East Herts Council Report

Audit and Governance Committee

Date of meeting: 31 May 2022

Report by: Tyron Suddes, Information Governance and Data Protection Manager

Report title: Data Protection Update

Ward(s) affected: All

Summary – To provide an update on data protection compliance, including data breaches and subject access requests.

RECOMMENDATIONS FOR AUDIT AND GOVERNANCE COMMITTEE:

a) **That the Committee notes the content of the report and provides any observations to the Information Governance and Data Protection Manager**

1.0 Proposal(s)

1.1 As above

2.0 Background

2.1 This report provides a regular six monthly update on data protection compliance, including the number of data breaches reported and responded to, and the number of Subject Access Requests (SARs) received in the six month reporting period.

2.2 Since the last update on the items noted in 2.1 above given on the 9th November 2021, the Information Governance and Data Protection Manager has carried out the following actions:

2.3 The Council's data processing activities and assets have uploaded onto OneTrust, a data protection and information management software. This is to allow for the automatic identification, assessment and update of the Council's data assets and processes. The software also allows for the automatic generation of the Council's latest Record of Processing Activity and Information Asset Register.

2.4 The Council's Data Protection and Information Governance Policies have been reviewed. A revised Data Protection policy has been drafted and is awaiting final approval. Training sessions will be offered to all staff on this policy once adopted with an emphasis on the recognition on data subject rights.

2.5 The Information Governance Policy will be revised jointly with Stevenage Borough Council to ensure consistent and effective information management within Microsoft 365.

2.6 An additional 10 privacy notices have been drafted and all privacy information on Council webforms is currently being reviewed.

2.7 Data Protection Impact Assessments are now being carried out using automated assessments on OneTrust. This leaner process ensures that risks are flagged, mitigated and monitored against the associated data processing activity or asset within a central platform.

2.8 Data breach training sessions were offered to staff which aimed to increase staff awareness of reporting a suspected breach and to share learning from past breaches within the Council and those reported to the Information Commissioner's Office. 179 staff members attended these sessions.

2.9 As part of a regular data protection update, the committee requested an update on data breaches and SARs.

2.10 There have been 9 reported breaches from the 26th October 2021 to the 30th April 2022, none of which posed a likely risk to data subjects

and were therefore not reported to the Information Commissioner's Office (ICO) or to the data subjects.

2.11 Of the nine reported breaches, eight were caused by human error whereby:

2.11.1 A register of electors was attached to a Myview claim in error
2.11.2 An email was sent to a housing association with incorrect customer details
2.11.3 A document was insufficiently redacted before publication
2.11.4 Four emails were sent to incorrect recipients
2.11.5 A letter was sent to an incorrect recipient

2.12 One breach was caused by a software error which resulted in a number of invitations to register being addressed to electors at an incorrect address.

2.13 Where breaches were due to human error, the following action(s) were taken:

2.13.1 The register was immediately deleted from Myview and the Councillor responsible was contacted by the Data Protection Officer and reminded of the serious implications had the data been more widely breached and of the limited uses of the register. The register cover sheet, which covers onward use of elector data, is currently being reviewed. Additionally, data breach training will be offered to Councillors.
2.13.2 The incorrect recipients of data, including the housing association, were asked to permanently destroy the data and confirm once done.
2.13.3 Staff were reminded to ensure sufficient redaction before sharing.
2.13.4 The Information Governance and Data Protection Manager is currently investigating a trial of Egress which uses machine learning to prompt users to check whether emails are being sent to the correct recipient. Microsoft 365 has a similar feature which will be trailed alongside Egress to identify the

best and most cost effective solution to implement to reduce the amount of breaches caused by human error.

2.14 Where a breach had occurred due to a software issue, the elections team have now taken steps with the software provider to address the issue and will ensure that data is checked and cleansed before importing and that data is spot checked following this.

2.15 The number of reported data breaches has increased from five in the previous reporting period to nine in the current, however, this may due to a greater understanding and awareness of data breach reporting following data breach training. Additionally, learning and actions taken following any breach are noted and shared with all staff via a data protection best practice page to prevent breaches of a similar nature occurring in future.

2.16 There have been two SARs received from the 26th October 2021 to the 30th April 2022. One request was provided in full and the other was part provided as some of the personal data formed part of a Monitoring Officer investigation and was therefore exempt under the Data Protection Act 2018.

3.0 Reason(s)

3.1 The Audit & Governance Committee has within its terms of reference; to provide an effective mechanism to monitor the control environment within the council, ensuring the highest standards of probity and public accountability by challenging and following up internal audit recommendations.

4.0 Options

4.1 The Committee requested an update and so there are no alternative options to consider

5.0 Risks

5.1 Data breaches can pose a financial and reputational risk to the council if they are not reported and dealt with correctly, however, the council, through e-learning and virtual classroom training and updated policies and procedures has limited the amount of breaches. Additionally, through regular reporting of breaches, the council is able to identify trends and possible actions to prevent these reoccurring.

5.2 Similarly, subject access requests, if not responded to correctly and within the statutory one month time frame, can pose financial and reputational risks to the council. This report provides reassurance that the council continues to respond to these requests in line with legislation.

6.0 Implications/Consultations

6.1 None

Community Safety

No

Data Protection

Yes – regular updates on data protection aim to provide assurance that the council remains complaint with data protection legislation. Equally, updating on data breaches and subject access requests provides assurance that the council remains compliant in these areas.

Equalities

No

Environmental Sustainability

No

Financial

No

Health and Safety

No

Human Resources

No

Human Rights

No

Legal

None, other than as identified above.

Specific Wards

No

7.0 Background papers, appendices and other relevant material

7.1 None

Contact Member

Councillor George Cutting – Executive Member for Corporate Services
George.Cutting@eastherts.gov.uk

Contact Officer

Tyron Suddes
Information Governance and Data Protection Manager
Tyron.Suddes@eastherts.gov.uk

James Ellis
Head of Legal and Democratic Services
01279 502170
James.Ellis@eastherts.gov.uk

Report Author

Tyron Suddes
Information Governance and Data Protection Manager
Tyron.Suddes@eastherts.gov.uk