Glasgow City Council

Data protection audit report

December 2024

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Glasgow City Council (GCC) were issued with an Assessment Notice on 28 October 2024. This was one of the outcomes of an investigation into GCC's failure to respond to subject access requests (SAR), within statutory timescales. Low response rates had led to a number of complaints being received by the ICO. The Assessment Notice required GCC to participate in a wider audit to establish if there are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data. The purpose of the audit is to provide the Information Commissioner and GCC with an independent assurance of the extent to which GCC is complying with this area of data protection legislation.

The Assessment Notice was carried out between 9-13 December 2024.

The ICO tailored the controls covered in the scope of the Assessment Notice to take into account the organisational structure of GCC and the nature and extent of the GCC's processing of personal data. As such, the scope of this audit is unique to GCC.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, remote interviews with selected staff, and a virtual review of evidential documentation.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist GCC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. GCC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Background to the Processing of SARs at GCC

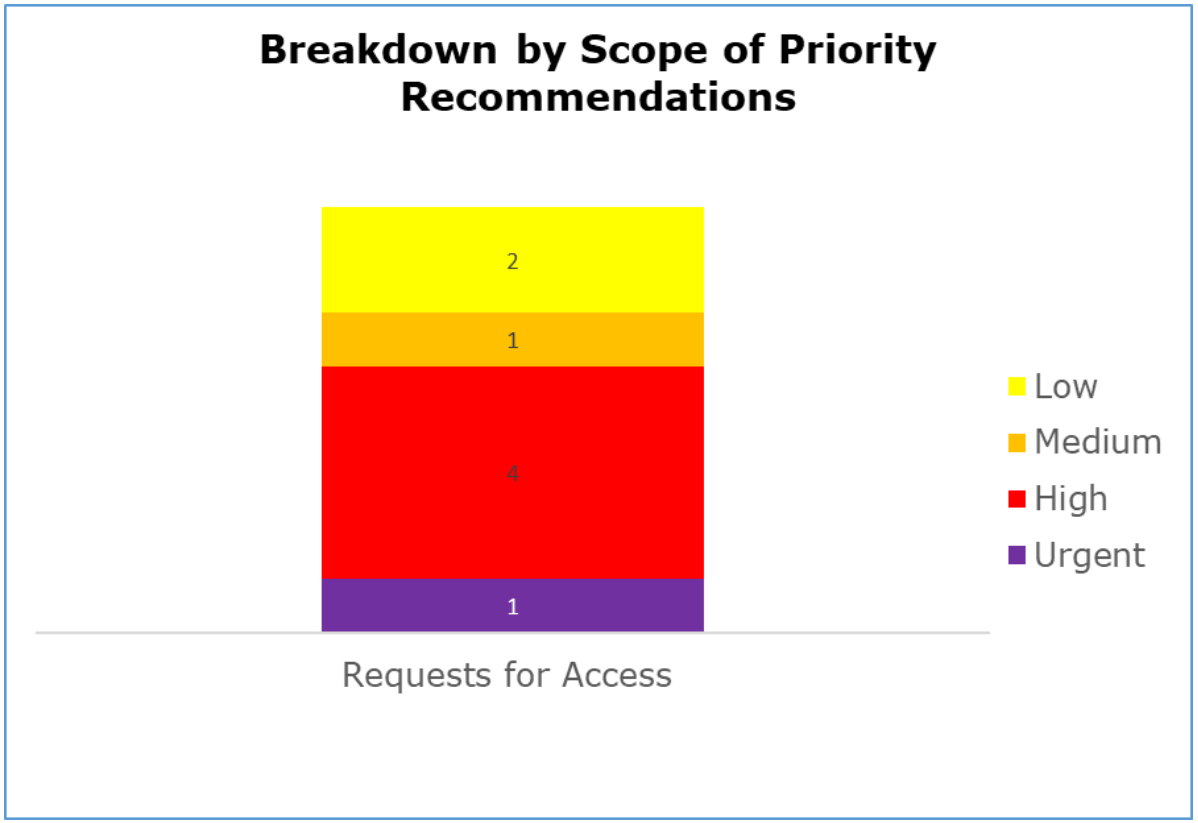
GCC is the local authority for approximately 620,000 people currently. However, the number of people whose personal data is processed will be much greater when including previous residents. In the previous 12 months GCC have received 1368 SARs. These will be managed by one of three areas:

1. Financial Services (FS). SARs are tracked by admin support staff who log requests and direct them to individual services within the FS directorate where the information requested will be held. The service will have responsibility for collating the information and providing a response to the requestor. This area received 54 SARs over the last 12 months and has high rate of responses issued within statutory timescales.

2. The Health and Social Care Partnership (HSCP). The Complaints, FOI and Investigations Team (CFIT) in HSCP are responsible for handling SARs. GCC's current poor response rate and subsequent backlogs of requests that led to the Assessment Notice are confined to this area. It was reported that the issues are primarily due to Scotland's Redress Scheme for survivors of historical child abuse in care in Scotland, which has generated much higher volumes of requests. In addition, a higher proportion of records requested are made up of physical documents which are held in offsite storage. This generated a large backlog during the COVID pandemic when this storage facility was closed for a period of time. Finally, the time needed to collate a response is higher than normal due to the amount of sensitive information contained in these records which requires more careful consideration for exemptions and redactions, as well as additional time to create electronic copies.
   CFIT largely follow the same processes for handling SARs as the other areas although have supplementary procedures to account for the handling of physical records and the nature of the information. CFIT have received 972 SARs over the previous 12 months.

3. Information and Data Protection Team (IDPT). This is a centralised team handing SARs for the Chief Executives' Department, the Neighbourhoods, Regeneration and Sustainability Department (NRS), Education Services as well as requests which relate to the Council as a whole. They also manage SARs on behalf of Glasgow Life however, whilst these follow the same processes they are logged separately and do not form part of GCC's own SAR performance figures. IDPT have received 342 requests over the previous 12 months and have high response rates within statutory timescales.

Priority Recommendations



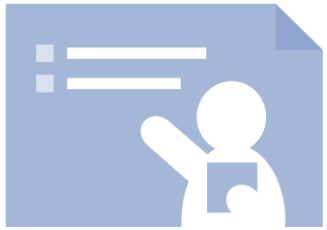
The bar chart above shows a breakdown of the priorities assigned to our recommendations. It contains 1 urgent, 4 high, 1 medium and 2 low priority recommendations.

Areas for Improvement

There is a reasonable level of assurance that processes and procedures are in place and capable of delivering data protection compliance where request volumes fall within available resource limitations. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation. These include:

- GCC should ensure all internal guidance and procedure documents are updated to include current practice and where helpful more detailed processes for certain tasks, for example ID verification, to maintain consistency and resilience in teams that manage SARs.
- GCC should update external facing guidance so that members of the public are informed of all the ways they are able to exercise their right to access their information.
- GCC should ensure that information advising staff about how to recognise SARs and what to do should they receive one is always included in mandatory annual training.
- GCC must take all reasonable steps, including further evaluation of technical and organisational measures, to ensure they are able to meet statutory response timescales.

Appendices



Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Glasgow City Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Glasgow City Council. The scope areas and controls covered by the audit have been tailored to Glasgow City Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.