ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	23 November 2023
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Internal Audit Report AC2406 – Data Protection
REPORT NUMBER	IA/AC2406
DIRECTOR	N/A
REPORT AUTHOR	Jamie Dale
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on Data Protection.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. CURRENT SITUATION

3.1 Internal Audit has completed the attached report which relates to an audit of Data Protection.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. ENVIRONMENTAL IMPLICATIONS

6.1 There are no direct environmental implications arising from the recommendations of this report.

7. RISK

7.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are detailed in the resultant Internal Audit reports. Recommendations, consistent with the Council's Risk Appetite Statement, are made to address the identified risks and Internal Audit follows up progress with implementing those that are agreed with management. Those not implemented by their agreed due date are detailed in the attached appendices.

8. OUTCOMES

8.1 There are no direct impacts, as a result of this report, in relation to the Council Delivery Plan, or the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place.

8.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

9. IMPACT ASSESSMENTS

Assessment	Outcome
Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required

10. BACKGROUND PAPERS

10.1 There are no relevant background papers related directly to this report.

11. APPENDICES

11.1 Internal Audit report AC2406 – Data Protection

12. REPORT AUTHOR CONTACT DETAILS

Name	Jamie Dale
Title	Chief Internal Auditor
Email Address	Jamie.Dale@aberdeenshire.gov.uk
Tel	(01467) 530 988

Internal Audit

Assurance Review of Data Protection

Status: Final
Date: 17 October 2023
Risk Level: Corporate

Report No: AC2406
Assurance Year: 2023/24

Net Risk Rating	Description	Assurance Assessment
Minor	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	Substantial

Report Tracking	Planned Date	Actual Date
Scope issued	14-Jun-23	14-Jun-23
Scope agreed	23-Jun-23	30-Jun-23
Fieldwork commenced	03-Jul-23	03-Jul-23
Fieldwork completed	21-Jul-23	14-Sep-23
Draft report issued	11-Aug-23	20-Sep-23
Process owner response	01-Sep-23	11-Oct-23
Director response	08-Sep-23	17-Oct-23
Final report issued	15-Sep-23	17-Oct-23
Audit Committee	23-Nov-23	

Distribution	
Document type	Assurance Report
Director	Gale Beattie, Director - Commissioning
Process Owner	Catriona Sim, Data Protection Officer
Stakeholder	Martin Murchie, Chief Officer – Data and Insights
	Caroline Anderson, Information and Data Manager
	Susan Sim, Information Governance Officer
	Sandie Scott, People Development Manager
	Alice Goodrum, Customer Feedback & Access to Information Ops Lead
	Deirdre Nicolson, Solicitor
	Sarah Clubley, Solicitor
	Lindsay MacInnes, Interim Chief Officer – People & Organisational Development*
	Vikki Cuthbert, Interim Chief Officer - Governance*
***Final only**	Jonathan Belford, Chief Officer - Finance*
	External Audit*
Lead auditor	Lyndsay Jarvis, Auditor

1 Introduction

1.1 Area subject to review

The General Data Protection Regulation (GDPR) and most of the provisions of the Data Protection Act 2018 (the 2018 Act) came into force on 25 May 2018. Upon the UK's exit from the European Union the EU GDPR was replaced domestically by the UK GDPR; the key principles, rights and obligations remain the same.

The UK GDPR regulates the processing of personal data from which a living individual could be identified. Processing of data includes collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, combining with other data, restriction, erasure, or destruction. The UK GDPR applies to any computerised or manual records containing personal information about living and identifiable people and requires that appropriate technical and organisational measures are taken to ensure compliance with the Regulation.

No personal data may be processed unless the Data Controller (organisation alone or jointly with others, determining the purposes and means of processing of personal data e.g., the Council) has identified an appropriate legal basis or bases, which meets the requirements of the UK GDPR. The legislation includes accountability and transparency requirements, rights for individuals in relation to their own personal data, and penalties can be issued by the UK Regulator, the Information Commissioner's Office (ICO) for breaching the requirements of the Data Protection legislation up to a maximum of €20 million or 4% of turnover. For instance, in November 2021, the ICO fined the Cabinet Office £500,000 for disclosing postal addresses of the 2020 New Year Honours recipients online.

The UK GDPR sets out seven principles:

1. Lawfulness, fairness, and transparency (privacy notices)
2. Purpose limitation (personal data collected for specific, explicit, and legitimate purposes)
3. Data minimisation (personal data should be adequate, relevant, and limited)
4. Accuracy (personal data should be accurate and kept up to date)
5. Storage limitation (do not retain for longer than necessary for purpose collected)
6. Integrity and confidentiality (security of personal data)
7. Accountability (must have measures and records to demonstrate compliance)

Under the UK GDPR an individual has eight defined rights in relation to the processing of their personal data:

1. The right to be informed (privacy notices)
2. The right of access (subject access)
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

1.2 Rationale for review

The objective of this review is to ensure the Council has adequate arrangements in place, which are understood throughout the organisation, to protect the Council's information.

The area was last audited in 2018 and arrangements were found to be adequate based on training; data protection impact assessments; records of processing activities; data breach monitoring; data retention guidance; freedom of information requests; postage guidance and confidential waste arrangements.

In order to enhance controls, Governance agreed to establish detailed procedures relating to individual's rights to data portability, and automated decision making and profiling. Other recommendations were made to update certain forms and notices, to review Information Sharing Agreements and data processor contracts, and to update the Surplus Property procedures to require documents containing personal data to be removed from vacated premises.

1.3 How to use this report

This report has several sections and is designed for different stakeholders. The executive summary (section 2) is designed for senior staff and is cross referenced to the more detailed narrative in later sections (3 onwards) of the report should the reader require it. Section 3 contains the detailed narrative for risks and issues we identified in our work.

2 Executive Summary

2.1 Overall opinion

The full chart of net risk and assurance assessment definitions can be found in Appendix 1 – Assurance Scope and Terms. We have assessed the net risk (risk arising after controls and risk mitigation actions have been applied) as:

Net Risk Rating	Description	Assurance Assessment
Minor	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	**Substantial**

The organisational risk level at which this risk assessment applies is:

Risk Level	Definition
Corporate	This issue / risk level impacts the Council as a whole. Mitigating actions should be taken at the Senior Leadership level.

2.2 Assurance assessment

The level of risk is assessed as **MINOR**, with the control framework deemed to provide **SUBSTANTIAL** assurance over the Council's approach to data protection.

The following governance, risk management and control measures were sufficiently robust and fit for purpose:

- **Governance Arrangements** – The Council is registered with the ICO and, in line with ICO best practice, has a full-time Data Protection Officer (DPO). Data entity-based Data Forums are meeting monthly and are attended by Information Asset Owners, Chief Officers from relevant Clusters and representatives from the Information and Data Governance Office. In addition, the Information Governance Group (IGG), chaired by the Senior Information Risk Owner (the Interim Chief Officer – Governance) is meeting quarterly to consider relevant information governance performance and compliance matters. Furthermore, AR&SC is receiving annual assurance over data protection and information security trends, issues, incidents, and breaches via the annual information governance management report, most recently in September 2023.
- **Incident Response Handling** – Eight data breach incidents reviewed were managed in accordance with procedure, with prompt reporting to the DPO, incidents were fully recorded and investigated, and subsequent reporting to the ICO took place where appropriate. Lessons had been learned and improvement action was taken as required.
- **Procurement and Contract Management** – Comprehensive guidance is in place on when and how Data Protection Impact Assessments (DPIAs) should be carried out during the procurement process, and DPIAs were in place for systems reviewed during audit testing. The Council's standard contractual terms and conditions cover data protection legislation requirements relating to data processors. In addition, Governance has advised that all new Council contracts since the introduction of the General Data Protection Regulation (GDPR) in May 2018 cover relevant data protection terms and conditions.

However, the review identified some areas of weakness where enhancements could be made to strengthen the framework of control, specifically:

- **Staff Policies, Procedures and Training** – Whilst the Council has a suite of Data Protection policies and procedures, most of the documents are past the stated due date for review and some contain obsolete advice and links e.g. reference to obsolete Information Security Officer

post, intranet site and online training platform. A mandatory training course required to be completed annually is in place however the course is not being completed annually as required (compliance rate 35%) indicating Service Managers and line managers are not monitoring training completion. As a result, this has been included on the Council's Performance Board agenda. The ability to report current completion rates at the level of individual staff has recently been added as a report within the Council's Manager's Portal, as a result the Performance Board is now receiving this data regularly and considering how to improve completion rates. Separately, all data sharing agreements are not currently published on the staff intranet, contrary to guidance in the Corporate Information Handbook. These issues reduce assurance over staff understanding of data protection requirements generally and data sharing obligations, increasing the risk of data breaches and inappropriate action in the event of a breach, risking ICO enforcement action and reputational damage.

- **Privacy Notices** – All data processing tasks reviewed had associated privacy notices. However, two (66%) of three paper application forms reviewed did not include the full text of the privacy notice meaning reasons for processing personal data were not being adequately conveyed to users without internet access. Three (60%) of five forms reviewed requesting special category data and one (50%) of two forms requiring criminal conviction data did not provide the necessary legal justifications required by UK GDPR Article 9 and Article 10 respectively. Customers are therefore being inadequately informed of the need for personal data, increasing the risk of ICO enforcement action and reputational damage.

- **Subject Access Requests** – The statutory response times for responding to subject access requests is between one and three months depending on the complexity of the information being requested however the Council is not meeting its targets. Compliance with statutory deadlines in 2022/23 was 68% for subject access requests, with subject access response times down from 77% in 2021/22. Failure to respond within statutory deadlines risks reputational damage for the Council.

Recommendations have been made to address these risks, including reviewing, and updating policies and procedures and improving their accessibility, reviewing accessibility arrangements for hard copy privacy notices, improving mandatory training completion rates through Service Manager and line manager monitoring and publishing data sharing agreements. Subject access request performance was reported to AR&SC in September 2023 as part of the annual information governance management report and action is already being taken to improve response times via a review of procedures, roles and responsibilities, and delivery of training.

2.3 Management response

The Council's Data Protection Officer (DPO) welcomes the improvements identified by the Internal Audit team. In line with the DPO's statutory role to advise the Council on data protection and monitor the Council's compliance, the DPO team will continue to support Information Asset Owners in managing data in line with data protection legislation including ensuring their customers are informed about how and why their data is used by the Council.

3 Issues / Risks, Recommendations, and Management Response

3.1 Issues / Risks, recommendations, and management response

Ref	Description	Risk Rating	Minor
1.1	**Policies, Procedures and Training** – Comprehensive written procedures and their effective communication are an essential element in any system of control. This is the same for training provided to users. This is particularly important in the case of data protection due to the Council's legal obligations to process personal data appropriately. Policies and Procedures Comprehensive policies and procedures governing data protection and information security matters are in place, including the Corporate Information Policy and Corporate Information Handbook (as referred to in the Corporate Information Policy), which cover data processing obligations generally, the Information Asset Owner Handbook, for staff responsible for managing data within systems, and the Information Security Incident Playbook and Reporting Procedure, for managing data protection, cyber security, and any other information security incidents. The documents all contain version control with dates for review. However, all are past due for review. The Corporate Information Policy and Handbook should have been reviewed in July 2021 and January 2021 respectively but were not. In addition, the Handbook is still titled the "Managing Information Handbook" instead of Corporate Information Handbook as per the Corporate Information Policy, and contains obsolete references, for example directing readers to the old staff intranet "the Zone". The Information Asset Owner Handbook was due for review in May 2019 but was not and refers to the training portal OIL which is no longer in use. The Information Security Incident Reporting Procedure should have been reviewed in May 2019 but was not and directs staff to contact the Information Security Officer, however this role no longer exists. In addition, the Playbook was amended in December 2021 but is still in draft form. If guidance is not kept up to date, there is a risk that activities undertaken by staff will not be compliant with current legislation or Council policies. Training There is one mandatory training course covering data protection, "Information Governance", and two optional courses on Cyber Security and Freedom of Information Requests. The Information Governance course is comprehensive and up to date. All employees are required to complete this course and complete a refresh every twelve months. Information Governance training, like all mandatory training is being monitored by the People Development team using the Managers Portal and reported and reviewed monthly at Employee Data Forum (Data & Insights and P&OD). However, the annual completion compliance rate across the Council is poor (35% as at 11 October 2023) and as a result this has been included on the Council's Performance Board agenda. The ability to report current completion rates at the level of individual staff has recently been added as a report within the Council's Manager's Portal, as a result the Performance Board is now receiving this data regularly and considering how to improve completion rates. People and Organisational Development advised that service managers are expected to access the Managers Portal on a regular basis to monitor compliance with mandatory training requirements, but that some managers may be unaware of this responsibility based on completion rates. Separately, the CR&D process is scheduled to be updated to include a	Risk Rating	Minor

Ref	Description	Risk Rating	Minor
	self-declaration by employees on mandatory training completion which will require line manager sign off helping to address this. The Council's Data Protection Officer advised that while the monitoring of mandatory training is a line management responsibility, the Council's Data Protection Officer, as part of the incident handling process, seeks assurance that individuals and or teams have completed their training. In addition, the Council's Data Protection Officer issues regular blogs, which included a reminder about completing Information Governance training in March 2023. Monitoring arrangements have been established and are about to be improved. However if course completion rates are inadequate, there is a greater risk that staff will not comply with data protection legislation and the Council may be found liable for data breaches by the ICO, risking financial penalties and reputational damage. Recommendations have been made to track progress with planned improvements.		
	IA Recommended Mitigating Actions a) Policies and procedures should be reviewed and updated where necessary. b) People and Organisational Development should formalise guidance for Service Managers on the use of the Managers Portal and implement the CR&D development on mandatory training self-declaration.		
	Management Actions to Address Issues/Risks *a) A review and update of policies and procedures had commenced prior to the audit. As per existing governance arrangements, any significant changes to the Policy will require to be approved by the Risk Board and thereafter committee. It is not expected that the changes will be deemed significant. As per existing governance arrangements, the updated Corporate Information Handbook will need to be approved by the Information Governance Group. The action to review and update will be completed by 31 March 2024.* *b) Agreed.*		

Risk Agreed	Person(s)	Due Date
a) Yes	a) Data Protection Officer	a) March 2024
b) Yes	b) People Development Manager	b) March 2024

Ref	Description	Risk Rating	Moderate
1.2	**Privacy Notices** – In accordance with UK GDPR Article 13, where personal data relating to a data subject is collected, the Council uses privacy notices to explain: 4 the purposes of processing 5 the legal basis for processing 6 the data subjects' rights in relation to their personal data held by the Council 7 data sharing with any other parties 8 any automated decision making or profiling using the personal data 9 the retention period 10 the contact details of the Data Protection Officer (DPO).		

Ref	Description	Risk Rating	Moderate
	Staff guidance on identifying the need for Privacy Notices (PNs), is comprehensive and clear. A sample of ten application forms for public use were selected and reviewed to confirm that processing complies with guidance and legislation, including the use PNs. Aberdeen City Council's approach to privacy notices is customer focussed with more than 300 notices available on the Council's website. <u>Accessibility</u> While PNs are available for all the tasks reviewed, two (66%) of three hard copy application forms (Housing Benefit / Council Tax Reduction application; and Council Tax Severe Mental Impairment Discount / Exemption application) reviewed did not include the full PN but instead had a typed-out web page address where the PN could be found. The Data Protection Officer advised that the Council encourages a "digital first" approach, however there are service users who do not have or cannot use digital devices and therefore have not been given sufficient access to the PN. <u>Special Category and Criminal Conviction Data</u> UK GDPR requires additional protection measures for sensitive "special category data" such as data revealing political opinions, religious beliefs, and sexual orientation, as well as personal data relating to criminal convictions and offences or related security measures. The latter covers information about offenders or suspected offenders in the context of criminal activity, allegations, investigations, and proceedings. The required legal bases for processing special category and criminal convictions personal data are set out in Article 9 and Article 10 of the UK GDPR respectively. Five (50%) of the tasks reviewed included special category data (Housing Benefit/Council Tax Reduction application [sexual orientation / racial or ethnic origin / health]; Council Tax Severe Mental Impairment application [health]; Free School Meals application [racial or ethnic origin / health]; School Place application [religious or philosophical beliefs]; Blue Badge application [health]). Two (20%) (Housing Benefit/CTR and Personal License to Sell Alcohol) also involved processing of data on criminal convictions. However, the privacy notices for three (60%) of these (Housing Benefit/CTR; CT SMI; School Place application) did not include the required justification under Article 9 for processing special category data and one (50%) of those requiring criminal conviction data (Housing Benefit/CTR) did not provide justification under Article 10. Data processing involving special category data and criminal offence data must have a legal basis that complies with UK GDPR and this must be explained to the affected Council customers or the Council may be found in breach of Data Protection legislation, risking ICO enforcement action and reputational damage.		
	IA Recommended Mitigating Actions a) Privacy notices should be reviewed to ensure special category and criminal conviction data processing is adequately justified. b) The Service should ensure hard copy privacy notices are available where necessary.		
	Management Actions to Address Issues/Risks *a) As there is a delegated Policy in place for the management of the Council's information, Information Asset Owners are responsible for ensuring privacy notices are in place and available where necessary. There are over 600 active privacy notices with over 300 customer facing notices published on the Council website, with updates and new privacy notices coming online to accommodate changes in policy and legislation. Employee related notices are published on the Council's People Anytime site. The Data Protection Officer will support the review and as appropriate the update of privacy notices through reminders directly to Information Asset Owners and through the Data Forums.*		

Ref	Description	Risk Rating	Moderate
	b) Where application forms are printed in large batches there is the risk that the privacy notice will become out of date before new batches are printed. In order to ensure customers can access the most up to date privacy information, often service areas refer customers to the Council's website. Where necessary, hard copy privacy notices are available upon request. The Data Protection officer will support Information Asset Owners to adhere to data protection obligations to communicate with customers about customers' rights and how and why we use customer data.		

Risk Agreed	Person(s)	Due Date
Yes	Chief Officer – Data & Insights / Information Asset Owners	October 2024

Ref	Description	Risk Rating	Minor
1.3	**Data Sharing Arrangements** – Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities. ICO guidance indicates that whilst it is not mandatory to establish Data Sharing Agreements (DSA), it is good practice to do so. The Council's procedure for identifying the need for a DSA is held in the Corporate Information Handbook and summarised on the Data Protection internal SharePoint site. The Handbook states that all signed off agreements must be updated on the data sharing agreement register (the register). D&I has advised that guidance on publishing has changed however these arrangements are yet to be formalised. Three DSAs are currently published in the Data Protection SharePoint site. The linked documents are complete, with all parties listed and version control details included. However, the data sharing agreement register included 135 complete data sharing agreements. If DSAs are not adequately published this risks staff being unaware of data sharing arrangements, risking a data breach, and associated reputational damage.		

IA Recommended Mitigating Actions

Council Data Sharing Agreement requirements should be formalised to ensure DSAs are made available to relevant staff.

Management Actions to Address Issues/Risks

In line with the Corporate Information Policy, Information Asset Owners are responsible for ensuring that they have the correct procedures, training and awareness in place for staff who have access to their information assets. This includes ensuring staff are aware of and are confident with the specific sharing arrangements in their business area. The Data Protection Officer will formalise the guidance in the updated Corporate Information Handbook on publishing DSAs and will remind Information Asset Owners of their responsibility to ensure staff are aware of and have access to the specific data sharing arrangements that relate to the work they do.

Risk Agreed	Person(s)	Due Date
Yes	Chief Officer – Data & Insights	March 2024

4 Appendix 1 – Assurance Terms and Rating Scales

4.1 Overall report level and net risk rating definitions

The following levels and ratings will be used to assess the risk in this report:

Risk level	Definition
Corporate	This issue / risk level impacts the Council as a whole. Mitigating actions should be taken at the Senior Leadership level.
Function	This issue / risk level has implications at the functional level and the potential to impact across a range of services. They could be mitigated through the redeployment of resources or a change of policy within a given function.
Cluster	This issue / risk level impacts a particular Service or Cluster. Mitigating actions should be implemented by the responsible Chief Officer.
Programme and Project	This issue / risk level impacts the programme or project that has been reviewed. Mitigating actions should be taken at the level of the programme or project concerned.

Net risk rating	Description	Assurance assessment
Minor	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	**Substantial**
Moderate	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	**Reasonable**
Major	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	**Limited**
Severe	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	**Minimal**

Individual issue / risk	Definitions
Minor	Although the element of internal control is satisfactory there is scope for improvement. Addressing this issue is considered desirable and should result in enhanced control or better value for money. Action should be taken within a 12 month period.
Moderate	An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on the audited area's adequacy and effectiveness. Action should be taken within a six month period.
Major	The absence of, or failure to comply with, an appropriate internal control, such as those described in the Council's Scheme of Governance. This could result in, for example, a material financial loss, a breach of legislative requirements or reputational damage to the Council. Action should be taken within three months.
Severe	This is an issue / risk that is likely to significantly affect the achievement of one or many of the Council's objectives or could impact the effectiveness or efficiency of the Council's activities or processes. Examples include a material recurring breach of legislative requirements or actions that will likely result in a material financial loss or significant reputational damage to the Council. Action is considered imperative to ensure that the Council is not exposed to severe risks and should be taken immediately.

5 Assurance review scoping document

5.1 Area subject to review

The General Data Protection Regulation (GDPR) and most of the provisions of the Data Protection Act 2018 (the 2018 Act) came into force on 25 May 2018. Upon the UK's exit from the European Union the EU GDPR was replaced domestically by the UK GDPR; the key principles, rights and obligations remain the same.

The GDPR regulates the processing of personal data from which a living individual could be identified. Processing of data includes collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, combining with other data, restriction, erasure, or destruction. The GDPR applies to any computerised or manual records containing personal information about living and identifiable people and requires that appropriate technical and organisational measures are taken to ensure compliance with the Regulation.

No personal data may be processed unless the Data Controller (organisation alone or jointly with others, determining the purposes and means of processing of personal data e.g. the Council) has identified an appropriate legal basis or bases, which meets the requirements of the GDPR. The legislation includes accountability and transparency requirements, rights for individuals in relation to their own personal data, and penalties can be issued by the UK Regulator, the Information Commissioner's Office (ICO) for breaching the requirements of the Data Protection legislation up to a maximum of €20 million or 4% of turnover. For instance, in November 2021, the ICO fined the Cabinet Office £500,000 for disclosing postal addresses of the 2020 New Year Honours recipients online.

The UK GDPR sets out seven principles:

8. Lawfulness, fairness, and transparency (privacy notices)
9. Purpose limitation (personal data collected for specific, explicit, and legitimate purposes)
10. Data minimisation (personal data should be adequate, relevant, and limited)
11. Accuracy (personal data should be accurate and kept up to date)
12. Storage limitation (do not retain for longer than necessary for purpose collected)
13. Integrity and confidentiality (security of personal data)
14. Accountability (must have measures and records to demonstrate compliance)

Under GDPR an individual has eight defined rights in relation to the processing of their personal data:

c) The right to be informed (privacy notices)
d) The right of access (subject access)
e) The right to rectification
f) The right to erasure
g) The right to restrict processing
h) The right to data portability
i) The right to object
j) Rights in relation to automated decision making and profiling.

5.2 Rationale for review

The objective of this review is to ensure the Council has adequate arrangements in place, which are understood throughout the organisation, to protect the Council's information.

The area was last audited in 2018 and arrangements were found to be adequate based on training; data protection impact assessments; records of processing activities; data breach monitoring; data retention guidance; freedom of information requests; postage guidance and confidential waste arrangements.

In order to enhance controls, Governance agreed to establish detailed procedures relating to individual's rights to data portability, and automated decision making and profiling. Other recommendations were made to update certain forms and notices, to review Information Sharing Agreements and data processor contracts, and to update the Surplus Property procedures to require documents containing personal data to be removed from vacated premises.

5.3 Scope and risk level of review

This review will offer the following judgements:

- An overall **net risk** rating at the Corporate level.
- Individual **net risk** ratings for findings.

5.3.1 Detailed scope areas

As a risk-based review this scope is not limited by the specific areas of activity listed below. Where related and other issues / risks are identified in the undertaking of this review these will be reported, as considered appropriate by IA, within the resulting report.

The specific areas to be covered by this review are:

- Policy, Procedures and Training
- Governance
- Compliance with GDPR Principles
- Data Protection Impact Assessments
- Subject Access Requests
- Data Processing Agreements and Data Sharing Agreements
- Data Breaches

5.4 Methodology

This review will be undertaken through interviews with key staff involved in the process(es) under review and analysis and review of supporting data, documentation, and paperwork. To support our work, we will review relevant legislation, codes of practice, policies, procedures, guidance.

Due to hybrid working across the Council, this review will be undertaken primarily remotely.

5.5 IA outputs

The IA outputs from this review will be:

- A risk-based report with the results of the review, to be shared with the following:
    - Council Key Contacts (see 1.7 below)
    - Audit, Risk and Scrutiny Committee (final only)
    - External Audit (final only)

5.6 IA staff

The IA staff assigned to this review are:

- Lyndsay Jarvis, Auditor **(audit lead)**
- Andrew Johnston, Audit Team Manager
- Jamie Dale, Chief Internal Auditor **(oversight only)**

5.7 Council key contacts

The key contacts for this review across the Council are:

- Andy MacDonald, Director – Customer Services
- Martin Murchie, Chief Officer – Data and Insights
- Caroline Anderson, Information and Data Manager
- Catriona Sim, Data Protection Officer **(process owner)**

5.8 Delivery plan and milestones

The key delivery plan and milestones are:

Milestone	Planned date
Scope issued	14/06/2023

Milestone	Planned date
Scope agreed	23/06/2023
Fieldwork commences	03/07/2023
Fieldwork completed	21/07/2023
Draft report issued	11/08/2023
Process owner response	01/09/2023
Director response	08/09/2023
Final report issued	15/09/2023