London Borough of Bromley

Report No. CSD17173	PART I – PUBLIC	Agenda Item No.:

Decision Maker:	**Executive**
Date:	**6th December 2017**
Decision Type:	Non-Urgent Executive Key
TITLE:	**THE GENERAL DATA PROTECTION REGULATIONS 2016**
Contact Officer:	Mark Bowen and Vinit Shukle Tel: 020 313 4461 email: Mark.Bowen@bromley.gov.uk; Vinit.Shukle@bromley.gov.uk
Chief Officer:	Mark Bowen, Director of Corporate Services
Ward:	All Wards

1. REASON FOR REPORT

This report details the significant changes that will be required to ensure that LB Bromley is compliant with the General Data Protection Regulations 2016 (GDPR). The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. RECOMMENDATIONS

Executive are requested to:

2.1 Note the changes proposed by the GDPR and the work to be undertaken to address them.

2.2 Agree a one-off cost of £495k from the under spend in the 2017/18 Central Contingency, in order to progress the works required to enable the Council to become GDPR compliant.

2.3 Agree growth of £287k for the two permanent staff, training & system running costs.

2.4 To note that an additional member of staff may be required to take on the additional responsibility of a Data Protection Officer (DPO) as required under the Article 37 of the GDPR. A report will be brought back to Members to confirm the allocation of this role.

Corporate Policy

1. Policy Status: Existing Policy

2. BBB Priority: Excellent Council

Financial

1. Cost of proposal: Estimated Cost £495k one-off costs and £287k on-going costs

2. On-going costs: Recurring Cost £287k per annum

3. Budget Head/Performance Centre: Information Management

4. Total current budget for this Head: £129k

5. Source of Funding: Existing revenue budget and Central Contingency

---

Staff

1. Number of staff (current and additional): 2 FTEs

2. If from existing staff resources, number of staff hours:

Legal

1) Legal Requirement: Statutory Requirement/Non-Statutory Requirement – Government guidance/No Statutory Requirement or Government Guidance

2) Call In: Call In is applicable/Call In is not applicable

Customer Impact

1. Estimated number of users/beneficiaries (current and projected)

Ward Councillor Views

1) Have Ward Councillors been asked for comments: No

2) Summary of Ward Councillors comments:

3. Commentary

The General Data Protection Regulation (GDPR) will replace the Current Data Protection Act (1998) on 25th May 2018. Although originating in EU law, the provisions will apply regardless of the position reached on Brexit and the government has introduced a Data Protection Bill to Parliament. This report highlights some of the key changes that will have an impact on the Council. The Report also outlines the initial and ongoing investment in resources and technology that will be required to ensure that LB Bromley adheres to this legislative change.

3.2 GDPR radically increases penalties. The maximum penalty for non-compliance and data breaches has increased from £500k to a maximum of £18m or 4% of the annual turnover of an organisation. Under the present system penalties of 10-20% of the maximum are frequently imposed for breaches and it is likely that significant (£1m+) penalties will be imposed from an early stage.

3.3 The GDPR places increased emphasis on the documentation that the Council must maintain in order to demonstrate accountability. Compliance within all areas listed in this report will require the Council to review its policies and approach to information governance and how data protection is managed as a corporate issue.

3.4 GDPR will impose significant changes on the information governance structure of the Council. This will include interaction with customers, the way in which information is recorded, the way in which data processing activities are communicated and a number of other areas all relating to the Council's processing activities of personal information. It will have a significant impact on all directorates and contractual arrangements. The Key Changes required by GDPR are set out in Appendix 1.

3.5 In preparation for this change, an independent review has been undertaken by the Data Protection People (DPP), who were invited to carry out a data protection compliance review and initial gap analysis to compare current practices against the GDPR.

3.6 The review identified good current practice but provided 51 recommendations that LBB need to action to advance towards being compliant with GDPR. A High Level Project Plan has also been provided to assist LBB in its efforts to be compliant by the go-live date of GDPR. The recommendations are attached as Appendix 2.

3.7 Taking the 51 recommendations set out by the Data Protection People, a project plan has been created expanding on the recommendations and creating actionable tasks for working towards GDPR compliance. The actions to ensure compliance to GDPR are attached as Appendix 3.

3.8 There is a need for additional staff support across the organisation to help balance the need for business as usual continuity and addressing the gaps between current practice and the requirements of the GDPR. The risk of diverting attention from one to the other without a measure of the consequences for not meeting either requirement could be detrimental to finances, reputation and compliance to meet various essential accreditations.

3.9 A need for an Information Management Team to be established has been identified to effectively deliver the change. This allocation of resources and associated costs is deemed proportionate to the potential fines and consequences of non-compliance.

3.10 The 25th May 2018 is not a finish line. There is an immediate need to accelerate and increase efforts to meet the go live date, balanced by consideration of the cost of upholding new ways of working. To maintain a demonstrable business process, manage efficiencies and sustain the effectiveness of technological implementations it is necessary to increase staffing to support the organisation.

3.11 Challenging system suppliers and application developers to provide a system that helps to support the business processes in GDPR compliance is a necessity.

3.12 The Council will be putting pressure on bespoke suppliers and in conjunction with other Councils that use common applications, add some weighted peer pressure to encourage them to provide updates to functionality that enables us to work effectively, efficiently and in line with the law.

3.13 It is likely these changes will come at a cost, and consideration needs to be given to having a central budget to support shortfalls in departmental budgets.

3.14 The Council is reviewing its information/data management procedures and policies. Appendix 4 sets out Current policies, where they have been reviewed and updated for GDPR compliance and also identifies new policies which are being or will need to be developed.

3.15 As part of the preparation for GDPR, consideration has to be given to how documents are stored, managed accessed and destroyed. This will also be a key aspect of the work required to move to paper light working, which will be necessary as a part of the accommodation changes.

3.16 The Council has purchased an information asset register system which is presently being rolled out across the Council. This will ensure that key information about the Council's records and systems is recorded in a way which will be compliant with GDPR. Work is also underway to revise polices on document retention and destruction.

3.17 Information Asset Owners and Assistants, who will be responsible for reviewing and implementing document retention policies for their departments have been identified and are being trained.

3.18 Work is also progressing to upgrade and improve SharePoint, which is the council's electronic system for storing and managing unstructured data/information.

3.19 In order to progress the work that has been carried out by the officers and to ensure compliance with the GDPR, additional resources are required including staffing, training and technology.

Staffing

3.20 A permanent Information Management Team is required to oversee and ensure that LBB will be ready for the change in legislation, as well as comply with the GDPR, Information Governance Toolkit, GDPR, Public Service Network (PSN) and Payment Card Industry Data Security Standards (PCI DSS). This will also ensure that LBB is advancing towards becoming a paper light council.

3.21 The team should be made up of a Head of Information or CISO (Chief Information Security Officer), an Information Governance Officer (IGO), an Information Management Officer (IMO) and to include a Support Officer role. The IGO and IMO roles are presently undertaken by existing officers within the Information Services team, who were not in scope for transfer to BT as part of the recent TUPE transfer. A successful bid has been made for support from the Council's Graduate scheme, to support GDPR work in the short to medium term.

3.22 A summary of key aspects of the roles is set out in Appendix 5.

3.23 The team will need to be reviewed annually to ensure adequate resources are assigned to ensure ongoing programs/projects and improvements in Information Management for the organisation. Two additional posts are required above the current establishment – A Head of Service and a Support Officer, which will cost approximately £117k.

3.24 The team will be responsible for the delivery and improvement of the following, to name a few:

- Information Governance Polices
- Development and review of Information Governance & GDPR e-training
- Development of the Corporate Data Sharing Agreement
- Audit of the contracts to ensure that the contract is supported by Data Sharing Agreement
- Development of the Privacy Impact Assessment framework and training for staff
- Data subject consent request on telephone and websites
- Possible communication to the public informing them of what LBB is doing to be compliant with GDPR and possible information relating to their data, that LBB are collecting
- Develop and form GDPR working group
- Develop and deliver an Information Asset Register
- Active Directory cleansing to remove all users that are no longer a LBB employee
- Streamline starter and leavers process
- Carry out system audits to ensure that all systems used by LBB comply with GDPR
- PSN Compliance
- PCI Compliance
- IG Toolkit Certification

3.25 In addition to the permanent team, four temporary workers will also be required, to develop and deliver the project/program. This would include two support officers and a project co-ordinator/Manager for 18 months to support the Information Governance Officer and Information Management Officer/Architect, in policy development that is required by GDPR and the Information Asset Register delivery.

3.26 A legal support will also be required for a period of 12 months to check and put in place Information Sharing Agreements, drafting of privacy notices, dealing with contract variations, drafting appropriate commercial contracts clauses and providing general legal support to the Information Management Team and the Council as a whole in connection with the GDPR coming into force

3.27 This will ensure coordination of departmental and corporate policies as well as develop, edit and review all processes and policies that are required. The resources will also be assigned to coordinate the GDPR Program with the Information Management Program that will run pre and post introduction of GDPR.

3.28 The estimated cost of the four temporary posts over the 18 months is £240k.

Information Strategy and Framework

3.29 With the Accommodation Project commencing, (subject to final Member decision) there will be a greater need for the Information Management and Information Retention policy to be written and communicated. The responsibility of this work will lie with the Information Management Team, who will commission the work.

3.30 A high level gap analysis of the current initiatives and future requirements has identified the need for a coordinated Information Management Strategy and Framework, which, together with the above mentioned initiatives, will provide the foundations for the Council's new working practices.

3.31 The approximate cost of £55k is envisaged for the key deliverables that are:

- A comprehensive framework for information governance and management
- A vision for how information should be managed through an Information Management Strategy
- Develop an enterprise approach to Information Architecture
- Provide a Target Operating Model for an information management function
- Identify how current initiatives including the Civic Centre Programme and the SharePoint Implementation can be improved and how these initiatives can be fitted into a wider programme of information management improvements
- A report outlining a series of pragmatic recommendations, detailing where appropriate, the associated estimated costs, effort, impact, risk and benefits of each

3.32 The Council is embarking on the FAST (Crayon) Software Asset Management programme. A gap analysis is being scheduled in the next 10 weeks to allow us to work towards Bronze accreditation. The ultimate goal is to reach Platinum level which takes a minimum of three years to achieve. In conjunction with BT the Council will be reviewing the software licenses held for Microsoft, IBM, Oracle and other

peripheral developers. This programme will be moderately labour intensive for the period of 3 years.

3.33 ISO27001is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

3.34 Recent development in Technology and infrastructure has resulted in the threat landscape evolving at an ever increasing pace, the threat agents becoming more intelligent and resourceful and the attack vectors and vulnerabilities being identified and circulated more efficiently on the dark web.

3.35 The ability of the Council to comply with PSN Certification, PCI DSS standards as well as remediate exploits and vulnerability, brings the Council close to achieving ISO27001 certification and align with ISO27002 (a best practice collection of information security guidelines that are intended to help an organisation implement, maintain, and improve its information security management).

3.36 As a Commissioner and Data Controller, we are increasingly demanding our Third Party Processors and Data Processors to be ISO27001 accredited and prove ongoing compliance. To be viewed as a trusted Commissioner, we should be in the same state of compliance.

Technology

3.37 Approximately £200k will be required to implement various technologies to ensure that LBB comply with GDPR, such as:

- HR System EDRM
- The Security Information and Management (SIEM)
- Data discovery tool that can assist with subject access requests, ring fencing for pause requests and subsequent erasure requests.
- Scanning and Document Management to promote paper light office
- Document Classification
- Email classification
- Pseudonymisation

3.38 From a technology perspective the Security Information and Management (SIEM) tool that provides a holistic and centrally managed view of an organisation's information technology (IT) security, will need to be introduced, as this will enable Information and Security Audits to take place. The cost of the system is £90k and it is envisaged that the on-going running costs will be approximately £50k per annum.

3.39 A key vulnerability will be around how HR information is held and consideration should be given to procuring a new consolidated HR system to manage documentation in a way which ensures compliance with GDPR.

3.40 Currently, HR holds all personnel files as hard copy, paper records. As well as the significant storage and office space this takes up, there is also a need to look at more secure ways of storing this information.

3.41 Having carried out some initial soft market testing with companies that could provide an EDRMS, it is envisaged that the initial set up costs would be approximately £110k and £90k per annum for on-going hosting and license costs.

3.42 As well as compliance of GDPR, a new HR system (EDRMS) will deliver a number of other benefits such as:

- Automatic retention schedules and deletion of data in line with these
- Freeing up of office space which will aid any development of the Civic Centre site
- Facilitating more flexible working
- More efficient way of working, less room for error
- Supporting any future changes to service
- Reduction in the time/cost of copying documents
- Easier transfer of information
- Ability to respond more quickly to information requests

Training

3.43 A clear communication plan and a training plan will be required for all staff at LBB to cover all aspects of GDPR. It is recommended that additional training resources and a budget of £30k be allocated to ensure that training is delivered and continually refreshed periodically throughout the organisation to keep staff updated.

Data Protection Officer

3.44 Article 37 states that all Local Authorities must appoint a Data Protection Officer (DPO). The main tasks of the DPO are provided within Article 39 and a cost of £70k per annum is anticipated should the responsibility not be allocated to an existing member of staff. A report will be brought back to Members with the outcome.

3.45 Article 37 of the GDPR also states that the person who is appointed into the role of the DPO must be designated on the basis of their professional qualities; in particular they will require expert knowledge of data protection law and practices and the tasks of the DPO cannot be delegated to a junior member of staff.

3.46 Article 38 also states that the Council must support the DPO in performing their tasks by providing resources necessary to carry out their tasks and to maintain their expert knowledge. Failure to provide an adequate budget could be classed as a breach of the Regulations.

3.47 Article 38 also explains that the role of the DPO contains protected Characteristics, it outlines that the DPO must be allowed to act independently of the Council and should not receive instructions from their employer on how they are to discharge their statutory functions. The DPO cannot be dismissed or penalized by the Council for performing these tasks.

4. POLICY IMPLICATIONS

4.1 This report supports BBB and Corporate Governance policies which invest in technology to enable greater flexible working.

5. FINANCIAL IMPLICATIONS

5.1 This report is highlighting the additional work that needs to be carried out in order to ensure that the Council is compliant with the GDPR.

5.2 Additional resources of £495k are required to carry out the one-off work to install new technology and temporary staff to develop and deliver the project in as well as £287k to cover the on-going costs for permanent staff, training and hosting services.

5.3 The table below summarises the costs between one-off and on-going, as well as the expected spend profile over the next four years: -

	One-Off £'000	On-Going £'000	2017/18 £'000	2018/19 £'000	2019/20 £'000	2020/21 £'000
Permamnent staffing (2 FTEs)	0	117	30	117	117	117
Temporary staffing (3FTEs)	171	0	28	114	29	0
Legal staffing (1FTE)	69	0	17	52	0	0
Training	0	30	8	30	30	30
Information strategy & framew ork	55	0	55	0	0	0
Security Information & Managemt system	90	50	90	50	50	50
HR System	110	90	110	90	90	90
Total	**495**	**287**	**338**	**453**	**316**	**287**

5.4 Approval is sought to drawdown funding from the underspend in the 2017/18 Central Contingency for the one-off costs of £495k and growth of £287k s required to meet the on-going costs, as profiled in the above table.

5.5 A future report will be brought back to Members with details of the allocation of the DPO role.

6. LEGAL IMPLICATIONS

6.1 The GDPR is due to come into force on 25 May 2018. The Government will repeal the Data Protection Act 1998 and replace it with a new Act which will set new standards for protection of general data in accordance with the GDPR.

6.2 Compliance with the GDPR and the new Act will be a statutory obligation on the Council. Non-compliance will lead to significant fines and reputational damage. It is necessary to put in place appropriate measures to ensure compliance with the Councils statutory obligations.

7. PERSONNEL IMPLICATIONS

7.1 As part of the introduction of the new GDPR regulations a review of existing contracts of employment and HR policies and procedures will need to be undertaken to ascertain whether or not existing contractual arrangements provides sufficient and necessary employee consents to allow the Council to process their personal data. Documentation relating to the processing of employee personal data may need to be amended if it is identified that this is not the case.

7.2. The newly created posts would be subject to job evaluation through the Council's agreed job evaluation processes. New posts would be advertised through the Council's normal recruitment processes, initially giving priority to any redeployees at risk elsewhere in the Council. In the case of the 4 temporary positions, they will either be filled on the basis of fixed-term contracts, or via Adecco, the Council's provider of agency workers. Existing staff within the Information Management team will be assimilated in to the redesignated roles of Information Governance Officer (IGO) and Information Management Officer (IMO).

Non-Applicable Sections:	
Background Documents: (Access via Contact Officer)	