PPERTH AND KINROSS COUNCIL

Scrutiny and Performance Committee
21 September 2022

DATA PROTECTION COMPLIANCE 2021-22

Report by Data Protection Officer
(Report No. 22/230)

1. PURPOSE

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 2021-22.

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 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 2021-22 and that progress towards increased compliance across all Services will continue during 2022-23

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 Action
- 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 Committee annually or more frequently, if considered necessary. It is the role of the Scrutiny 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 Data Protection Officer 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. 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 During 2021-22 the previous DPO retired resulting in the need for structural change within the wider Legal and Governance Service. The DPO and the Information Governance Team have now transitioned smoothly into the new Audit and Governance Team, with the DPO maintaining a separate and distinct reporting line to the Head of Service in her capacity as Senior Information Risk Officer.

Resources of DPO

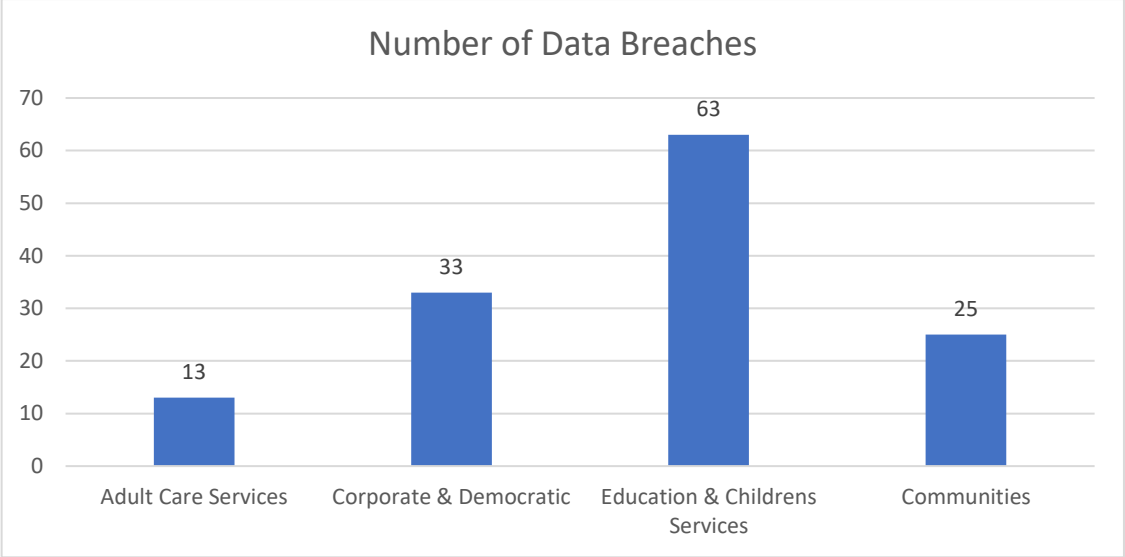
4.4 The legislation also provides that adequate resources should be made available to the DPO to enable them to fulfil their role. The Data Protection Officer function does not have a dedicated team but is supported by the Information Governance and Information Security teams (referred to as the DPO's 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 Governance team who have specialised data protection knowledge. It is recognised by the DPO that there is an increasing need to direct more resources towards supporting the organisation to ensure compliance through support and training; however, at present almost all staff time is required to deal with responsive work, which is increasing in complexity and volume.

5. PERFORMANCE : DATA BREACHES

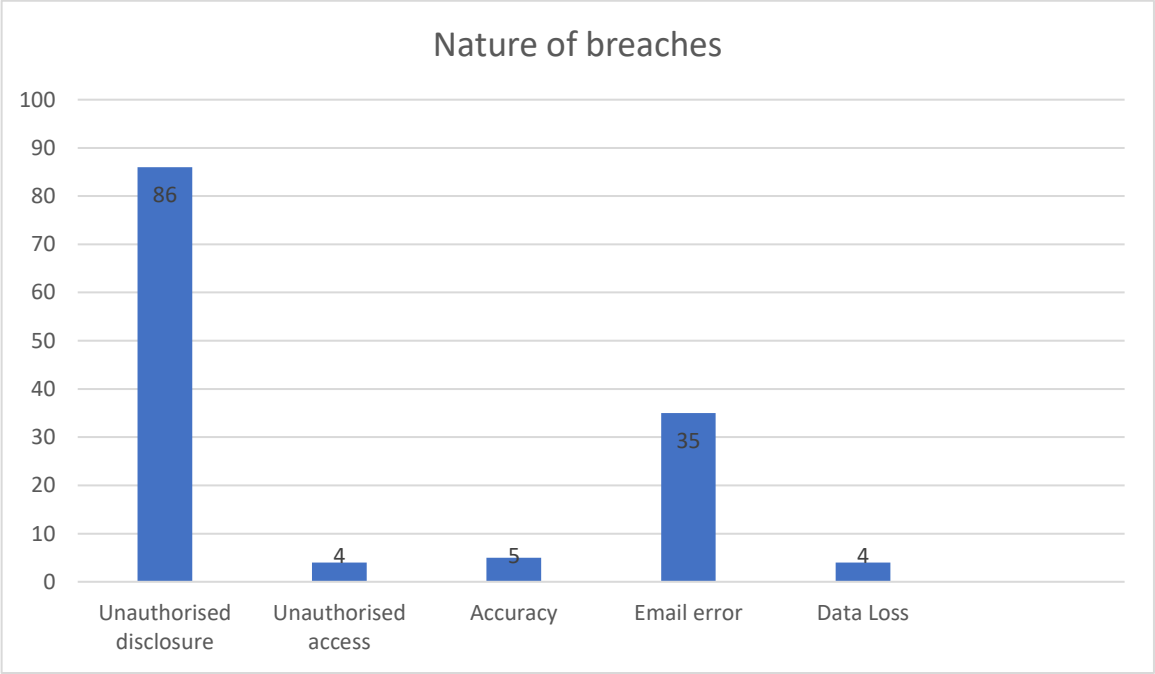
5.1 A data breach is defined as an incident involving "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data". The term 'security' refers to both technical measures and organisational measures such as policy, procedure 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 2021 and 31 March 2022, the Council recorded a total of 134 data breaches (compared to 146 during the previous year). 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 would confirm 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.

- of the 134 breaches, the DPO determined that 9 required to be reported to the Commissioner's Office (ICO) following an risk-based assessment of potential impact on the data subject based on the nature/circumstances of the information disclosed.

5.6 Of the 9 breached reported to the the ICO;-

- Four of these breaches were due to the unauthorised access of personal information, three to unauthorised disclosure of data, one to the accuracy of information recorded and one to the loss data.
- In relation to 5 of the 9 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.
- The DPO can confirm that the actions which the ICO required the Council to take in relation to the other 4 breaches, have been completed.

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

5.8 The DPO considers that generally, there is a good understanding across the Council in relation to data breaches caused by email errors and the unauthorised disclosure of personal information; however, other types of data breach may be less well understood. 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 19% increase in the number of subject access requests received during 2021-22, compared to 2020-21. This increase is 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. Given the nature of the information being accessed, requesters often require support and assistance from the DPO's team when accessing their files.

6.3 Additional resources were made available to the DPO during the second half of 2021-22, which enabled two additional officers to be employed to assist with processing subject access requests relating to the Redress Scheme.

6.4 Between 1 April 2021 and 31 March 2022, the Council received 166 requests for access to personal information, of which:

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

6.5 Of the 140 requests that were processed:

- 55 were completed within the 28-day timescale (39%).
- 85 were responded to outwith the 28-day timescale (61%).

6.6 A significant proportion of those requests processed outwith the 28-day timescale were considered to be complex requests, where the legislation permits an extension period of up to two months.The Council's ongoing response to the Covid-19 pandemic was also a factor in some cases as staff were deployed to other tasks to deliver essential services, which caused delays in accessing and collating the necessary information

6.7 Performance improved throughout the period 2021-22 helped by the additional resource recruited to assist in requests related to the redress scheme. Performance in the last quarter of the period saw 88% of subject access requestsresponded to within 28 days.

6.8 There was a 19% increase in the number of subject access requests received during 2021-22, compared to 2020-21. This increase is 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. Given the nature of the information being accessed, requesters often require support and assistance from the DPO's team when accessing their files.

6.9 Additional resources were made available to the DPO during the second half of 2021-22, which enabled two additional officers to be employed to assist with processing subject access requests relating to the Redress Scheme.

6.10 Over and above the 140 data subject access requests referred to above, the Council received 12 other data subject requests during 2021-22:-

- 4 requests for erasure (individuals have the right to request their personal data is deleted)
- 4 requests for rectification (individuals can request that inaccurate personal data is corrected)

- 4 requests regarding processing (individuals can request that the processing of their information is restricted).

6.11 In addition, the he Council also received 35 information related complaints, either directly from the data subjects or via the ICO, about the way personal data had been handled. All of these complaints have been dealt with.

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

7. TRAINING

7.1 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.

7.2 The DPO team has also delivered multiple targeted training sessions to individual teams and groups of staff, on request throughout the year. Online data protection training is available to all Council staff, the content of which is presently being reviewed and refreshed.

7.3 Data Protection training has also been provided to elected members as part of their Induction programme and refresher training and updates will be provided as part of their wider training and development programme.

7.4 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 DPO apporiately.

8. DATA PROTECTION POLICY AND PROCESS

8.1 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. It should be noted that the UK GDPR is the implementation in UK law of the original EU GDPR following exit from the European Union; it came into force on 1 January 2021 and is, in all relevant aspects, identical to the original EU regulation.

8.2 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 Processing Arrangements
- Privacy Notices
- Data Sharing Agreements (DSAs)

8.3 It is the responsibility of the Council to create/ produce DPIAs, detail of Processing Arrangements and Privacy Notices. The role of the DPO is to assist and advise in their creation and to maintain registers of the documentation.

8.4 Recognising that the DPIA process can be labour intensive but acknowledgeing the need to ensure compliance with DP legislation and the benefit in involving the DPO in projects, programmes and procurement activity, a shortened online version of a DPIA (the DPIA Checklist) was developed. THe purpose of this is to enable the DPO and services to make a risk based assessment in terms of which projects/programmes/procurement activities require the more though and indepth full DPIA to be carried out. This has ensured that resources are directed appropriately and effectively, ensuring that the higher risk projects etc. are prioritised and ultimately speeding up the approval process.

8.5 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 montiro,re view 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 in place, generally as required. are in place as required; Work is ongling with Services to ensure that the corresponding detailed privacy notices, are also in place.

8.6 Where personal information requires to be shared with other parties (eg Police, Health etc) best practice erquires 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.

8.7 The UK government has announced its intention to make changes to data protection legislation. The draft Data Protection and Digital Information Bill amends rather than repeals existing legislation and this is being now being considered as part of the wider legislative process. The extent of the proposed changes are not as significant as first anticipated however there will be the need to review our policies and processes in due course once the new legislation comes into force.

9. IMPROVEMENT ACTIONS

9.1 The Information Governance team is developing relationships with other local authorities to ensure people requiring evidence to apply to the Redress scheme receive as comprehensive a response as possible.

9.2 The online data protection training for all staff is being reviewed and refreshed and will be available during 2022-23.

9.3 The DPO is exploring the possibility of a new case management system to process and report of requests for information made unde both data Protection and Freedom of Information legislation to automate processes and further enhance performance across both areas.

10. CONCLUSION

10.1 Given the breadth of local government activity and the millions of transactions involving personal data that are processed each year, no Council can state categorically that it is fully compliant with data protection legislation. It is the opinion of the DPO, however, that the Council is currently achieving a reasonable and acceptable level of compliance which is continuing to improve.

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

10.3 As a result of the ongoing impact of the global pandemic during 2021-22 ,the Council has continued to operate under different and challenging circumstances, with many staff still working from home. During that time new arrangements for communicating with citizens and providing services continued to be developed, many of which have required the attention and support of the DPO team. Work is ongoing to support the Council as it moves towards a longer term model of hybrid working.

10.4 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	30 August 2022

APPENDICES

Not applicable.

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

None.