East Herts Council Report

Audit and Governance Committee

Date of meeting: 9 November 2021

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 and information governance 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 27th May 2021, the Information Governance and Data Protection Manager has carried out the following actions:

2.3 The data mapping exercise is near completion and the information gathered through the exercise has been used to update the Council's Record of Processing Activity (ROPA) and Information Asset Register (IAR).

2.4 Additionally, the mapping exercise information is being uploaded to OneTrust, a data protection and information governance 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 ROPA and IAR.

2.5 The Council's Access to Information, Data Breach and Data Retention Policies have been approved and adopted. The associated procedural documents, including the data breach notification process, have been reviewed and revised in line with these policies. These have been communicated with all staff and are available on the Council's intranet. The Council's Data Protection and Information Governance Policies are currently being reviewed.

2.6 Sixteen privacy notices have been reviewed and revised, including the Council's Corporate and Staff Privacy Notices.

2.7 The Council's Data Protection Impact Assessment (DPIA) process is has been reviewed and replaced with OneTrust's

automated DPIA process to allow for a simpler and less time consuming process.

2.8 The Council's mandatory Data Protection e-learning course has been reviewed and three training sessions have been held with council staff to ensure an understanding of the requirements of the Access to Information, Data Breach and Data Retention policies. A total of 124 council staff 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 a total of 5 reported breaches from the beginning of May 2021 to end of October 2021, one of which was deemed serious enough to be reported to the Information Commissioner's Office (ICO) as, although it was unlikely the risks of the breach would be realised, the number of data subjects affected posed a high risk. This breach was caused by a ransomware attack on Gallagher Bassett, one of the Council's data processors, whereby limited data including name, address and insurance claim information (not including any payment or banking details) was compromised. Gallagher Bassett had put actions into place to reduce the level of risk including offering notifiable individuals identity theft protection and monitoring services. The ICO took no further action and was satisfied with the actions both the Council and processor put in place. The ICO also found that the Council had sufficiently ensured that the processor acted in a manner that meets the security requirements of the UK GDPR.

2.11 The other 4 minor breaches were caused by human error whereby:

2.11.1 An email was sent to an unintended recipient;
2.11.2 Personal data was insufficiently redacted.

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

2.12.1 Recipients who had received personal data incorrectly via email where asked to delete the data and confirm once complete;
2.12.2 Where personal data had been published this was immediately removed;
2.12.3 Staff responsible for the breach were reminded of the serious implications of a data breach, to take more care in future and were advised to re-take the data protection e-learning course;
2.12.4 Staff were advised to clear the autocomplete cache in Outlook;
2.12.5 The data protection best practice page was updated to reflect lessons learnt and this was communicated with all staff.

2.13 Keeping in mind that the amount of personal data that the council processes every day through communications, emails, online accounts and applications is high, the amount of reported breaches that occurred over the last six month period is relatively low. Additionally, the number of reported data breaches has reduced from 20 during the previous

reporting period (November 2020 – April 2021) to 5 during the current reporting period (May 2021 – October 2021).

2.14 There have been a total of 4 SARs received from the beginning of May 2021 to the end of October 2021. All requests were provided in full and a response was given within the one month time limit.

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 online training and updated policies and procedures has limited the amount of medium to high risk breaches. Additionally, through regular reporting of lower risk 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