PERTH AND KINROSS COUNCIL

Scrutiny and Performance Committee

13 September 2023

DATA PROTECTION COMPLIANCE 2022-23

Report by Data Protection Officer (DPO)
(Report No. 23/247)

1. PURPOSE

1.1 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 her in accordance with the legislation). This report relates to the year 2022-23.

2. RECOMMENDATIONS

2.1 It is recommended that the Committee:

(i) Notes the DPO's assessment of the Council's compliance with the requirements of data protection legislation.

(ii) Considers the Council's performance in terms of compliance with the GDPR and provides constructive scrutiny and comment.

(iii) Notes that the DPO is confident that a reasonable degree of compliance with data protection legislation has been achieved during 2022-23 and that progress towards increased compliance across all Services will continue during 2023-24

3. STRUCTURE OF REPORT

3.1 This report is structured over the following sections:

- Section 4: Background
- Section 5: Data Breaches
- Section 6: Data Subject requests
- Section 7: Policy and Process
- Section 8: Training
- Section 9: Improvement Actions
- Section 10: Conclusion

4. BACKGROUND

4.1 The UK General Data Protection Regulation ("GDPR") requires the Council, as a public authority, 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. The Council's Data Protection Policy sets out that the DPO will present a report on the Council's data protection compliance to the Scrutiny and Performance Committee annually or more frequently, if considered necessary. It is the role of the Scrutiny and Performance Committee to consider the DPO's report in relation to the Council's compliance and to provide appropriate constructive challenge and comment.

Role of DPO

4.2 The role of the DPO is defined in the GDPR; 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. It should be noted that legal responsibility for compliance with data protection law lies with the Council as a public body and not the DPO as an individual. The DPO does have a role in providing advice and guidance to support the Council in complying with the legislation and to monitor and report on its performance. The Committee can be assured that all formal advice provided by the DPO, to date, to support the organisation and ensure compliance, has been accepted.

4.3 The DPO and the Information Rights Team sit within the Audit and Governance Team, with the DPO maintaining a separate and distinct reporting line to the Head of Legal and Governance Services in her capacity as Senior Information Risk Officer.

Resources of DPO

4.4 The legislation also provides that adequate resources should be made available to the DPO to enable them to fulfil their role. The Data Protection Officer function does not have a dedicated team but is supported by the Information Rights (formerly the Information Governance team) and Information Security teams (referred to as the DPO's team for the purposes of this report). In terms of skills and expertise, as well as the DPO, there are 2 officers (1.7 FTE) within the Information Rights team who have specialised data protection knowledge. At present, almost all staff time is required to deal with increasing volumes of complex responsive work.

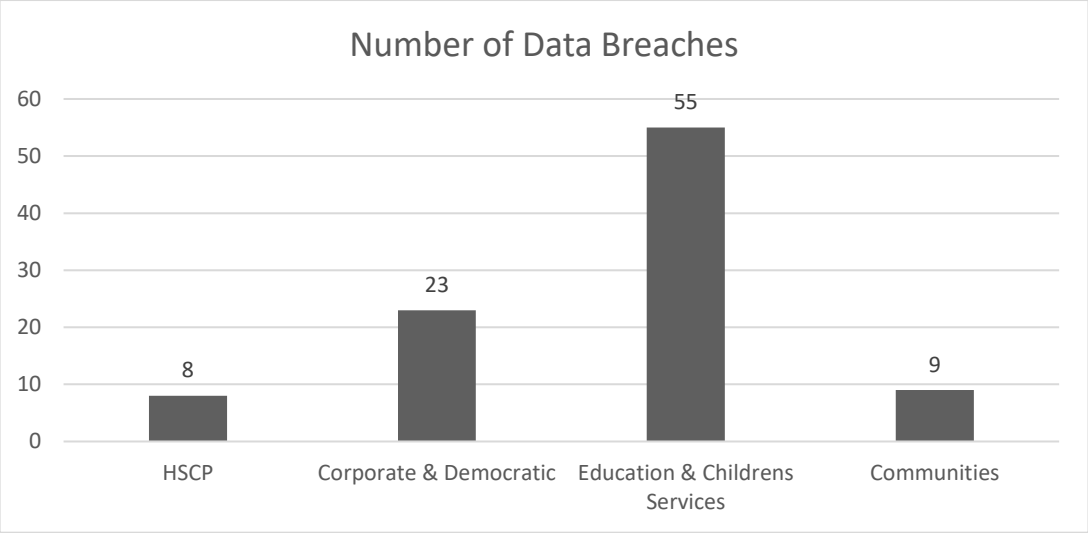
5. PERFORMANCE: DATA BREACHES

5.1 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, procedures and practice.

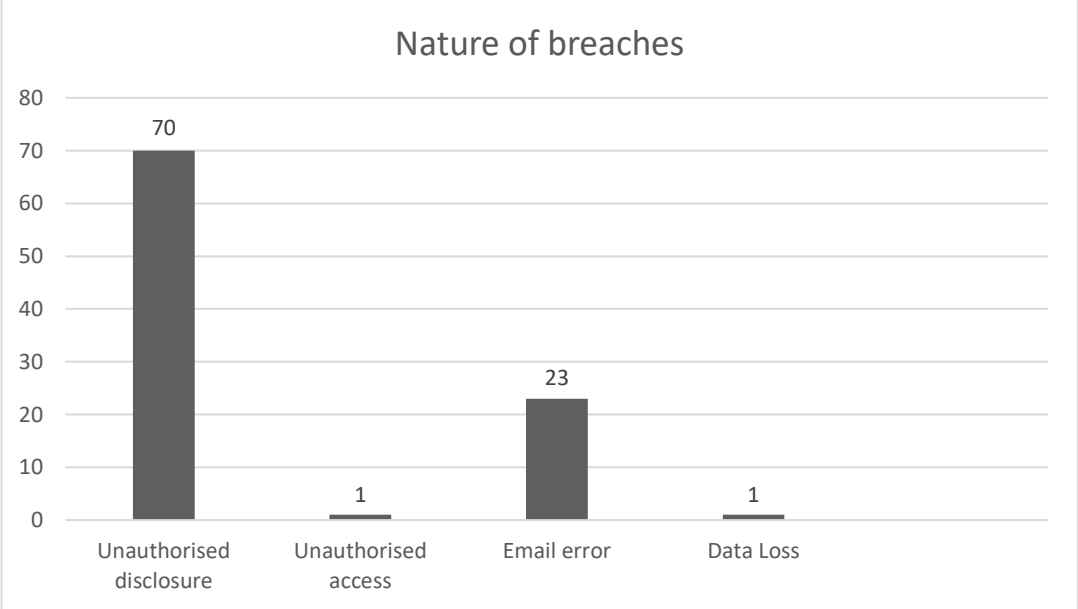
5.2 The Council is required to maintain a register of data breaches and, where appropriate, report them to the Information Commissioner's office.

5.3 Between 1 April 2022 and 31 March 2023, the Council recorded a total of 95 data breaches (compared to 134 during the previous year). This 29% reduction in the number of breaches may be attributable to increasing awareness of what constitutes a data breach, advice on improving processes previously provided by the Information Rights team and greater familiarity with technology and processes adopted rapidly during the pandemic. However, it is recognised that continued training on recognising and reporting data breaches would provide assurance that all breaches were reported appropriately.

Any data breach is a matter which the DPO takes seriously, but in terms of numbers, this figure 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 in the course of a year. The split of data breaches by Service is illustrated below: -



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



5.5 In relation to the data breaches which have been recorded, the DPO confirms that: -

- almost all recorded breaches were reported promptly to the DPO and any remedial action which was requested was taken quickly;
- where breaches have been identified, the relevant service area has been keen to engage with the DPO to amend and improve practice;
- of the recorded breaches, particularly those categorised as email error or unauthorised disclosure breaches, almost all appear to be attributable to human error as a consequence of resource pressures within the relevant service areas as opposed to any systemic failure of process or policy; and
- of the 95 breaches, the DPO determined that 6 required to be reported to the Commissioner's Office (ICO) following a risk-based assessment of potential impact on the data subject based on the nature/ circumstances of the information disclosed.

5.6 Of the 6 breaches reported to the ICO: -

- Five of these breaches were due to the unauthorised disclosure of personal information and one to the loss of data.
- In relation to all of the reported breaches, the ICO was satisfied that the actions taken by the Council in response to the breaches were appropriate and did not require any further action.

5.7 The DPO provides support and advice to services and teams when a data breach has occurred and, where necessary, provides additional staff training and written guidance.

5.8 The DPO considers that there is a generally good and increasing understanding across the Council in relation to what constitutes a data breach. Breaches will continue to be monitored and advice and training provided as appropriate.

6. PERFORMANCE: DATA SUBJECT REQUESTS

6.1 The GDPR gives data subjects a number of specific rights, such as accessing and receiving a copy of information held about them, and having inaccurate personal data rectified. Requests to exercise these rights must be responded to within 1 month (interpreted by the Council as 28 calendar days), unless the information requested is particularly complex in nature or the request is from an individual who has made multiple requests; in these cases, an additional two months to respond is permitted by the legislation. The DPO has responsibility for dealing with requests received by the Council.

6.2 There was a 27% increase in the number of subject access requests received during 2022-23, compared to 2021-22. This increase is partly attributable to individuals seeking confirmation of their care experience, in order to apply to Scotland's Redress Scheme for survivors of historical child abuse in care. Many of the records processed in relation to this scheme contain a very large

volume of information, some of which will contain sensitive personal information relating to other individuals which may require to be redacted.

6.3 Between 1 April 2022 and 31 March 2023, the Council received 211 requests for access to personal information, of which: -

- 154 have been completed.
- 57 are on hold pending further information from the requester (this is sometimes never provided) or a decision on whether they wish to proceed with making a request.

6.4 Of the 154 requests that were processed: -

- 129 were completed within 28 days (84%).
- 25 were responded to outwith the 28-day timescale (16%).

6.5 Eighteen (72%) of those requests processed outwith the 28-day timescale were complex requests, where the legislation permits an extension period of up to two months. In many of these cases, information was released in batches i.e., individuals received at least of part of their information within the first 28 days.

6.6 Over and above the 211 data subject access requests referred to above, the Council received 10 other data subject requests during 2022-23: -

- 3 requests for erasure (individuals have the right to request their personal data is deleted);
- 6 requests for rectification (individuals can request that inaccurate personal data is corrected); and
- 1 request regarding processing (individuals can request that the processing of their information is restricted).

6.7 In addition, the Council also received 38 information related complaints, either directly from the data subjects or via the ICO, about the way personal data had been handled. All these complaints have been dealt with.

6.8 The Information Rights team also processed 43 requests for information made during 2022-23, under a provision in data protection legislation which permits authorities, such as Police and HMRC, to request personal information to assist with criminal investigations and the assessment and collection of taxes.

6.9 During 2022-23, the process through which information held in relation to historical and current childcare files was streamlined. Rather than asking officers from Education and Children's Services to carry out searches and extract information, officers from the Information Rights team now access systems directly to identify and extract information held.

6.10 Applicants for compensation from Scotland's Redress Scheme can ask the Council to verify that they have not previously received compensation related to their experience in care. The Information Rights team now carries out these

verification checks and liaises directly with the Scheme, rather than this work being carried out by Education and Children's Services.

6.11 The Council is sometimes unable to provide information requested by survivors of historical child abuse in care, usually because the person in question was in an institution not run by local government. Recognising the distress that this may cause applicants, work by the Information Rights team to identify the location of records and to work with other local authorities and educational establishments to ensure as comprehensive a response as possible is provided, is ongoing.

6.12 Where information held about requestors may cause them distress, the Information Rights team now provides advance warning of this before issuing their response. Individuals are regularly signposted to organisations that can provide them with support going through their records.

6.13 A new case management system for recording, processing and reporting on information requests more efficiently will come into use in August 2023.

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

7. SURVEILLANCE & INTERCEPTION OF COMMUNICATIONS

7.1 The Council has powers under the Regulation of Investigatory Powers (Scotland) Act to undertake directed surveillance and to utilise covert human intelligence sources. The Council also has powers under the Regulation of Investigatory Powers Act to obtain information ('intercept') about electronic communications.

7.2 Council officers have a duty to report on the use of these powers to Elected Members.

7.3 During 2022/23, no directed surveillance was authorised, no covert human intelligence sources were used, and no electronic communications information was obtained.

7.4 The Council's policy statement on the use of directed surveillance and the intercept of communications is attached as Appendix 1.

8. TRAINING

8.1 Throughout the year, the importance of data protection has been signposted to all staff through use of the Council's intranet and Managers' briefings, as well as reminders about data protection issues in staff communications, at the DPO's request.

8.2 The DPO has also delivered targeted training sessions to individual teams and groups of staff, on request throughout the year.

8.3 The DPO and her team provided training to elected members following the election of the new Council in May 2022. Support, awareness- raising and advice is provided to councillors on an ongoing basis, as required.

8.4 It is acknowledged that increasing workload of the small team has limited the ability to provide more general training throughout the year.

8.5 New online data protection training will be made available to all Council staff during August 2023.

8.6 The DPO considers there to be a reasonable level of general awareness across the Council and notes that staff appear to be willing to seek advice and support from the DPO.

9. DATA PROTECTION POLICY AND PROCESS

9.1 The DPO is satisfied that the Council has a Data Protection Policy which complies with the separate requirements of the UK GDPR and the Data Protection Act 2018.

9.2 It is a statutory requirement that the Council be able to provide evidence of its compliance with the legislation at all times. Compliance is therefore documented and evidenced by the Council's use of: -

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

9.3 It is the responsibility of the Council to carry out DPIAs and ensure Data Processing Agreements and Privacy Notices are in place. The role of the DPO is to assist and advise in their creation and to maintain registers of the documentation.

9.4 The DPO is satisfied that there is some form of privacy notice in place in relation to all processing of personal information carried out by the Council. Processing may be covered by the General Privacy Notice which appears on the Council website or by more specific short or detailed privacy notices. The DPO continues to monitor, review and provide advice to services as required. Privacy notices are required where we collect personal data. The Council has a general privacy notice in place and short privacy notices are generally in place as required. Work is ongoing with Services to ensure that corresponding detailed privacy notices are also in place.

9.5 Where personal information requires to be shared with other parties (e.g., Police, Health etc) best practice requires that Data Sharing Agreements should be put in place. These are specialised documents which tend to be lengthy and time-consuming pieces of work, often needing extensive consultation with the other organisations involved. The DPO is satisfied that

Data Sharing Agreements are in place where required, and that the Council is adopting best practice wherever possible.

9.6 The UK government has announced its intention to make changes to data protection legislation. The draft Data Protection and Digital Information Bill, which was introduced in June 2022, amended rather than repealed existing legislation. After a period of consideration, this Bill was withdrawn and the Data Protection and Digital Information (No. 2) Bill was introduced to Parliament in March 2023. This is being now being considered as part of the wider legislative process. The extent of the proposed changes is expected to be relatively limited; however, there will be a requirement to review our policies and processes once the new legislation comes into force.

10. IMPROVEMENT ACTIONS

10.1 Work to further streamline processes in relation to collating responses to subject access requests will continue during 2023-24.

10.2 Training on recognising and reporting data breaches will be developed and delivered during 2023-24 to ensure as far as possible that all incidents are reported to the DPO.

11. CONCLUSION

11.1 Given the breadth of all local authorities' activities and the millions of transactions involving personal data that are processed each year, no local authority can state categorically that it is fully compliant with data protection legislation. It is the opinion of the DPO, however, that the Council continues to achieve a reasonable and acceptable level of compliance.

11.2 The DPO is satisfied that the principles of GDPR compliance are understood and embedded as normal practice across the Council. When procedural failings involving data protection occur, these can almost always be attributed to human error as opposed to a systemic failure in terms of policy or process.

11.3 Whilst the Council would wish to avoid any data breach, given the volume and range of personal information which it processes, the number of reported breaches remains very low, with only a small percentage of these meeting the threshold requiring them to be reported to the Information Commissioner's Office.

Author(s)

Name	Designation	Contact Details
Jillian Walker	Data Protection Officer	DPO@pkc.gov.uk

Approved

Name	Designation	Date
Lisa Simpson	Head of Legal & Governance / Senior Information Risk Officer	8 August 2023
Karen Donaldson	Chief Operating Officer	9 August 2023

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.

2. BACKGROUND PAPERS

None.

3. APPENDICES

The Regulation of Investigatory Powers (Scotland) Act 2000 Policy Statement.