TEWKESBURY BOROUGH COUNCIL

Report to:	Audit and Governance Committee
Date of Meeting:	15 December 2021
Subject:	Data Protection Officer Annual Report
Report of:	Head of Corporate Services
Corporate Lead:	Borough Solicitor
Lead Member:	Lead Member for Corporate Governance
Number of Appendices:	One

Executive Summary:

This report provides the Committee with the Data Protection Officer's assessment of the Council's general activity during the year to ensure broad compliance with the General Data Protection Regulation (GDPR). The role of the Data Protection Officer is to monitor compliance by the Data Controller of GDPR legislation. It is a statutory role fulfilled by the Borough Solicitor. The Data Controller (the Chief Executive) has a duty to comply with GDPR legislation. A Single Point of Contact (SPoC) for GDPR supports service areas in maintaining operational compliance with legislation and has developed and oversees the action plan attached at Appendix 1.

Recommendation:

To receive the annual report on the actions undertaken during the year and to CONSIDER the action plan, attached at Appendix 1, to further improve the Council's General Data Protection Regulation (GDPR) arrangements.

Reasons for Recommendation:

It is good practice that the Data Protection Officer provides annual assurance to the Audit and Governance Committee on the adequacy of the Council's GDPR arrangements.

Resource Implications:

None arising directly from this report.

Legal Implications:

The authority has a duty to ensure compliance with its obligations under GDPR. Failure to comply could result in action from the Information Commissioner's Office that can include enforcement notices, prosecutions and fines.

Risk Management Implications:

Ongoing compliance monitoring and implementation of the GDPR action plan aims to mitigate the following risks:

- Accidental or deliberate breach of data protection requirements.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office.
- Council reputational damage.

Performance Management Follow-up:

Progress on delivering the GDPR action plan is monitored by an internal Information Board. This Board includes the Chief Executive, supported by officers from ICT, Corporate Services and One Legal. Once operational, as part of its COVID-19 recovery plan, internal audit can be used to obtain additional assurance where relevant.

Environmental Implications:

None arising directly from this report.

1.0 INTRODUCTION/BACKGROUND

1.1 The Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) came into effect on 25 May 2018. The Council must comply with all relevant legislation and maintain good practices to protect the personal data held. A significant amount of work was undertaken prior to this date to ensure the Council was broadly compliant and this work is ongoing to maintain compliance. The Council has an approved Data Protection Policy that provides guidance to ensure that all personal data is lawfully processed by the Council and meets the seven key principles of the regulation.

1.2 The Council's policy details the roles and responsibilities to oversee compliance which these are as follows:

- Senior Information Risk Owner (SIRO) – to ensure that information assets are appropriately managed. Oversees and is responsible for the whole information governance framework and the risk associated with it. This role is fulfilled by the Chief Executive.
- Data Protection Officer (DPO) – to undertake the statutory role by monitoring compliance and by providing training, advice and assistance to the SIRO. This role is fulfilled by the Borough Solicitor.
- GDPR Single Point of Contact (SPoC) – acts as the single point of contact for customers, staff, Members and the DPO in relation to personal data. Oversees delivery of the GDPR action plan, providing advice and support to information asset owners. This role is fulfilled by the Internal Audit and GDPR Officer.
- Information Asset Owners (IAO) – each operational manager has been designated as the IAO for their service. It is their responsibility to ensure their services are compliant with data protection legislation.

An internal Information Board meets on a regular basis to oversee GDPR related activity. One key objective of the Board is to oversee delivery of the GDPR action plan. A consolidated action plan was developed pre-COVID and pulled together actions including any recommendations from internal audit and areas of further improvement identified by the Internal Audit and GDPR Officer following a complete review of the Council's arrangements. The action plan can be found at Appendix 1.

2.0 GDPR WORK UNDERTAKEN IN THE YEAR

2.1 It is good practice that the DPO, as the compliance monitoring officer, provides assurance to the Audit and Governance Committee as to the broad compliance with GDPR and any action that has been taken over the last year to strengthen arrangements. As identified within the action plan, a large number of actions are to review the current arrangements, including policy and processes, to ensure they remain relevant. In terms of the key actions undertaken during the year, these include:

- The implementation of a stand-alone communications plan to raise staff awareness. This has included staff briefings and intranet articles, particularly around preventing and reporting data breaches, managing data in a remote setting and data retention.
- Procurement of an e-learning training platform that will shortly be rolled out to staff and Members.
- Training of all relevant staff on the importance of retention and redaction and the equipping of all relevant services with redaction software.
- Support to all emerging projects that require a Data Protection Impact Assessment (DPIA). A DPIA is a process designed to systematically analyse, identify, and minimise the data protection risks of a project or plan. Projects include COVID-19 support grant schemes, digital recruitment, High Street Heritage Action Zone, HR self-service, Land Registry migration, new digital platform, paperless billing etc.
- Support to the timely reporting and submission of any data breaches – within the last year there have been 20 recorded breaches, of which, 19 were categorised as low risk and one categorised as a medium risk.
- The development by the Business Transformation team of a case management system to manage and respond to data requests, including Subject Access Requests (SAR). This allows residents to request a copy of the personal information we hold about them and to check that we are lawfully processing it. Data requests are increasing in number and during the last year 64 have been received.
- The positive conclusion of a self-assessment against the Information Commissioner's Office GDPR toolkit.
- Providing a consultation response to the Department of Culture, Media and Sport, in relation to proposed changes to the UK GDPR and Data Protection Act 2018.

3.0 LOOKING FORWARD

3.1 The action plan is a comprehensive document, providing an excellent platform to enhance the Council's arrangements. Key actions moving forward include:

- Support to the implementation of the new website project. This will include a review of all privacy notices to ensure they are up to date.
- The implementation of an 'information classification' project.
- Undertaking a review of key policies such as the overarching Data Protection Policy, Breach Reporting Policy and providing support to ICT related policies such as cyber security and asset management.
- Once fully operational, for internal audit to build into the scope of its work plan that lessons learnt in respect of any breaches are implemented and test that data is being retained in accordance with the corporate retention policy.

4.0 DATA PROTECTION OFFICER ANNUAL CONCLUSION

4.1 Ensuring compliance with Data Protection requirements is a continuous process requiring continual development and learning. The support of the GDPR Single Point of Contact has been invaluable in assisting both the Senior Information Risk Owner and the Data Protection Officer in securing and monitoring the Council's development and compliance. It is pleasing to report that there have been a low number of data breaches recorded, none being categorised as high risk, and therefore the Council has not been required to notify the Information Commissioner of any breaches. Nevertheless, it is important that the Council's arrangements are continually reviewed and that the GDPR action plan attached at Appendix 1 is delivered in order to secure the Council's continued compliance.

5.0 OTHER OPTIONS CONSIDERED

5.1 None.

6.0 CONSULTATION

6.1 None.

7.0 RELEVANT COUNCIL POLICIES/STRATEGIES

7.1 Data Protection Policy

8.0 RELEVANT GOVERNMENT POLICIES

8.1 None.

9.0 RESOURCE IMPLICATIONS (Human/Property)

9.1 None

10.0 SUSTAINABILITY IMPLICATIONS (Social/Community Safety/Cultural/ Economic/ Environment)

10.1 None

11.0 IMPACT UPON (Value For Money/Equalities/E-Government/Human Rights/Health And Safety)

11.1 None

12.0 RELATED DECISIONS AND ANY OTHER RELEVANT FACTS

12.1 None.

Background Papers: None

Contact Officer: Borough Solicitor (Data Protection Officer)
01684 272011 Sara.Freckleton@tewkesbury.gov.uk

Appendices: Appendix 1 – GDPR Action Plan