CORPORATE COMMITTEE 14 NOVEMBER 2019

Report title: Data Protection Act 2018 (DPA) General Data Protection Regulation (GDPR) Update Report

Wards: All

Portfolio: Councillors Jim Dickson and Donatus Anyanwu, Cabinet Members for the Voluntary Sector & Partnerships (job-share)

Report Authorised by: Andrew Travers: Chief Executive

Contact for enquiries: Padraig O'Mahony, Project Manager, GDPR Phase 2, 0207 926 3184, pomahony1@lambeth.gov.uk

Report summary

Under DPA 2018 and GDPR the council has a number of new responsibilities including data by design and by default which means considering DPA issues at the outset of any projects, adherence to the data protection principles, ensuring all individual rights are upheld and no charge for Data Subject Access Requests in most instances. Some of these new responsibilities were addressed under phase 1 of the Council's GDPR project with the remaining forming part of phase 2.

This report is a follow up report to the Corporate Committee report dated 21 March 2018 'General Data Protection Regulations 2018 (GDPR) Implementation' and outlines the work that has been done to date under Phase 1 (risk analysis and data mapping) of the DPA/GDPR Project and summarises the work currently being undertaken in Phase 2 (implementation and risk mitigation) in order to ensure that the Council is addressing its obligations under the Data Protection Act 2018 (the 'DPA 2018').

Phase 1 of the GDPR Project delivered a number of data protection policies, procedures guidance and templates; this is known as the Information Governance Framework (see Appendix 1). It also established an Information Asset Register (IAR). The IAR portal is a tool to record and manage all the council's information assets and processes and risk assess all aspects of data protection. It also includes the directorate, team, legal basis for processing, retention times, data types collected, data sharing and data processing agreements. An online portal to facilitate the maintenance of the IAR is being developed.

Phase 2 will mainly focus on ensuring awareness and use of the Information Governance Framework policies and procedures, using the Information Asset Register online portal and training across the council. The project will also deliver risk assessments and mitigating actions for all data processes to address any existing and new risks. Information Sharing and Data Processing Agreements reviews and compliance will form part of the project too. Data Protection Impact Assessment will also be embedded as part Information Asset Owners (IAOs) and Deputy Information Asset Owners (DIAOs) training.

Finance summary

The additional funding allocated for Phase 2 detailed in Finance section 3 below is £680,000.

Recommendations

1. To note the work undertaken in Phase 1 of the GDPR Project (see appendix 1) including work carried forward to Phase 2
2. To note the risk assessments and mitigating actions for all data processes within the council being undertaken as part of Phase 2 of the Project.
3. To note the Information Governance framework including Information Management policy, procedure, training and awareness and to provide any comments on the implementation plan.
4. To note the implementation plan for regularisation of all information sharing and data processing agreements between the council and third parties.

1. CONTEXT

1.1 DPA 2018 requires every local authority to comply with the principles of data protection and as part of this it is essential to create a framework to ensure data protection is monitored, updated and reviewed in line with data protection legislation. The DPA 2018 sets out seven key principles (see appendix 2 below) that are a requirement for all public bodies to adhere to. Failure to adhere to these principles could result in the imposition of significant penalties by the Information Commissioners Office ("ICO") and reputational damage to the Council. Ultimate responsibility and accountability lies with the senior management of the Council.

1.2 The DPA 2018 is intended to:

- make our data protection laws fit for the digital age when an ever-increasing amount of data is being processed;
- empower people to take control of their data; and,
- support UK businesses and organisations through this change.

1.3 The GDPR and DPA 2018 readiness project was initiated in January 2018. The project ran in two stages, with the intention of providing the Council with an assessment of readiness for GDPR and DPA 2018. Phase 1 of the project delivered an Information Governance Framework (IGF) which is set of policies and procedures based on Managing, Protecting and Using information. It includes the Data Protection Policy, Data Breach procedure, Subject Access Procedure and Data Protection Impact Assessment procedure. Phase 1 also produced an Information Asset Register (IAR) which manages the Council's information assets and the risks associated with them. It identifies gaps between information assets, processes, third parties and other parts of the council.

1.4 The IGF issues identified as part of Phase 1 were risk assessed and prioritised for action in May 2019. Since that date a project manager and project officers have been appointed for Phase 2. The project manager has reviewed GDPR training roll out , assisted the Council in awareness and use of GDPR principles and requirements such as data by default and data by design and assisted with reviewing the way the Council deals with data management and reviewing the Phase 1 issues referred to above.

1.5 Following the conclusion of Phase 1, the Data Protection Phase 2 project's aims are to:

- Address risks, both known (through phase 1) and to be disclosed throughout the phase 2;
- Identify further risks and recommend corrective actions and mitigation;
- Ensuring use and familiarity with the Council's IGF documents such as the Information Management Policy;
- Provide training and guidance during IAR transfer to Information Asset Owners (IAOs);
- Provide training to Deputy Information Asset Owners (DIAOs);
- Identify and regularise Data Sharing and Data Processing Agreements; and,
- Monitor compliance.

1.6 Phase 1 utilised a risk assessment approach and identified over 1700 risks across the council. Phase 2 will incorporate the council's risk assessment approach. While some of the intolerable risks (there were 9 in total) were mitigated against, three intolerable/high risks (see Section 6 Risk Management below for details) are still outstanding and will be tracked as part of Phase 2. The remaining risks will be managed by the Project Manager as part of the project as well as additional risks that arise during the course of the project. An overview of the risks will be undertaken as detailed in Risk Management section below. The medium risk will be managed as part of business as usual.

1.7 Phase 2 will last for approximately 18 months. The Information Asset Register (IAR) portal will form the focal point of the project. The IAR is also the Record of Processing Activities (RoPA) a requirement under Data Protection Act 2018. The RoPA activities is a record of all personal data processes within Lambeth Council.

2. PROPOSAL AND REASONS

2.1 Phase 2 project will cover:

- Updating and implementing the Information Governance Framework (The Information Governance Framework is all the data protection policies, procedures, templates and guide – See Appendix 1).
- Mitigation of the 1700 risks to Information Assets identified by Phase 1
- Mandatory induction data protection training followed by annual refresher training
- Corporate internal communications plan for all staff to increase IG awareness
- Awareness training workshop for Information Asset Owners (IAOs). (IAOs are senior / responsible individuals working in a relevant business area. Their role is to understand what information is held within their business area, what is added and what is removed, how information is moved, who has access and why.)
- Training workshops for designated Deputy Information Asset Owners (DIAOs). (The DIAO have day-to-day responsibility, and ensure that policies and procedures are applied and adhered to by staff and can recognise actual or potential security incidents. They are responsible for reporting such incidents to their IAO and consulting the IAO on incident management.)
- Revision of Job descriptions to include IG accountabilities specific to grade
- Reviewing and updating Information Sharing and Data Processing Agreements

2.2 The Phase 2 project seeks to embed the Information Governance Framework to make it business as usual across the Council. It will include addressing the following:

- Each service area manages personal information assets in order to deliver their services.
- There are hundreds of information assets that need to be protected to deliver better customer service and build customer trust.
- The Council must demonstrate compliance with information security measures, to include organisational and technical measures.
- The training and IGF policies will bring about a change culture as more customer centric digital services are implemented
- The Phase 2 project will drive change as staff become increasingly aware that data handling must be proficient to generally improve data quality and management and to minimise any potential risks/issues/breaches.
- Data Protection Impact Assessment will form part of training for IAOs and DIAOs and will be embedded as part of the Information Governance Framework.
- Assets are defined in our 'Information Management Policy' as information that is valuable to Lambeth Council's business, its customers or its communities. As an example, the information held on the records management system relating to social care and any supporting files and documents, either provided by the data subject or generated by the relevant service area, would be information assets regardless of the format (e.g. paper, electronic, or microfilm).

3. FINANCE

3.1 The costs for resources for undertaking Phase 2 of the project total £680k and comprise 5 officers for a period until March 2021. A Project Manager has been appointed and four Project Officers will be working on this project.

4. LEGAL AND DEMOCRACY

4.1 The Council is addressing Data Protection Act 2018(DPA) principles (see Appendix 2) and legal requirements (such as personal data recordkeeping and risk mitigation). An Information Governance Framework is in place and as part of business as usual the IG Team ensures that breaches are investigated and advice, training and assistance is provided to departments. Enforcement actions by the Information Commissioner's Office could result in severe penalties to the Council, in addition to incurring reputational damage.

4.2 Data Protection Phase 2 will help address identified risks, compliance with data protection principles and ensure the Council satisfies the requirements of the NHS toolkit by adequately staffing the Information Governance team to handle business as usual activities in addition to addressing urgent compliance issues.

4.3 There were no further comments from Democratic Services.

5. CONSULTATION AND CO-PRODUCTION

5.1 The Council's Risk Manager has been consulted regarding the outstanding risks and evidence of lack of compliance. He has added the high risks to the Corporate Risk Register.

5.2 The Senior Information Responsible Officer ("SIRO") has been informed of the known risks and the need to implement organisational change to address the Council's legal obligations. Relevant internal and external consultation has been undertaken in relation to the project deliverables. Some of the points of consultation are outlined here:

- Meeting with Phase 1 Project members to discuss their risks, issues and lessons learnt;
- Using ICO website for consultation; and,
- The Project Manager is a member of Information Governance for London (IGfL) group, a group of London boroughs dealing with Information Governance and Data Protection issues.

6. RISK MANAGEMENT

6.1 The proposed compliance project is all about risk management of noncompliance with DPA. A failure to address and mitigate risks for a potential data breach can result in financial and reputational damage to the Council, and an inability to efficiently manage the Council's data to provide valuable services.

6.2 The three highest risks for phase 2 to address are:

Risk	Mitigating actions	Directorate / Team
Information asset risk: non-compliance with data sharing, storage & retention protocols	Plan in place for directorate to address and mitigate risk; identify what data can be removed as part of retention policy	Community safety / youth violence teams
Information asset risk - Non-compliance with protocols for the access, non-deletion and storage of home visit data (housing)	Plan in place to identify users & their appropriate access with managers with service; identify what data can be removed as part of retention policy	Housing
ICasework compliance and data migration risk: ○ The current version of ICasework is no longer supported and will fail the next security audit ○ The supplier is unable to transfer all required data from Lambeth server to cloud service	A number of options are being considered including: 1. Asking Icasework to migrate data but this is unlikely 2. Source an external contractor to move current hosted service 3. Migrate to stand alone laptop 4. Source a new complaints/FOI/SAR/ Members system	Performance and Business Improvement

6.3 The Council's risk strategy will be followed during the project. The Risk Scoring Matrix is shown below. High risks will be escalated to the project board and medium and low risks will form part of BAU for business.

6.4 The types of risks identified under phase 1 included the following:

- Nonadherence to council's retention policy;
- Failure to conduct regular reviews of policies/procedures/users' access;
- Nonadherence to Information Management Policy;
- GDPR training level across the council lower than expected; and,
- Lack of awareness about Information Asset Register.

Risk Scoring Matrix

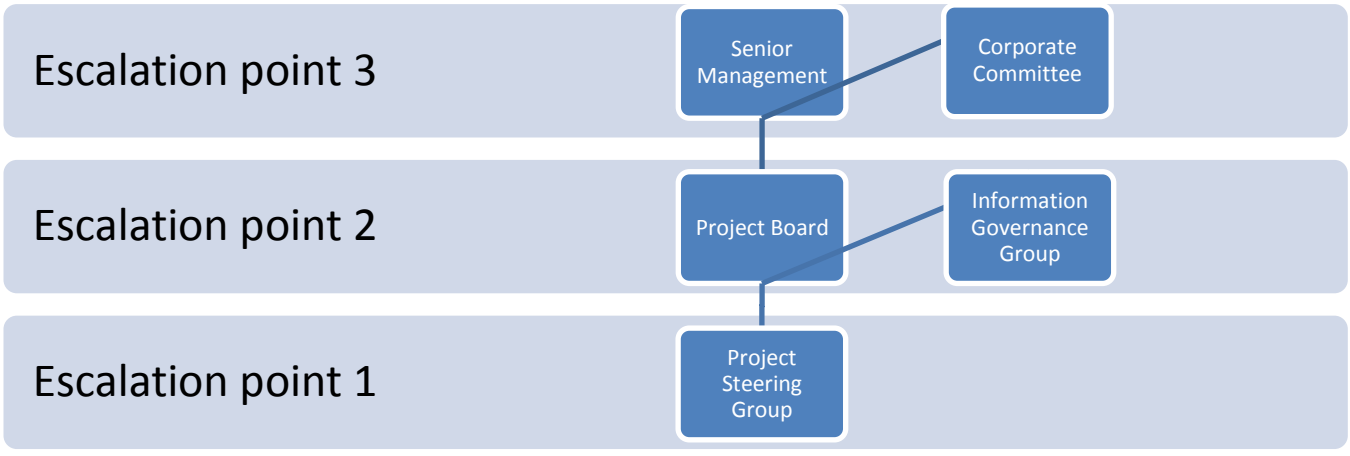
Threats	Impact			
Likelihood / X	Minor (1)	Significant (2)	Serious (4)	Major (8)
Very likely (4)	4	8	16	32
Likely (3)	3	6	12	24
Unlikely (2)	2	4	8	16
Very unlikely (1)	1	2	4	8

(Red – High risk, Amber – Medium risk, Green – Low risk)

Governance

6.5 The governance of the project will incorporate a number of areas. They will include oversight by the Project Board, project documentation from steering group, regular reporting to project board and Information Governance Group, staff training and awareness, IAOs and DIAOs training, embedding the Information Governance Framework and liaising with data protection experts such as ICO. There will also be oversight by the Corporate Committee on an annual basis. The service has recently been audited by Internal Audit and an action plan is being implemented.

6.6 The escalation process for the project has been outlined below:



7. EQUALITIES IMPACT ASSESSMENT

7.1 Not applicable.

8. COMMUNITY SAFETY

8.1 Not applicable.

9. ORGANISATIONAL IMPLICATIONS

9.5 Data protection is everyone's responsibility. Phase 2 of the GDPR Implementation Plan will embed this using the Information Governance Framework. It is recommended that data protection be a standing item on all senior management meetings and this approach should be cascaded down throughout the council.

9.6 The Information Management policy will ensure each Director is accountable to the SIRO for the accuracy and security of information assets within their respective service area and is the Information Asset Owner (IAO). Each service IAO area will be required to designate a Deputy Information Asset Owner (DIAO) who reports to the IAO and is a Head of Service. The IAO and DIAO will need to work together to identify a sufficient number of Data Owners (DO) (senior managers working within the service area) to be responsible for the collection, creation, modification and deletion of specified records holding personal data, contained in a collection of one or more data sets or files that are being processed for permitted purposes that appear on the Service Area's Information Asset Register. Performance & Business Improvement are developing an IAR portal and it is envisaged that this will assist the IAOs, DIAOs and DOs with their roles and responsibilities.

10. TIMETABLE FOR IMPLEMENTATION

10.1 The timetable for implementation for the project is as follows:

Appointment of Project Manager	Jul 2019	Sept 2019	Head of IG
Terms of Reference signed off	Sept 2019	Oct 2019	PM
PID signed off	Sept 2019	Oct 2019	PM
Project Board finalised	Sept 2019	Oct 2019	Head of IG, PM
Appointment of Project Officers	Aug 2019	Oct 2019	Head of IG, PM
Risk Assess all processes in each of the 4 Directorates [746*]	Nov 2019	Dec 2020	PM + POs
Identify IAO and IAA	Nov 2019	Mar 2020	Head of IG, PM, POs
Establish ownership of the IAR within the Council	Dec 2019	Mar 2020	PM + POs
Embedding Information Management Framework	Nov 2019	Dec 2020	Head of IG, PM, POs

Develop IAR Procedure	Jan 2020	June 2020	Head of IG, PM, POs
Provide training on data protection for IOAs and DIAOs	Mar 2020	Sept 2020	PM + POs
Transfer IAR to IAOs	Jun 2020	Sept 2020	PM + POs
Prioritise service areas processes for each Directorate.	Dec 2020	Mar 2021	PM + POs
Identify Information Sharing Agreements (joint-controllers)	Sept 2020	Mar 2021	PM + POs
Identify Data Processing Agreements (processors)	Sept 2020	Mar 2021	PM + POs
Analysis of data processes for Medium priority services, to be addressed as BAU.	Dec 2020	Mar 2021	PM + POs
Closure report	Jan 2021	Mar 2021	PM

AUDIT TRAIL				
Consultation				
Name/Position	**Lambeth directorate / department or partner**	**Date Sent**	**Date Received**	**Comments in paragraph:**
Councillors Jim Dickon and Donatus Anyanwu	Cabinet Members for Voluntary Sector and Partnerships	05.11.19	06.11.19	
Andrew Travers	Chief Executive	05.11.19	For info	N/A
Christina Thompson, Finance	Finance & Investment	05.11.19	06.11.19	
Alison McKane, Legal Services	Legal and Governance	11.10.19	03.11.19	
David Rose, Democratic Services	Legal & Governance	04.11.19	05.11.19	

REPORT HISTORY	
Original discussion with Cabinet Member	N/A
Report deadline	01.11.19
Date final report sent	06.11.19
Part II Exempt from Disclosure/confidential accompanying report?	No
Key decision report	No
Date first appeared on forward plan	N/A
Key decision reasons	4. Not applicable
Background information	N/A
Appendices	Appendix 1 – Lambeth Council Corporate Information Governance Structure Infographic Appendix 2 – Glossary of Information Governance Terms