For General Release

REPORT TO:	**CABINET 19 MARCH 2018**
SUBJECT:	**IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION (GDPR)**
LEAD OFFICER:	**RICHARD SIMPSON EXECUTIVE DIRECTOR OF FINANCE** **JACQUELINE HARRIS-BAKER DIRECTOR OF LAW AND MONITORING OFFICER**
CABINET MEMBER:	**COUNCILLOR SIMON HALL**
WARDS:	**ALL**

CORPORATE PRIORITY/POLICY CONTEXT/AMBITIOUS FOR CROYDON:

Compliance with these new legal requirements is mandatory.

Having in place good corporate governance seeks to ensure the Council maintains high standards to protect the personal data of residents and staff underpinning the values and priorities of the Council.

Implementation of these changes will give the Council the opportunity to review and strengthen its processes and procedures in relation to information management and data protection for all its residents and staff.

If GDPR is implemented correctly and in the right spirit this will help the Council foster the public's trust in the way it works.

FINANCIAL IMPACT:

Fines for non-compliance are set at a maximum of €20 million or 4% of turnover. Other financial consequences are set out within the report.

KEY DECISION REFERENCE NO: Not a key decision.

The Leader of the Council has delegated to the Cabinet the power to make the decisions set out in the recommendations below:

1 RECOMMENDATIONS

The Cabinet is recommended to:

(i) Note the impact arising from the introduction of the General Data Protection Regulation;

(ii) Note the proposed actions by the Council to meet the new statutory duties.

2 EXECUTIVE SUMMARY

2.1 The Data Protection Act 1998 regulates how the Council uses and stores the personal data of its residents and staff. An EU directive the General Data Protection Regulation (GDPR) will replace the Data Protection Act (DPA). The GDPR sets out how organisations can collect and use personal data. The GDPR comes into force on 25 May 2018. Separately the government has introduced a Data Protection Bill which covers these and other matters.

2.2 The GDPR applies to processing of personal data carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods and services to individuals in the EU. The GDPR and the Data Protection Bill will continue to apply in the UK after the UK leaves the EU.

2.3 This report provides an overview of the new requirements and a summary of the steps taken by officers and the Council's current readiness for implementation of the new rules.

3 INTRODUCTION

3.1 Europe's main concepts and principles for data protection laws are now contained in the General Data Protection Regulation (GDPR). This will replace the current directive upon which the Data Protection Act 1998 is based. There is also a Data Protection Bill which is going through parliament.

3.2 The new regulation starts on 25 May 2018 and will be enforced by the Information Commissioner's Office (ICO).

3.3 The UK's decision to leave the European Union will not alter this.

4 DETAIL

WHAT ARE THE NEW GDPR REQUIREMENTS?

4.1 This is the biggest overhaul to data protection law in twenty years. Its aim is to establish a single set of rules for all EU members' states and to update the law to reflect changes in the way data is generated and used in the digital world. The GDPR extends the rights of individuals and will require the Council to review and in some cases develop new policies and procedures to protect personal data and also adopt appropriate technical and organisational measures in a range of areas.

4.2 A summary of the new requirements placed upon the Council is set out in Appendix 1 of this report. Further details can be found in the ICO publication Overview of the General Data Protection Regulation (GDPR)

https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf

WHAT DO WE HAVE TO DO TO COMPLY?

4.3 Many of the GDPR'S main concepts and principles are like those in the Data Protection Act 1998 (DPA). If the Council is complying with the current law,

then this is a good starting point. However, there are many new elements and significant enhancements which requires the Council to do some things differently and others for the first time.

4.4 There are 12 key steps to compliance which have been identified by the ICO. A summary of the 12 key steps is set out in Appendix 2 of this report. Further details can be found in the ICO publication preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

WHAT ARE THE COUNCIL'S GOVERNANCE ARRANGEMENTS?

4.5 Officers have established a *GDPR Project Board* to assess the Council's readiness for compliance with the new Regulations and to put in pace a programme of actions to assist departments with compliance. The Board is chaired by the Council's Director of Law and Monitoring Officer.

4.6 The GDPR Board feeds into the Council's *Information Management Steering Group (IMSG)* which is responsible for, amongst other things, ensuring compliance with data protection and the GDPR. The IMSG is currently chaired by the Council's acting Chief Information Officer. All officer appointed Information Management Champions and officers who are members of the Information Management Team are also members of the IMSG.

4.7 The IMSG reports into the *Governance Board* which is jointly chaired by the Director of Governance and the Director of Law and Monitoring Officer which in turn reports into *Corporate Management Team*.

WHAT IS THE ROLE OF THE DATA PROTECTION OFFICER (DPO)?

4.8 GDPR introduces for the first time a statutory requirement upon the Council to designate a DPO. The DPO should be designated based on expert knowledge of data protection law and practice and the ability to fulfil the tasks set out in Article 39 of the GDPR. The DPO may be a staff member or may fulfil the tasks based on a service contract. Contact details for the DPO shall be published by the controller/processer and communicated to the ICO. The DPO shall report directly to the highest management level of the controller/processor. The DPO shall be provided with resources necessary to carry out the tasks set out in Article 39.

4.9 Article 39 identifies the key tasks of the Council's designated DPO:

- To inform and advise the Council and its employees of their obligations pursuant to GDPR;

- Monitor compliance with the GDPR including the assignment of responsibilities, awareness raising, and training of staff involved in the processing operations and related audits;

- To provide advice where requested about the data protection impact assessment process and monitor its performance pursuant to article 33;

- To co-operate with the ICO; and

- To act as the contact point for the ICO and the public on issues related to the processing of personal data.

4.10 The Council has appointed the Head of Litigation and Corporate Law as the Council's Data Protection Officer.

WHAT STEPS ARE CURRENTLY BEING TAKEN?

4.11 To date the following steps have been taken by the Council:

- **Data Audit**. The Information Management Team have prepared a Data Audit document which was circulated to Executive Directors, Directors, Heads of Service and Managers in October 2017. The data audit is the starting point for compliance. Only Managers know what information they hold, for what purpose and who this is shared with. Completed audit responses are being received and a gap analysis prepared. A link with the Information Asset Register is being explored to assist with the data audit.

- **Training.** A training programme is underway to raise awareness of the GDPR requirements. Training was provided to ELT on 22 November 2017. Briefing sessions have been running during January/February/March to get Directors, Heads of Service and Managers to engage with the process, assist them to complete their audit responses and brief/train them in the new requirements for GDPR. An on-line training module is being developed for staff and councillors. This will be available in February/March 2018

- **Raising awareness/Communications**. The Communications Team have prepared a communications programme. A range of articles are proposed to include a GDPR quiz which has been uploaded to the intranet.

- **GDPR Project Board**. A GDPR Project Board has been established, Chaired by the Director of Law, to assess the Council's readiness for GDPR compliance and put in place a programme of actions to assist compliance. The Project Board feeds into the IMSG and Governance Board and ultimately ELT.

- **Appointment of a Data Protection Officer**. The Head of Litigation and Corporate Law was nominated on 1 November 2017 as the Council's Data Protection Officer.

- **Action Plan.** A detailed Action Plan has been developed providing information for departments as to the key actions they are required to take. An Implementation Plan is now being developed identifying

individual projects and workstreams with SMART targets with named accountability and responsibilities.

- **Appointment of a GDPR Project Manager**. GDPR is a corporate wide transformation project. The extra conditions introduced by the GDPR will require a project management approach to compliance. Approval has been given under delegated authority to recruit a Project Manager on a temporary basis to manage the many workstreams arising from the new requirements. An advert is currently running for this position. It is hoped to be able to recruit as a secondment opportunity.

- **Nomination of additional Information Management Champions. (IM Champions).** IM Champions are part of the IM Steering Group chaired by the Council's Chief Information Officer and play a key role across the Council. They are responsible for promoting information management within their areas of responsibility, supporting staff with IM issues and then subsequently raising them with the IM Steering Group of which they are members. Their responsibilities cover both freedom of information and data protection matters. The IM Champions will be a key component in helping to shape and deliver the GDPR Project across the Council. Requests have been made for Directors to identify IM Champions for all areas for which they are responsible. Any newly appointed IM Champions will need to be fully trained before being able to undertake this additional responsibility.

- **Resourcing review.** The Information Management Team are a key component to the project and the Council's compliance. The team was created many years ago following a significant data breach and have worked well to improve standards and put in place processes and procedures across the Council. The team work well with the legal team who provide legal advice and assistance when required. The team sits within the Corporate and Customer Services Directorate. A review of resourcing/capacity both within the IM Team and across the Council to deliver this project is underway.

5 CONSULTATION

5.1 There has been no external consultation on this report.

6 FINANCIAL AND RISK ASSESSMENT CONSIDERATIONS

Revenue and Capital consequences of report recommendations

6.1 Non-compliance with the GDPR could have a serious financial implication for the Council. Organisations that breach the current Data Protection Act are liable to a fine capped at £500,000. Under GDPR organisations are liable to a fine up to 20 million euros or 4% of turnover, whichever is the higher. In addition, if a breach involves personal data of an individual they can claim damages.

6.2 There may be a cost associated with upgrading systems to comply with new requirements. These costs are still to be developed and once known any funding required will need to be identified to ensure the Council remains GDPR compliant.

6.3 There will be a loss of revenue from the removal of current fees in connection with Subject Access Requests. This income is currently very low at £10 per request.

6.4 There may be a cost associated with processing increased numbers of Subject Access Requests. At this stage it is difficult to calculate this cost as demand remains unknown and will only become apparent after the implementation of GDPR, when a further assessment will need to be made.

6.5 There may be a cost associated with producing Data Protection Impact Assessments.

The effect of the decision

6.6 The report is for noting at this stage.

Risks

6.7 Failure of the Council to comply with the new GDPR requirements has been added to the Risk Register. The risks of non-compliance are, amongst other things, significant financial penalty, reputational damage, customer dissatisfaction, organisational scrutiny, enforcement action, criminal prosecution and damages.

Options

6.8 Compliance with the new GDPR is a statutory requirement.

Future savings/efficiencies

6.9 Implementation of the necessary changes to practices and procedures around data protection will give the Council the opportunity to strengthen its processes in relation to information management and data protection for all its residents and staff. Whilst savings are unlikely to be found efficiencies in process should be explored.

(Approved by: Lisa Taylor, Director of Finance, Investment and Risk)

7 COMMENTS OF THE COUNCIL SOLICITOR AND MONITORING OFFICER

7.1 The Solicitor to the Council comments that GDPR is a large document of regulations – over 80 pages. It replaces the previous 1995 Data Protection Directive which current UK is based upon. The GDPR introduces many new elements and significant enhancements to the requirements placed upon controllers and processors of personal data. Further detail is already set out within this report.

*(*Approved by*:* Sandra Herbert Head of Litigation and Corporate Law on behalf of the Director of Law and Monitoring Officer)

8 HUMAN RESOURCES IMPACT

8.1 The Council has a structure of officer working groups that oversees data protection. The GDPR requires organisations to demonstrate compliance; this includes training, internal audits, data protection by design and the appointment of a Data Protection Officer (DPO).

8.2 The Head of Litigation and Corporate Law has been appointed as the Council's Data Protection Officer.

8.3 The ELT have been asked to nominate Information Management Champions from within their areas of responsibility to take forward the additional requirements of the new regulation.

8.4 The DPO is not responsible for compliance with GDPR; this is the responsibility of the Council. The DPO will monitor how the Council implements GDPR and will provide advice. The DPO will report on performance to senior management and councillors and will be the Council's link with the Information Commissioner who oversees data protection nationally.

8.5 A programme of briefings and training is underway for all staff and councillors. GDPR will also form part of the councillor induction training following the elections in May 2018.

8.6 There may be a need to recruit additional support to services that struggle with the number of additional tasks they need to undertake as we get nearer the 25 May 2018 deadline.

8.7 Project management support has been approved under officer delegated authority for a temporary period of 8 months. The position has been evaluated as a Grade 14.

(Approved by: Sue Moorman Director of Human Resources)

9 EQUALITIES IMPACT

9.1 An Equality Impact Assessment is an important framework for demonstrating due regard to the Public Sector Equality Duty through considering evidence and analysis to help identify the likely positive and negative impacts that policy proposals may have. The requirements of the GDPR are embodied in the Data Protection Bill which is being promoted by the government. The government considers that overall the Bill will help to protect and promote equality of opportunity between those who share protected characteristics and those who do not and helps to eliminate unlawful discrimination. The government considers that the Bill will not harm or create barriers to good relations between individuals who share protected characteristics and those who do not.

The Bill has undergone a full Equality Impact Assessment a copy of which can be accessed:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664404/Equality_Impact_Assessment.pdf

10 ENVIRONMENTAL IMPACT

10.1 There is no known impact.

11 CRIME AND DISORDER REDUCTION IMPACT

11.1 There is no known impact.

12 REASONS FOR RECOMMENDATIONS/PROPOSED DECISION

12.1 The report is for information only and is presented to ensure Members are fully briefed on the new requirements of the GDPR, the steps currently underway, the impact this is likely to have on current and future resources and the potential risks for the authority.

13 OPTIONS CONSIDERED AND REJECTED

13.1 Compliance with the new GDPR is a statutory requirement. The report is for information.

CONTACT OFFICER: Sandra Herbert
Head of Litigation and Corporate Law
extension 62928

APPENDICES TO THIS REPORT: Appendix 1 Overview of the GDPR requirements
Appendix 2 12 steps to compliance with GDPR

BACKGROUND PAPERS:

Regulation (EU) 2016/679 of the European Parliament and of the Council 27April 2016 (GDPR)