Corporate Governance and Standards Committee Report

Ward(s) affected: n/a

Report of Director of Environment

Author: Joyce Hamilton

Tel: 01483 444053

Email: joyce.hamilton@guildford.gov.uk

Lead Councillor responsible: Matt Furniss

Tel: 07891 022206

Email: matt.furniss@guildford.gov.uk

Date: 28 March 2019

Data Protection and Information Security Update Report

Summary

The transactions and interactions customers, residents and staff make with the Council can involve those individuals sharing personal data, such as their name, address and birth date. Most individuals share data online, for example, when visiting a website, searching for or buying a product/service, using social media or sending an email. Sharing data helps make life easier, more convenient and connected.

The data of the Council's staff, customers and residents does not belong to the Council; it is therefore important that this data is used only in ways reasonably expected, and that it stays safe. Data protection law makes sure everyone's data is used properly and legally.

Recommendation to Committee

To note the report.

1. Data Protection

1.1 Since May 2018, there has been both the expansion of the information available and the publication of detailed guidance that assists the Council with its legal obligations. These include:

- Children and the General Data Protection Regulation (GDPR);
- Automated decision making and profiling;
- Codes of conduct;
- Data Protection Impact Assessments (DPIAs);
- Right to data portability;
- Consent;

- Exemptions
- Encryption;
- Contracts and liabilities; and
- European Data Protection Board (EDPB) guidelines

1.2 The Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It works alongside the General Data Protection Regulation (GDPR), and tailors how the GDPR applies in the UK - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

a) Brexit

1.3 The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data – but it does not apply to processing for law enforcement purposes, or to areas outside EU law such as national security or defence.

1.4 The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After these events, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

1.5 As the Council is an organisation in the UK and the GDPR applies to it, there are key practical points and considerations for the Council to consider in relation to its data protection obligations. This is being reviewed by the Council's Information Risk Group (IRG). For example, the UK leaving the EU would mean there would be some parts of the GDPR that will no longer be relevant or apply to the UK.

1.6 After exiting the EU, all guidance will reflect the UK data protection regime and possible effects of any transitional period if a deal is agreed.

b) Will the GDPR still apply if we leave the EU without a deal?

1.7 The GDPR is an EU Regulation and, in principle, it will no longer apply to the UK if we leave the EU on 29 March 2019 without a deal. However, as an organisation that operates inside the UK, the Council will need to comply with UK data protection law. The government intends to incorporate the GDPR into UK data protection law when it exits the EU. This means in practice there will be little change to the core data protection principles, rights and obligations found in the GDPR.

1.8 The EU version of the GDPR would still apply directly to the Council if it either operated in Europe, offered goods or services to individuals in Europe, or monitored the behaviour of individuals in Europe.

1.9 The GDPR would still apply to any organisations in Europe who send the Council data, in this scenario the Council would need to work with the said organisation to decide how best to transfer personal data to the UK in line with the GDPR.

1.10 The Information Commissioner's Office (ICO) will not be the regulator for any European-specific activities caught by the EU version of the GDPR, although they will continue to work closely with European supervisory authorities.

c) What will the UK data protection law be if we leave without a deal?

1.11 The Data Protection Act 2018 (DPA 2018), which currently supplements and tailors the GDPR within the UK will continue to apply. The provisions of the GDPR will be incorporated directly into UK law if we leave the EU without a deal, to sit alongside the DPA 2018. New data protection exit regulations have been passed which will make technical amendments to the GDPR so that it works in a UK-only context from exit day.

Is the ICO's GDPR guidance still relevant?

1.12 UK data protection law is expected to be aligned with the GDPR, so the Council should continue to use the existing guidance. The data protection principles, obligations and rights will remain the same.

d) Freedom of Information (FOI) Act and Environmental Information Regulations (EIR)

FOI

1.13 A new Section 45 Code of Practice was issued on 4 July 2018. This Code of Practice provides guidance for public authorities on best practice in meeting their responsibilities under Part I of the Act (Access to information held by public authorities). It sets the standard for all public authorities when considering how to respond to Freedom of Information requests. The Information Commissioner also has a statutory duty to promote good practice by public authorities, including following this Code of Practice.

Brexit – will FOI and EIR still apply?

1.14 The Freedom of Information Act 2000 forms part of UK law and will continue to apply. The Environmental Information Regulations will continue to apply unless specifically repealed or amended. Both Acts derive from EU law, but are set out in UK law. The UK has also independently signed up to the underlying international treaty on access to environmental information (the Aarhus Convention).

e) Data protection compliance since May 2018

1.15 The staff training and awareness programme was successful and new employees are trained as part of their induction. Existing corporate policies and procedures were amended and new policies and procedures introduced.

1.16 The Council launched a new Data Protection and privacy web page to reflect the changes to the law and the Council's approach to data protection. https://www.guildford.gov.uk/article/21422/Data-protection-and-privacy

1.17 Since the GDPR came into force, there has been an increase in the public using their personal rights, for example Subject Access Requests (SARs).

1.18 Legal Services have amended the Council's contracts to reflect GDPR requirements and this will be kept under review as part of its role in contract management, procurement and the transparency code.

1.19 The data protection team have received a high level of requests for advice and support across a number of areas within the Council and this work will continue going forwards.

1.20 The outcome of internal audit reviews by KPMG were positive. These audits have focussed on privacy management, data management and collection, data security, third party agreements and incident management/escalation. The IRG worked with KPMG to conduct and complete this audit.

1.21 Cyber security awareness training for staff took place in September. The awareness course was delivered and covered the following topics:

- Passwords
- Secure Devices
- Public Wi-Fi
- Privacy/E-Safety/Social media
- Cyber drills/Personal resilience
- Supply Chain/Accreditation
- Phishing/Social engineering
- Case studies
- Insider threat
- Threat horizon/Current trends
- Useful resources for business and personal use, including advice for parents and those
- Working with young people

f) Data protection compliance over the next 6 months

1.22 The Data Protection Officer (DPO) has recommended that they should be consulted as part of the Council's organisational changes, namely Future Guildford and the ICT Transformation Programme, changes to working practices, hot desking, flexible working and office relocations. This will ensure the DPO has an understanding of these projects and can provide advice to the project managers to assist with GDPR compliance (for example, Data Privacy Impact Assessments (DPIA) must be completed by the Project Managers and to assist this, DPIAs should be included in project management training).

2. Information Assurance Manager

2.1 Information security successes since May 2018:

- In partnership with SEROCU (South East Regional Organised Crime Unit) cyber awareness training was delivered to high risk targeted Managers with a further interactive training session provided for Senior Leaders.
- Obtained formal PSN connection compliance Certification in December 2018 from the Cabinet Office (the Council last held this compliance certificate, which expired July 2017).
- Recently obtained formal Cyber Essentials Certification for the Council, which provides a level of assurance to our staff, customers and residents, that the Council takes information security seriously.
- Completed an internal KPMG GDPR Audit and received an Amber Red Rating (Partial Assurance with Improvements required). All improvements have been actioned and completed.
- Completed an internal KPMG Network Controls Audit. Received Amber Green Rating (Significant Assurance with Minor Improvements Assurance). Currently implementing the recommended minor improvements.
- Completed Local Government Association Audit on Information security position of Council, which produced Amber Green rating.
- Improved Governance and Risk Management in relation to security patches on all computer servers within the estate and removed identified vulnerabilities. Monthly patching now in place following the introduction of Nessus, which scans the internal network for vulnerabilities.
- Authored Information Systems Security Policy and ICT Users Policy
- Data protection team also authored Data Breach Response and Notification Policy and Data Protection Policy
- Reviewed and removed insecure FTP connections and replaced with SFTP connections from external suppliers to Council.
- Implemented NCSC (National Cyber Security Centre) monitoring of GBC network
- Introduced NCSC Web Check which monitors Council's external IP Address for vulnerabilities

2.2 Objectives for the next 6 months:

- Manage internal and External Penetration Testing of Council wide systems and mitigate any high-risk issues.
- Manage external ICT Audit being performed by Grant Thornton
- Manage security Penetration Testing of Council's Microsoft Azure Cloud
- Author new Password, Internet and Email, Patch Management and Firewall Policies and publicise Council wide
- Work closely with Finance Department to obtain formal PCI-DSS (Payment Card Industry – Data Secure Standard) for Council compliance
- Continue to attend NCSC meetings and information security events
- Implement NCSC DNS Service and Mail Check service which will mitigate spoofing

3. Information Rights Officer

3.1 Information Rights successes since May 2018:

- FOI/EIR Disclosure log is now live online https://guildford.disclosurelog.co.uk/
- FOI/EIR compliance rate for 2018 is at 93% - the highest since records began
- Transparency audit with KPMG completed in Oct/Nov 2018
- New Data Protection Policy (updated to cover GDPR & DPA 2018) and Data Breach Response & Notification Procedure updated and approved
- New Regulation Investigation Powers Act (RIPA) Policy approved and training completed for authorised officers
- Councillors' guides to FOI and data protection updated for Democratic Services team
- CCTV revenue costs now unified within single account code following recommendation in CCTV Audit
- Privacy Impact Assessment procedure for new CCTV's set up
- New section on cyber-security added to data protection training for new staff
- Council Records Retention & Disposal schedule updated following consultation with various service areas
- Privacy statements amended to reflect changes brought in by GDPR/DPA 2018
- New Policies and Procedures section added to Sharepoint as reference point for all staff to access
- Official form used by external bodies (e.g. police/HMRC) to request third party personal data for purposes of crime prevention/debt collection is now updated.

4. Objectives for the next 6 months

- To update Council and Surrey Police's CCTV joint Code of Practice in consultation with police representatives
- To review existing CCTV coverage to ensure data protection compliance in relation to signage/scope of vision, etc
- To further improve Ecase's functionality (for example to incorporate SARs etc)
- FOI section on Council website to be made more prominent to enable the disclosure log to be more visible

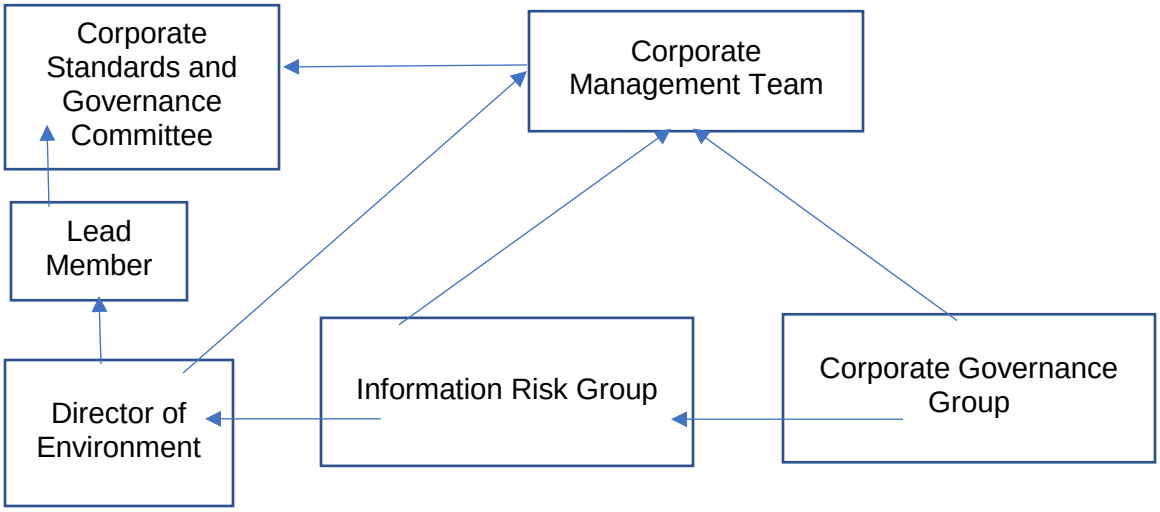
5. Appendices

Appendix 1: Data Protection and Information Security Governance Structure

Appendix 1

Data Protection and Information Security Governance Structure

The overall layout of the governance arrangements with the various groups and individuals involved is set out below. The diagram includes reporting lines.



The Information Risk Group (IRG)

The IRG's role is to oversee the Council's response to all information risks. This includes Data Protection and covers Information Rights and the security of records. The group meets every 6 weeks and its members are:

- Principal Solicitor (Corporate) (who is the Data Protection Officer, DPO)
- Chief Information Officer (who is the Senior Information Risk Owner, SIRO)
- Information Assurance Manager (Information Security)
- Information Rights Officer (IRO)

The Corporate Governance Group (CGG)

The CGG monitors the Council's standards of governance, including information issues. The group meets quarterly and its members are:

- The Head of Paid Service
- Chief Finance Officer
- Monitoring Officer
- Deputy Monitoring Officers
- Principal Solicitor (Corporate) & DPO