Aberdeenshire COUNCIL Business Services

**REPORT TO AUDIT COMMITTEE – 16 SEPTEMBER 2021**

**DATA PROTECTION OFFICER ANNUAL REPORT**

## 1 Reason for Report / Summary

1.1 The Committee requested that an Information Governance report be provided on an annual basis.

## 2 Recommendations

**Audit Committee is recommended to:**

**2.1 Discuss and acknowledge the Data Protection Officer Annual Report for 2020/21.**

## 3 Purpose and Decision Making Route

3.1 Purpose

3.1.1 At a forward planning workshop, the Committee requested that an Information Governance report be provided to Committee on an annual basis. Information Governance has since been split with the Data Protection function now residing within Legal & People and the Information / Cyber Security function residing within Customer and Digital Services. The Data Protection Officer (DPO) has prepared a Data Protection Annual Report for Committee.

3.2 Decision Making Route

3.2.1 This Annual Report has not previously been considered by this or another Committee.

## 4 Discussion

4.1 The EU General Data Protection Regulation (GDPR) and Data Protection Act (2018) both came into force on 25th May 2018, increasing organisational data protection obligations, and accountability, as well as enhancing individual's data protection rights. Processes and working practices across the Council have since been adapted to ensure compliance. The UK GDPR, which replicates the EU GDPR into UK law, came into force on 1st January 2021.

4.2 The DPO produces a monthly management report for Directors outlining identified issues and concerns which are usually addressed by services. Overall, while the DPO feels the Council does not have any significant risks in this service area, there is some room for improvement, as detailed at 4.3 to 4.7.

4.3 The target percentage for completion of Data Protection Awareness Training is 90%. As of 25th May 2021, 86% of staff and Councillors have completed mandatory training. A significant majority of outstanding training is within Education & Children's Services.

Education & Children's Services, and where necessary Councillors, should take action to comply with the previously received formal undertaking from the ICO to ensure completion percentage is above 90%.

4.4 In the previous two annual reports, the DPO expressed concern that the percentage of responses issued late was too high (19% in 2018/19 and 16% in 2019/20) and that there was room for improvement. During 2020/21, 17% of responses were issued late thus there remains ongoing room for improvement.

Council Services must take action to increase the number of responses to requests issued on time to above 90% by ensuring Services have appropriate resource in place to meet statutory timeframes.

4.5 The number of suspected data breaches reported to the DPO, which have subsequently been confirmed by the DPO as breaches, has increased from 70 to 107, a 53% increase from the previous year. Lack of due care when using email accounts for 66% of confirmed data breaches in the past year (a 14% increase from 2019/20 and 24% increase from 2018/19). The DPO has continuing concerns with the increasing volume of email-related data breaches arising within the Council.

All Council Services should inform staff of the increasing number of arising data breaches, particularly in relation to use of email, and continue to remind staff, on an ongoing basis, of the need to take appropriate care when processing personal data and to take care when sending emails.

4.6 Several systems, with rejected DPIAs, are in continued use within the Council despite significant privacy concerns having been identified by the DPO, the Legal Commercial Team and/or the Information Security Officer.

Where a DPIA has been rejected due to significant privacy concerns, the Council should be actively addressing concerns. Where this is not possible, the DPO strongly recommends ceasing processing.

4.7 Several long-outstanding DPIAs, highlighted in the previous annual report, have been completed during the past year with only a few now outstanding for more than one year. These outstanding DPIAs warrant appropriate prioritisation by Services.

All Council Services should ensure DPIAs are undertaken, when necessary, and ensure DPIAs are seen through to completion.

## 5 Council Priorities, Implications and Risk

5.1 The report helps deliver Council Priority 10 – Having the right people, in the right place, doing the right thing, at the right time.

5.2 The table below shows whether risks and implications apply if the recommendation(s) is(are) agreed.

| Subject | Yes | No | N/A |
|---|---|---|---|
| Financial | | | X |
| Staffing | | | X |
| Equalities | | | X |
| Fairer Scotland Duty | | | X |
| Town Centre First | | | X |
| Sustainability | | | X |
| Children and Young People's Rights and Wellbeing | | | X |

5.3 An equality impact assessment is not required because this report informs the Committee of the planned reporting activity and does not have a differential impact on any of the protected characteristics.

5.4 The following Risks have been identified as relevant to this matter on a Corporate Level:

ACORP002: Changes in legislation and regulation
ACORP006: Reputation Management
ACORP008: Data Protection and Cyber Security

## 6 Scheme of Governance

6.1 The Head of Finance and Monitoring Officer within Business Services have been consulted in the preparation of this report and are satisfied that the report complies with the Scheme of Governance and relevant legislation.

6.2 The Committee is able to consider/comment on this item in terms of Section G.1.1 of the List of Committee Powers in Part 2A of the Scheme of Governance as the report relates to matters delegated to the Committee.

**Ritchie Johnson**
**Director of Business Services**

Report by A Lawson, Principal Information Governance Officer (Data Protection Officer)
Date: 19th July 2021

**List of Appendices** –

Appendix 1: Data Protection Officer's Annual Report – May 2020 to May 2021

**APPENDIX 1**

Aberdeenshire COUNCIL

# DATA PROTECTION OFFICER'S ANNUAL REPORT

## MAY 2020 TO MAY 2021

# Table of Contents

## Foreword

During the past year, the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations which have now been fully embedded into working practices across the Council.

COVID-19 has had a significant impact on data protection resource during the past year with data sharing agreements written and Data Protection Impact Assessments (DPIAs) undertaken relating to humanitarian assistance, testing, track and trace, and vaccinations. DPIAs have also been undertaken in relation to different ways of working including virtual site visits for planning applications and bookable visits to waste recycling centres. The Data Protection Officer (DPO) has had to ensure that data protection has not been cited incorrectly as a barrier to proportionate and necessary data sharing, while of course balancing that with the continuing need to protect and secure personal data and ensure data processing remains transparent.

The past year has seen welcome improvement in the number of staff and Councillors with up-to-date Data Protection training with the overall completion rate now falling just a few percent below the Council's 90% completion target.

There remains however ongoing room for improvement in responding to access requests within statutory timeframes.

Of significant concern during the past year is a >50% increase in the number of confirmed data breaches reported to the DPO. Most of these breaches are resulting from lack of due care when sending emails.

Several DPIAs have been rejected during the past year due to identification of significant privacy concerns. Where significant concerns are identified, these should be addressed promptly to mitigate risk. Several long-outstanding DPIAs have been completed during the past year with only a few now outstanding for longer than one year. Outstanding DPIAs warrant appropriate prioritisation by Services.

It is important for the Council to continue to pay sufficient regard to Data Protection not only to ensure individuals' rights are upheld but also due to the fact enhanced enforcement powers granted to the ICO, including the power to levy a fine of £17,500,000 or up to 4% of annual global turnover, whichever is larger, have not gone away.

Andrew Lawson
Data Protection Officer

## The Role of the DPO

The General Data Protection Regulation (GDPR) requires all public authority data controllers to designate a Data Protection Officer (DPO). The DPO must be designated based on professional qualities and expert knowledge of data protection law and practices, and the ability to fulfil the statutory tasks set out in the GDPR.

The designated Data Protection Officer must directly report to the highest management level, must not receive instructions regarding the exercising of statutory tasks, and shall not be penalised or dismissed for performing those tasks. The Council must support the DPO in performing his tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations.

During the past year, Andrew Lawson has been designated substantive DPO for Aberdeenshire Council, Aberdeenshire Licensing Board, Aberdeenshire Integrated Joint Board and the Aberdeenshire Returning Officer.

## Data Protection Policy

The Council's Data Protection Policy was re-written for the GDPR and approved by Business Services Committee on 14th June 2018. The policy was last reviewed on 29th April 2021 when several minor amendments were made including post-Brexit removal of references to the EU, updated references to updated Council security policy and mandatory codes of practice, removal of the mandatory requirement to put a Data Sharing Agreement in place between partner organisations, strengthening of requirements relating to the processing of personal data outside of the EU, and clarification added as to when a Data Protection Impact Assessment needs to be undertaken.

## Data Protection Awareness

In April 2018, Data Protection awareness training was refreshed for the GDPR, and made available to staff via ALDO. Awareness training consists of six short videos and a multiple-choice assessment with an overall duration of 30 minutes.

Following a previous data breach, the Council received a formal undertaking from the Information Commissioner's Office requiring all staff to undertake data protection training and regular refresher training. The percentage at which the ICO considered this formal undertaking to be fulfilled was 90%.

As of 25th May 2021, 86% of staff and Councillors have completed mandatory training. While this is a significant improvement from 69% completion as of 2019/20, the percentage complete remains 4% below the 90% target. A significant majority of outstanding training is within Education & Children's Services.

**Education & Children's Services, and where necessary Councillors, should take action to comply with the previously received formal undertaking from the ICO.**

Data Protection Awareness Training Completion by Service:

| Service | Total number of staff required to undertake training | Total number of staff who have completed training | Total number of staff outstanding | Percentage complete |
|---|---|---|---|---|
| Business Services | 910 | 881 | 29 | 97% |
| Education & Children's Services | 11,574 | 9,638 | 1,936 | 83% |
| Health & Social Care Partnership | 2,553 | 2,298 | 255 | 90% |
| Infrastructure Services | 1,357 | 1,260 | 97 | 93% |
| Chief Executive | 5 | 5 | 0 | 100% |
| Councillors | 69 | 59 | 10 | 86% |
| Total | **16,468** | **14,141** | **2,327** | **86%** |

Stats as of 25th May 2021

## Information Rights

Under the GDPR, individuals have several rights including the right to be informed, the right to make an access request, the right to rectification, the right to erasure (the right to be forgotten), the right to restriction of processing and the right of data portability. Individuals' rights are covered within Council Data Protection Policy.

Number of valid requests received during 2020-2021:

| Right | Number received | Number of responses issued on time | Percentage of responses issued on time |
|---|---|---|---|
| Access Requests | 155 | 128 | 83% |
| Rectification Requests | 1 | 1 | 100% |
| Erasure Requests | 2 | 1 | 50% |
| Restriction of Processing Requests | 0 | 0 | N/A |

| | | | |
|---|---|---|---|
| Data Portability Requests | 0 | 0 | N/A |

In the previous two annual reports, the DPO expressed concern that the percentage of responses issued late was too high (19% in 2018/19 and 16% in 2019/20) and that there was room for improvement. During 2020/21, 17% of responses were issued late thus there remains ongoing room for improvement.

It should be noted that there has been a 29% increase in the number of Access Requests received during 2020/21 with no associated increase in Service resource. Service representatives have advised that they are struggling to respond to requests on time due to the size and complexity of requests and not having sufficient resource.

Number of valid Access Requests received by year:

| Year | Number of access requests received |
|---|---|
| 2021-2020 | 155 |
| 2019-2020 | 120 |
| 2018-2019 | 130 |
| 2017-2018 | 77 |
| 2016-2017 | 43 |

***Council Services must take action to increase the number of responses to requests issued on time to above 90% by ensuring Services have appropriate resource in place to meet statutory timeframes.***

As well as processing requests received from members of the public and staff, the Council also processes requests made under Schedule 2 of the Data Protection Act (2018), primarily from Police Scotland, seeking information held to assist with the prevention and detection of crime and the apprehension and prosecution of offenders. The number of valid Schedule 2 requests received has again decreased in the past year.

Number of valid Schedule 2 requests received by year:

| Year | Number of S2 requests received |
|---|---|
| 2020-2021 | 114 |
| 2019-2020 | 145 |

| | |
|---|---|
| 2018-2019 | 172 |
| 2017-2018 | 57 |
| 2016-2017 | 31 |

## Data Breaches

During the third year of the GDPR, the number of suspected data breaches reported to the DPO, which have subsequently been confirmed by the DPO as breaches, has increased from 70 to 107, a 53% increase from the previous year.

Number of confirmed data breaches reported by year:

| Year | Number of confirmed data breaches |
|---|---|
| May 2020 – May 2021 | 107 |
| May 2019 – May 2020 | 70 |
| May 2018 – May 2019 | 67 |
| May 2017 – May 2018 | 28 |
| May 2016 – May 2017 | 8 |
| May 2015 – May 2016 | 8 |

Almost all data breaches arise due to human error and lack of due care. Lack of due care when using email accounts for 66% of confirmed data breaches in the past year, a 14% increase from 2019/20 and 24% increase from 2018/19. The DPO has continuing concerns with the increasing volume of email-related data breaches arising within the Council.

While the DPO and the Council's Data Protection Working Group have recommended disabling email autofill, which is by far the leading contributor to email breaches to incorrect recipients, following a trial by Council Digital Champions, Digital Champions recommended leaving autofill enabled primarily due to resulting inconvenience on disabling this functionality.

Data breaches by data breach type:

| Data Breach by Type | Number of confirmed data breaches 2020/21 | Number of confirmed data breaches 2019/20 |
|---|---|---|
| Email - incorrect external recipient | 41 | 18 |
| Email - failure to use BCC | 18 | 12 |

| | | |
|---|---|---|
| Email - incorrect attachment | 12 | 6 |
| Postal mail - incorrect address | 2 | 8 |
| Postal mail - Incorrect personal data contained in letter | 4 | 5 |
| Postal mail - Mail lost in delivery (Royal Mail) | 1 | 0 |
| Inappropriate disclosure to third party (written & verbal) | 12 | 12 |
| Excessive data provided to third party | 7 | 0 |
| Loss of paper file | 3 | 1 |
| Lost unencrypted USB drive | 1 | 1 |
| Personal data uploaded into system against incorrect individual | 1 | 0 |
| Data Processor breach | 2 | 2 |
| System error | 2 | 0 |
| Upload to Social Media without consent | 1 | 2 |
| Failure to redact appropriately (FOI responses) | 0 | 1 |
| Failure to redact appropriately (other) | 0 | 1 |
| Disclosure to third party without having contract in place | 0 | 1 |
| **Total** | **107** | **70** |

Data breaches arising by Service:

| Data Breaches by Service | Number of confirmed data breaches 2020/21 | Number of confirmed data breaches 2019/20 |
|---|---|---|
| Education & Children's Services | 51 | 41 |
| Business Services | 15 | 10 |
| Health & Social Care Partnership | 24 | 6 |
| Infrastructure Services | 17 | 13 |
| **Total** | **107** | **70** |

The above breakdown by Service highlights a statistically significant and concerning 400% increase in confirmed data breaches arising within the Health & Social Care Partnership.

**All Council Services should inform staff of the increasing number of arising data breaches, particularly in relation to use of email, and continue to remind staff, on an ongoing basis, of the need to take appropriate care when processing personal data and to take care when sending emails.**

Most data breaches arising fall below the threshold for reporting to the ICO. During the third year of the GDPR, only two data breaches were deemed by the DPO to require reporting to the ICO. Further detail concerning these two data breaches can be found at Appendix 1.

## Data Protection Complaints

The Council Feedback Team administers data protection complaints on behalf of the DPO, seeking input as necessary from relevant service(s) and the DPO.

Number of formal complaints received:

| Data Breaches by Service | Number of complaints received |
|---|---|
| 2020/21 | 19 |
| 2019/20 | 9 |
| 2018/19 | 12 |

## Data Protection Impact Assessments

The GDPR introduced a requirement for Data Controllers to undertake a Data Protection Impact Assessment to help identify and minimise data protection risk where processing is likely to result in a high risk to individuals.

During 2020/21, many DPIAs were undertaken and approved including booking of Waste Recycling Centre visits, Planning Application virtual site visits, Corporate EDRMS, the Humanitarian Assistance Centre, Parents Portal, Test and Protect, Refugee Resettlement, Salary Finance, Housing Online, Brightsolid Data Centre, Vivup Employee Benefits, iTrent HR system, Covid-19 Vaccinations, Social Care Out of Hours, Engagement HQ, UK Gov Notify, Cherwell HR system, Carefirst, Xerox Hybrid Mail, Offsite Records Storage and numerous school apps.

A small number of DPIAs have been rejected due to significant privacy concerns:

SeeSaw – a system in existing use within Aberdeenshire Council schools. The supplier permits data access to 15 US-based sub-processors. The Council cannot carry out due diligence on such a high number of sub-processors.

Version 1 – despite most finance data having a retention period of seven years, data is being kept indefinitely within the Council's Finance system. Twenty two years of data is currently held. This is not compliant with the principle of keeping data only for as long as necessary.

ActiveLearn – a system in existing use within Aberdeenshire Council schools. The supplier permits companies located in India, Sri Lanka and the Philippines to access the data in order to provide support.

Microsoft 365 – used widely throughout the Council including for storage of Council records. Rejected due to IT decision to not back up M365 files but instead rely on file recovery capability provided by Microsoft going back only 30 days. Microsoft state that this "does not protect against ransomware attacks that copy files, encrypt them, and then delete the original files." There is potential for the Council to lose some or all files, including Council records, in the event of such a ransomware attack. Without backups,

the impact of a ransomware attack could be significant with recovery difficult if not impossible. Backing up files should be considered as part of a broader piece of risk mitigation around the impact of/recovery from ransomware.

ThingLink – a school app rejected due to Information Security concerns.

Several of the above systems, with rejected DPIAs, are in continued use within the Council despite significant privacy concerns having been identified by the DPO, the Legal Commercial Team and/or the Information Security Officer.

**Where a DPIA has been rejected due to significant privacy concerns, the Council should be actively addressing concerns. Where this is not possible, the DPO strongly recommends ceasing processing.**

Several long-outstanding DPIAs, highlighted in the previous annual report, have been completed during the past year with only a few now outstanding for more than one year. Outstanding DPIAs warrant appropriate prioritisation by Services. Outstanding DPIAs which were also highlighted in the previous annual report include GLOW and Caledonian System.

**All Council Services should ensure DPIAs are undertaken, when necessary, and ensure DPIAs are seen through to completion.**

## Data Sharing

During the third year of the GDPR, the DPO has reviewed and provided feedback in relation to numerous draft Data Sharing Agreements including: Castlehill Housing Association, COVID-19 Outbreak Reporting, Defra, European Structural Funds, Food Standards Scotland, Landlord Registration, LSCMI, Memex IDB, NE Suicide Review, National Entitlement Card, COVID-19 Assistance Centre, Skills Development Scotland, Transport for Vaccination Appointments, UK Community Renewal Fund and Vaccination Data Sharing.

## COVID-19

COVID-19 has had a significant impact on data protection resource during the past year with data sharing agreements written and adopted relating to humanitarian assistance, testing, test and protect, and vaccinations. Associated Data Protection Impact Assessments have also been undertaken and in relation to different ways of working including virtual site visits for planning applications and bookable visits to waste recycling centres. The DPO has had to ensure that data protection has not been cited incorrectly as a barrier to proportionate and necessary data sharing, while of course balancing that with the continuing need to protect and secure personal data and ensure data processing remains transparent.

The DPO is grateful that the practice of discouraging individuals from submitting information requests, which was highlighted as a concern in the previous annual report, has ceased.

## Brexit

Post-Brexit, the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations.

During the past year there has been considerable uncertainty as to whether the EU would grant an adequacy decision for the UK. Work was therefore undertaken within the Council to identify all EU-based processing with a view to potentially having to put Standard Contractual Clauses in place with each company in the event of no adequacy decision.

It should be noted that at the time of writing this report an adequacy decision has been granted permitting continued data flow between the UK and the EU.

## Working Groups

During the third year of the GDPR, the DPO has been an active participant in several working groups.

SOLAR Data Protection/FOI Working Group – a working group consisting of Data Protection and Freedom of Information representatives from the 32 Scottish Local Authorities. This is an extremely useful working group which discusses matters of shared concern and which is also used to share effort such that all 32 Scottish Local Authorities do not have to re-invent the same wheel. During the pandemic, this group has increased the frequency of meetings which now take place via Teams.

The Data Protection Working Group – the DPO chairs this internal group which includes Data Protection and Freedom of Information Service representatives.

## Contact the DPO

If you would like to find out more about this annual report, or provide any feedback, please contact the Data Protection Officer.

Phone: 01467 536035
Email: dataprotection@aberdeenshire.gov.uk

In writing to:
Data Protection Officer
Aberdeenshire Council
34 Low Street
Banff
AB45 1AY
Visit: https://aberdeenshire.gov.uk/online/legal-notices/data-protection/

## Appendix 1

Data Breaches reported to the ICO:

| Breach ID | Description | Outcome |
|---|---|---|
| DB70 | Two paper registers for an out of school basketball club were lost. These contained the names, class and gender of 39 pupils and contact details of 72 emergency contacts. The registers also contained information as to whether pupils were picked up or walked home from school, and medical details including e.g. poor motor skills, peanut allergies, penicillin allergies, etc.<br><br>It was suggested that these registers may have fallen out of the member of staff's bag/car and blown away into farmland. | The DPO proposed a set of recommendations which were accepted by the Service and the ICO.<br><br>No further action taken by the ICO. |
| DB87 | An email containing a sensitive attachment was sent to an incorrect external recipient. A member of staff incorrectly looked-up an email address on the internet, without confirming the address, and then sent the email without using encryption which was necessary due to the sensitivity of information. The attachment contained a significant volume of health information relating to a vulnerable individual along with his current location. | The DPO proposed a set of recommendations which were accepted by the Service and the ICO.<br><br>No further action taken by the ICO. |