PERTH AND KINROSS COUNCIL

Scrutiny Committee - 9 June 2021

DATA PROTECTION COMPLIANCE 2020-21

Report by Data Protection Officer
(Report No. 21/87)

PURPOSE OF REPORT
This report is the professional assessment of the Council's compliance with the UK 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 2020-21.

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 and volume of the Council's activities, it is unlikely that any 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 human error, a lack of training/awareness, and workload pressures.

2.3 The Council has been working under different circumstances this year, requiring a rapid adjustment to often unfamiliar technology and working without the assistance of physically close colleagues. In itself, this has probably generated more issues requiring the attention of the DPO team, but there also has been a significant amount of additional work for the DPO team generated by the implementation of measures in response to the pandemic. Despite periods of reduced staff numbers, the DPO team has managed to cope with the workload reasonably well.

2.4 Whilst the Council would wish to avoid any data breach, the total number of breaches recorded in the year remains very small given the volume and wide range of personal data that is processed across the Council in the course of a year. Of the breaches recorded, few were considered as needing reported to the information Commissioner's Office.

2.5 The DPO has highlighted issues arising from a lack of adequate resources in the DPO team, supplier intransigence, and 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 UK GDPR and the Data Protection Act 2018. It should be noted that the UK GDPR is the implementation in UK law of the original EU GDPR, it came into force on 1 January 2021 and is, in all relevant aspects, identical to the original.

3.1.2 The current version of the policy was approved in November 2018 and will be reviewed during 2021-22.

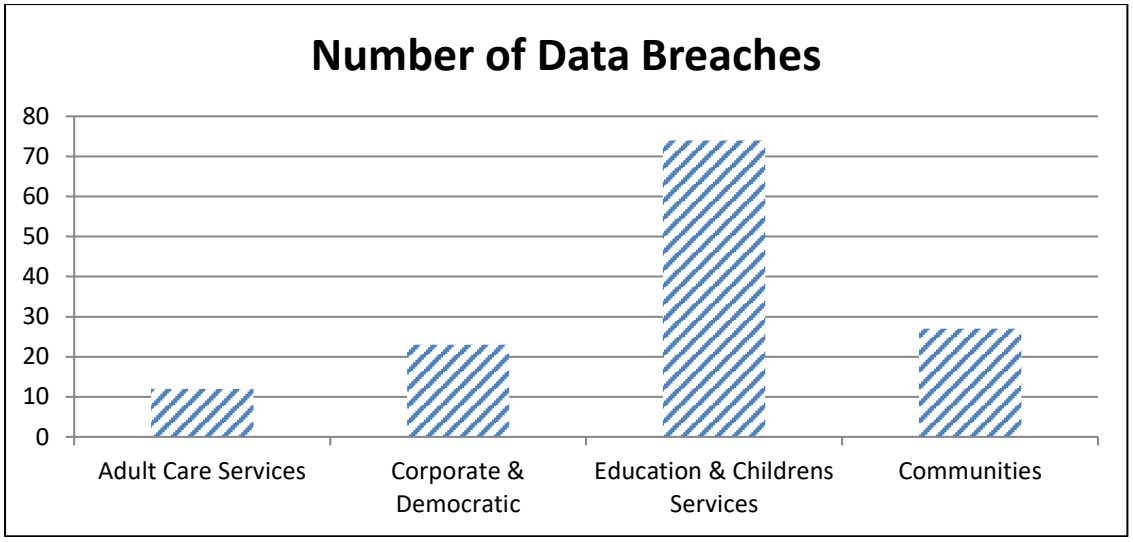
3.2 Data Breaches

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". The term 'security' refers to both technical measures and organisational measures such as policy, procedure and practice.

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 2020 and 31 March 2021, the Council recorded a total of 146 data breaches (compared to 96 during the previous year). Any data breach is a matter which the DPO takes seriously but in terms of numbers, this needs to be considered in the context of the many millions of interactions and transactions involving the processing of personal information entailed in the delivery of all Council services.

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 Many of the breaches in the year, particularly email error and unauthorised disclosure breaches, are attributable to time pressures and unfamiliarity with new ways of working and the associated technology, all brought about by the pandemic.

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

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

3.2.9 Of the 146 breaches, the DPO considered seven required to be reported to the Commissioner's Office (ICO). This was based on an assessment of the likely level of risk to the individuals arising from the breach in each case.

3.2.10 For five 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 one of the breaches, the ICO did require further actions; these have been completed. The ICO has not yet concluded its consideration of the most recent breach.

3.2.11 Three of these breaches were due to email errors, three to unauthorised disclosure of information and one to the loss of personal data.

3.2.12 It would appear that employees across the organisation understand breaches caused by email error and through other unauthorised disclosure. 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 137 requests for access to personal information, of which:-

- 16 are still in progress
- 37 are on hold awaiting further information from the requester (normally proof of identity and often never provided)
- 84 have been completed

3.3.3 Of the 84 requests that were processed

- 60 were completed within the statutory timescale (71%).
- 24 were late (many of these requests were complex and involved the processing of a very large volume of information).

3.3.4 It is anticipated that a number of the requests still in progress will also be late.

3.3.5 It should be noted that processing requests for access to information were adversely affected by the Council's initial suspension of non-essential services at the beginning of 2020-21. The implementation of coronavirus measures across the Council has also slowed the availability of information from Service areas on occasion due to the involvement of staff in other essential activities.

3.3.6 The Council received 8 other requests: -

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

3.3.7 The Council also received 21 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.

3.3.8 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 general training sessions this year, partly due to the circumstances and partly to workload. Training has been provided for individual teams, 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 and there is an apparent willingness for employees to clarify particular issues with the DPO team when they arise.

3.4.4 The Council does have basic data protection training in place, but the DPO is concerned at the level of uptake, particularly in relation to regular refresher training. It is the DPO team's intention to revise the current training module, when resources become available to do so, to make it more engaging and better able to influence general behaviour regarding the protection of personal data.

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 The pre-DPIA checklist, introduced last year to allow the early identification of projects that would require a full DPIA prior to the project going live, has proved successful and has been transferred to an online process. The DPO team is aware of a backlog of incomplete DPIAs and hopes to progress this during 2021-22, if resources are available within the DPO team.

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

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 proved impractical due to resource availability both within the DPO team and within Services who are required to provide the team 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.

3.5.7 The DPO team's continuing inability to address these major issues of compliance for the Council is concerning.

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

3.6.3 The current postholder will retire during 2021-22. The Council has plans to address this.

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 function does not have a dedicated team but is supported from the Information Governance Team who have significant other responsibilities, in addition to data protection - freedom of information, information security, information and records management, and corporate complaints handling.

3.7.3 Within that team, the following have specialist knowledge and expertise in data protection

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

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

3.7.5 As with many other teams across the organisation, resources are an issue as reflected in the outstanding activities identified above. Much of the section's business is responsive, with statutory timescales and constraints attached, which often means that to manage the associated risks, strategic and development activities are sacrificed.

3.7.6 The DPO considers that, whilst directing resources to "urgent" work has been adequate in the short-term, the continuing inability to deliver an appropriate level of training or review practice and policy, is likely to become a significant issue for the Council in the next 24 months.

3.7.7 In the reports for both 2018-19 and 2019-20, 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.

3.7.8 The DPO considers that this situation has not changed and the lack of adequate resources for the DPO function is an increasing risk to the Council. This situation will be compounded by the retirement of the current postholder and the consequent loss of knowledge and experience.

3.7.9 The DPO considers that the function is currently being exercised appropriately and effectively.

3.8 **Compliance Monitoring**

3.8.1 This report has been based on the compliance information currently available to the DPO team.

3.8.2 It is planned to ensure a more robust assessment in the future by building additional questions into the Council's preparations for the Annual Governance Statement. These will provide appropriate evidence of the Council's compliance with the data protection legislation.

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 There have been a number of occasions recently where data protection has not been considered relevant to projects and the DPO has not been involved appropriately until a relatively late stage. This inevitably results in delays to the project. These occurrences may be due to the circumstances of the last year or simply to a lack of awareness and understanding. The latter can only be addressed through a comprehensive awareness and training programme for the Council for data protection.

4.3 The situation for data protection regarding the UK's exit from the EU should be clarified shortly, with an 'adequacy decision' expected from the EU regarding the UK's data protection arrangements. This will mean that the Council's personal data can continue to be held and processed in the EU.

4.4 Following the UK exit from the EU, and also the court decision in 2020 regarding data transfers to the USA, the situation regarding the international transfer of information is now being monitored much more closely. The Council's standard contractual terms now take account of this and a risk-based approach is taken in each case. In one significant instance steps were taken during the year to re-locate information from the USA to the EU.

5. CONCLUSION AND RECOMMENDATIONS

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 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) Scrutinise the work of the Council in terms of compliance with GDPR.

Author(s)

Name	Designation	Contact Details
Donald Henderson	Data Protection Officer	x77930

Approved

Name	Designation	Date
Karen Donaldson	Chief Operating Officer	

If you or someone you know would like a copy of this document in another language or format, (on occasion, only a summary of the document will be provided in translation), this can be arranged by contacting the Customer Service Centre on 01738 475000.

You can also send us a text message on 07824 498145.

All Council Services can offer a telephone translation facility.

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 Implications

Not applicable.

2. Resource Implications

Not applicable.

3. Assessments

- Equality Impact Assessment – not applicable
- Strategic Environmental Assessment – not applicable
- Sustainability – not applicable
- Legal and Governance – not applicable
- Risk – not applicable

4. Consultation

Not applicable.

5. Communication

Not applicable.

4. BACKGROUND PAPERS

None.

5. APPENDICES

None.