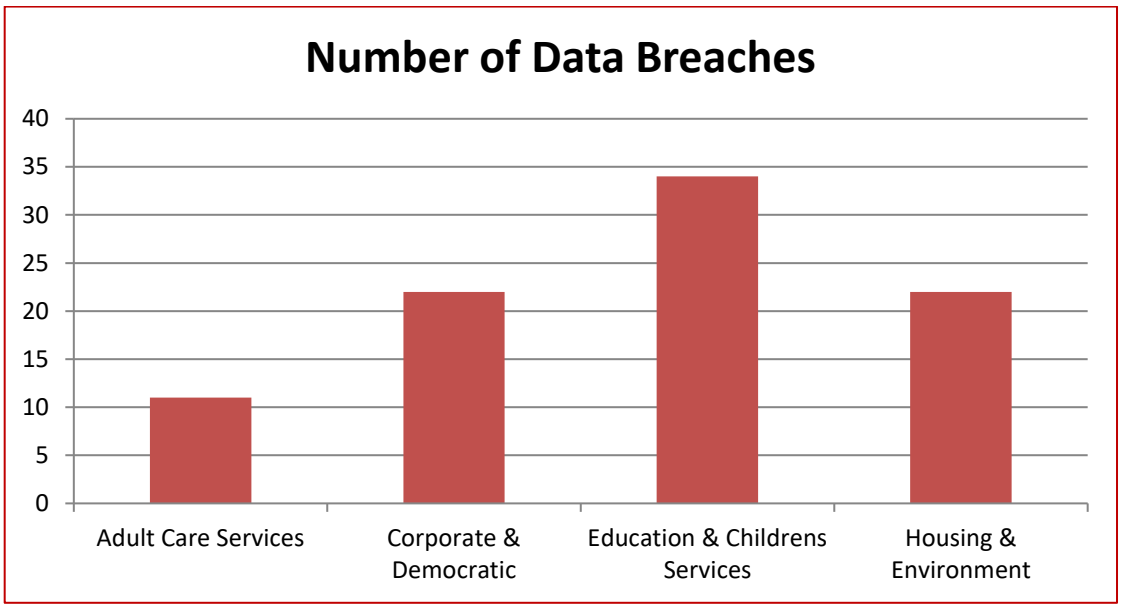
3.2 Data Breaches

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".

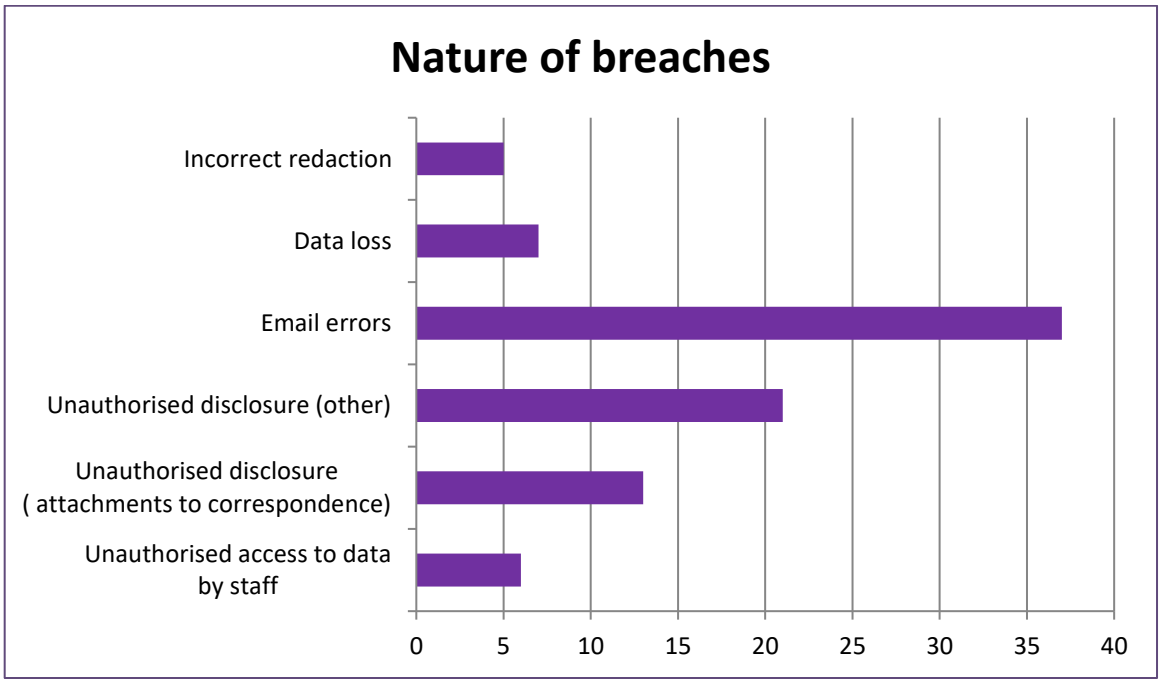
3.2.2 The Council is required to maintain a register of data breaches and, where appropriate, report them to the Information Commissioner's office.

3.2.3 Between 1 April 2018 and 31 March 2019, the Council recorded a total of 89 data breaches.

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 few cases however there were some 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 Service has been keen to engage with the DPO to amend and improve practice.

3.2.8 Of the 89 breaches, the DPO considered 13 of those required to be reported to the Commissioner's Office (ICO). As stated above, a few may not in fact meet the criteria for reporting, as this has become better understood by DPOs.

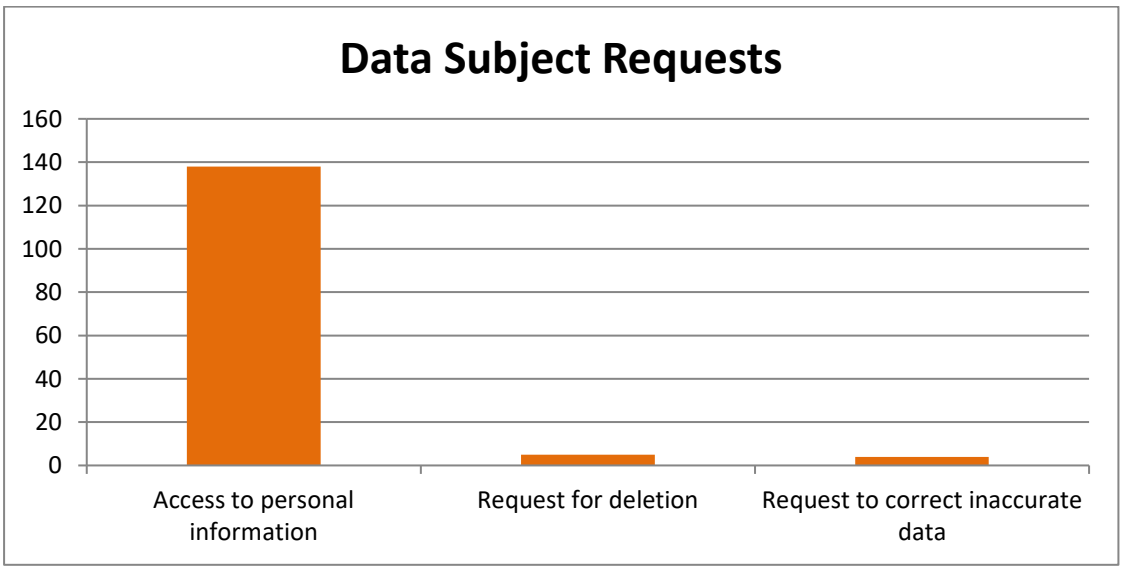
3.2.9 Of the 13 cases reported, 2 remain open with the ICO. In relation to the other 11 cases, the ICO considered that the actions taken by the Council in response to the breaches were appropriate and did not require any further action.

3.2.10 It would appear that across the organisation staff understand disclosure breaches and in this respect the DPO is fairly confident that all significant data breaches of this nature were reported during the year. Given the concerns expressed re the uptake of training however , across the organisation there may be but less understanding of the other potential grounds for breach. The DPO is therefore less convinced that all minor breaches are necessarily being captured but will continue to provide advice and guidance and is hopeful that ongoing training and greater experience will address this.

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 2018 and 31 March 2019, the Council received 147 requests of which:-



3.3.3. In terms of processing the 138 subject access requests;-

- 11 subject access requests are still currently in progress
- 28 are on hold awaiting further information (normally proof of identity) from the requester
- 99 subject access requests completed

3.3.4 Of the 99 requests that were processed

- 81 were completed within the statutory timescale (82% success).
- 18 were late (Many of these requests were complex and involved a the processing of a very large volume of information).

3.3.5 Of the 9 other requests;-

- 1 is on hold awaiting further information from requester
- 8 completed within timescale

3.3.6 The Council also received 15 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.

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

3.4 **Training**

3.4.1 The DP team has delivered introductory GDPR training in two series of Learn, Innovate, Grow sessions and has also provided a considerable number of more informal sessions to individual teams across the organisation on request. As stated above a risk based approach was taken and more tailored training was delivered to particular services and teams who routinely processed particularly sensitive personal basis

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 Given the communication of GDPR information, there appears to be a good level of general awareness across the Council.

3.4.4 In terms of breadth of knowledge, the Council has an e-Learning module about the GDPR and a supplementary module about data breaches. Uptake of these is disappointing, with only 32% of the possible staff (almost 5,200) having completed the GDPR module and 9% the data breach module.

3.4.5 This poor uptake of training was highlighted in a report (18-21) to the Audit Committee on 27 March 2019. The Management Action Plan included an action to ensure that managers are aware of what essential training is required to be undertaken by their teams.

3.4.6 Where a breach has been reported to the ICO, the most common response from the ICO is to ask whether employees involved in a data breach have undertaken data protection training within the last 12 months. It would appear, therefore, that the Information Commissioner has an expectation that all employees involved in processing personal data are undertaking data protection training every year. The DPO is concerned that the Council cannot meet that expectation.

3.4.7 The DPO team plans to re-write the main GDPR e-Learning module during 2019-20 and also prepare two further Learn, Innovate, Grow sessions – one specifically about the section of the Data Protection Act covering law enforcement and a general one for use on an on-going basis.

3.4.8 The DPO is seeking management support to ensure that the Audit action identified is implemented to ensure that relevant staff undertake appropriate training.

3.5 Data Protection Impact Assessments

3.5.1 The Council's Data Protection Policy requires a data protection impact assessment (DPIA) to be completed for any new project or policy that will involve processing personal data.

3.5.2 It should be noted that the DPIA process is not a simple administrative process; these can be complex often taking several weeks to complete properly, with the DPO team supporting services to get the correct information in place to make a proper assessment.

3.5.3 During the period 93 DPIAs have been initiated. To date ;-

- 16 have been approved
- 3 have been closed as a result of problems identified in the processing;

3.5.4 The rest remain in progress or have stalled often due to workload issues in either the DPO team or the Service area. The DPO intends to review the status of these in the course of the coming year, resources permitting.

3.5.5 It is intended that completed DPIAs will be published on the Council website in due course, but it has not yet been possible to under undertake this exercise.

3.5.6 As the DPO is reliant upon services being proactive and advising of the new projects, it is unclear to the DPO whether DPIAs are being completed for all new projects or policies involving the processing of personal data.

3.6 Data Sharing Agreements

3.6.1 A Data Sharing Agreement (DSA) sets out what, why and how personal data is to be shared between two organisations where each organisation separately determines the purpose and means of processing the personal data, for example between the Council and Police Scotland.

3.6.2 The DPO is required by the Council's Data Protection Policy to maintain a register of DSAs and must be consulted prior to any new DSA being signed. The register currently contains information about 28 DSAs, of which 11 have been signed by the Council.

3.6.3 Whilst It would seem that most of the remaining 17 DSAs have been approved at some point in the past, it has not been possible for Services to locate final, signed copies of them. It is planned to review the status of this remainder and to develop new DSAs where required during 2019-20.

3.6.4 It is intended that completed DSAs will be published on the Council website in due course, but it has not yet been possible to undertake this exercise.

3.6.5 As with DPIAs, the DPO is dependent upon Services advising of their existence. It is unclear therefore whether all new DSAs are passed to the DPO.

3.7 Register of Processing Activities

3.7.1 The Council is required by law to maintain a record of every activity it undertakes involving the processing of personal data. The collection of these records is usually referred to as the Register of Processing Activities (RoPA).

3.7.2 There are currently 450 entries in the register. Almost all of these were made prior to the implementation of the GDPR and the individual records are known to be relatively incomplete. Given the volume and breadth of the Council's business it is also considered that a significant number of records still require to be added to the register.

3.7.3 The DPO plans to conduct an exercise with Services during 2019 to ensure that the entries are all complete, add any missing entries to the register and put in place a procedure for its on-going maintenance.

3.8 Privacy Notices

3.8.1 The Council is required by law to provide information to data subjects about their personal data at the point it is collected. The details to be provided are set out in the GDPR. This is known as a privacy notice or privacy policy.

3.8.2 The Council follows the ICO's advice about this and provides a minimal amount of information at the actual point of collection, but provides links to further detailed information on the Council website.

3.8.3 Much of the information to be provided on the website is general (data subject rights and contact details, etc.) but there also needs to be a detailed set of information on the website for each individual activity.

3.8.4 It is considered that there are a considerable number of detailed privacy notices still to be written and published, and the DPO plans to address this with Services this as part of the exercise to address deficiencies in the RoPA mentioned above.

3.9 Data Protection Officer

3.9.1 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.

3.9.2 As the DPO is also the Council's Information Governance Manager with an established operational portfolio, further work requires to be done to develop understanding of this new statutory strategic role, across the organisation.

3.9.3 As part of the council's governance framework, a mechanism has been agreed for the formal provision of advice by the DPO to the Council and all formal advice provided to date had been accepted.

3.10 DPO Resources

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

3.10.2 The Data Protection Officer's team comprises 2.5 FTEs

- the Information Governance Manager, who is the DPO
- 1.5 FTE Information Governance Officers who can deputise

3.10.3 The DPO team are members of the Information Governance Team and therefore have a broader portfolio than data protection, dealing also with freedom of information, information security and management, statutory records management and corporate complaints.

3.10.4 The DPO team are heavily involved in providing advice to employees on a daily basis in response to telephone calls and emails. They also deal with all:-

- Data subject requests
- Data breach investigations
- All communications with the ICO
- Providing strategic advice as regards data protection policy and practice
- Providing technical advice by way of guidance documents, procedures
- Providing professional and practical support in the preparation of DPIAs, Privacy Notices, DSAs and the RoPA
- Designing and delivering training
- Reviewing existing and new contracts to ensure that they are complaint with legal data protection requirements

3.10.5 As the Council is required to involve the DPO in the decision-making related to any new project involving processing personal data, DPO currently also sits on a number of project boards or steering groups for major projects in the Council.

3.10.6 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.

3.10.7 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.

3.10.8 The DPO advises that the demands of the function cannot be met within current resources but is mindful of the financial climate in which the organisation is operating. That being acknowledged, the DPO has a responsibility to flag this to the Council as a risk.

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

3.11 **Compliance Monitoring**

3.11.1 This report has been based on the information currently available to the DPO team and for reasons outlined within the report, cannot be considered a comprehensive assessment of the Council’s compliance with data protection legislation during the year.

3.11.2 As part of the Council's wider review of the governance framework the DPO will work with Senior Management and in particular the Head of Legal & Governance Services to develop a more systematic approach to obtaining assurance as regards compliance across the organisation.

4 CONCLUSION AND RECOMMENDATION(S)

4.1 Whilst like all other local authorities an organisations undertaking a similar range of functions and volume of activities, the Council is not fully complaint the DPO is assured that they are reasonably so business and will continue to progress towards increased compliance across all Services.

4.2 The level of uptake of the generic data protection training needs to be addressed by the organisation.

4.3 It is recommended that the Committee:-

(i) note the DPOs assessment of the Council's compliance with the requirements of the 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
Jim Valentine	Depute Chief Executive	25 May 2019

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