Part I
Item No: 12
Main author: Farhad Cantel
Executive Member: Duncan Bell

WELWYN HATFIELD COUNCIL
CABINET – 2 AUGUST 2016
REPORT OF THE DIRECTOR (FINANCE AND OPERATIONS)

EUROPEAN UNION – GENERAL DATA PROTECTION REGULATIONS

1 Executive Summary

1.1 The purpose of this report is to advise Members of the new EU data protection framework which has finally been agreed after over three years of discussion, and to make some preparatory changes in readiness for this. The new General Data Protection Regulations (GDPR) will replace the current Data Protection Act 1998. It will not come into force immediately and is likely to be in the first half of 2018. However, as it contains some onerous obligations, it will have an immediate impact.

1.2 Now that agreement has been reached, there will be a period of technical checking and formal approvals. This may take several months and there could yet be last minute changes during this time. Only after that process is complete will the two year period run before the GDPR is in force.

1.3 Despite the EU referendum result our data protection governing body, the Information Commissioners Office, has for some time thought that there are numerous areas of the data protection legislation that need re-visiting. They were fully behind the implementation of the GDPR and that has not changed and they have stated that they will press the Government to implement the terms of the GDPR. Also, any EU based personal data can only be transferred easily either within the EU or to countries on a white list. To get on the white list your legislation must offer equivalent protection to that given to data in the EU, so we still need to implement similar, if not identical legislation, to the EU member states. This will mean that the GDPR will remain relevant and important.

1.4 Appendix A summarises the key components of the GDPR.

2 Recommendation(s)

2.1 Cabinet is asked to note the contents of this report.

3 Explanation

3.1 The General Data Protection Regulation (Regulation (EU) 2016/679) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). It also addresses export of personal data outside the EU. The Commission's primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR comes into force it will replace the Data Protection Act 1998. The regulation was adopted on 27 April 2016 and it will enter into force after a two-year transition period.

3.2 There are certain steps we can take now to prepare for the new Regulation. Some of these are listed below and some of these will be brought out in an update of our Data Protection Policy.

3.2.1 Establish policies and procedures, where appropriate.

3.2.2 Encrypt as much of our personal and business confidential data as is practicable and on a risk-based approach, paying particular attention to sensitive personal data, mobile devices and data transfers outside the business. We already do a lot of this with the ability to wipe data from mobile devices; encrypting laptops, only allowing encrypted memory sticks to access our network; encrypt emails and block CDs.

3.2.3 Assess and minimise risks by conducting privacy impact assessments on data processing and the supporting IT systems. A report on this went to Executive Board in July 2014 suggesting that privacy impact assessments were used for new and existing projects.

3.2.4 Document and raise awareness of what to do in the event of a data breach. The reporting of these will need to happen in a tight timeframe and we will have to document what has been lost, how the leak was addressed, etc. We will need to document decision processes, conclusions and breaches thoroughly, as any possible sanctions could be based on how well prepared we were. We currently have a very informal process for dealing with data breaches.

3.2.5 Making extra effort to be transparent to our residents, explaining clearly and simply how personal data is handled.

3.2.6 Keeping a record of consent given for sharing any data. The burden of proof with this is on us and may need to be presented to the relevant data protection authority.

3.2.7 Making sure all relevant staff receive training in data protection so they know what they need to do or when they need to ask questions. Proof of training is important in cases of negligence or malicious actions. On line training has been rolled out to all staff and we are looking at rolling out training in 2017/18 through an external company.

3.2.8 Consideration needs to be given to formalising the role of a Data Protection Officer. This will be a requirement for any company that has more than 250 employees, or processes more than 5,000 people's data.

3.3 A plan of action to address all the above points will be managed by the Corporate Governance Group.

Implications

4 Legal Implication(s)

4.1 The new data protection framework takes the form of a Regulation, the General Data Protection Regulation, and will replace the Data Protection Act 1998. It will be applicable in all member states without the need for implementing national legislation.

5 Financial Implication(s)

5.1 This is unknown at this moment in time. There will be a cost associated with any preparatory work required with meeting the GDPR.

6 Risk Management Implications

6.1 As we handle people's data we are responsible for keeping it safe and are bound by law to comply with data protection regulations. This applies to data whilst it flows between service areas; moves across different systems; is passed between individuals; transitions onto new platforms or programs and is handed to a third party.

6.2 Throughout the GDPR, organisations that control the processing of personal data are encouraged to implement protective measures corresponding to the level of risk of their data processing activities. However, the GDPR is silent on how we should assess and quantify risk.

7 Security & Terrorism Implication(s)

7.1 There are no security and terrorism implications with the recommendation in this report.

8 Procurement Implication(s)

8.1 There are none.

9 Climate Change Implication(s)

9.1 The proposals in this report will not impact on green house gas emissions.

10 Link to Corporate Priorities

10.1 The subject of this report is linked to the Council's Corporate Priority: Engage with our communities and provide value for money.

11 Equality and Diversity

11.1 A full Equality Impact Assessment has been carried out in connection with the GDPR. An initial impact assessment on changes we make resulting from these regulations will be carried out accordingly.

Name of author	Farhad Cantel
Title	Client Support Services Manager
Date	July 2016

Appendix A

General Data Protection Regulations – Summary

The regulation (rather than the current directive) is intended to establish one single set of rules across Europe which EU policy makers believe will make it simpler and cheaper for organisations to do business across the Union.

What is Personal Data

Personal data is defined in both the Directive and the General Data Protection Regulations **(**GDPR) as any information relating to a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Online identifiers including Internet Protocol addresses, cookies and so forth will now be regarded as personal data if they can be (or are capable of being) without undue effort linked back to the data subject. There is no distinction between personal data about individuals in their private, public or work roles. The person is the person.

Controllers and Processors

The Regulation separates responsibilities and duties of data controllers and processors, obligating controllers to engage only those processors that provide sufficient guarantees to implement appropriate technical and organisational measures to meet the Regulation's requirements and protect data subjects' rights.

Controllers and processors are required to implement appropriate technical and organisational measures taking into account the state of the art and the costs of implementation and the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.

The regulation provides specific suggestions for what kinds of security actions might be considered "appropriate to the risk," including:

- The pseudonymisation and/or encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Controllers and processors that adhere to either an approved code of conduct or an approved certification may use these tools to demonstrate compliance.

The controller processor relationships must be documented and managed with contracts that mandate privacy obligations. Ultimately controllers must assure themselves of processors privacy capabilities.

A Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. A Data Processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Fines and Enforcement

There will be a substantial increase in fines for organisations that do not comply with the new regulation. Regulators will now have authority to issue penalties equal to the greater of €10 million or 2% of gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations.

However violations of obligations related to legal justification for processing (including consent), data subject rights, and cross-border data transfers may result in penalties of the greater of €20 million or 4% of gross revenue.

It remains to be seen how the supervisory authority tasked with asking for these fines will work. The current Information Commissioner's Office framework will probably need to change as funding mechanisms will be different.

Data Protection Officers

Data Protection Officers must be appointed for all public authorities, and where the core activities of the controller or the processor involve regular and systematic monitoring of data subjects on a large scale or where the entity conducts large-scale processing of "special categories of personal data" (such as that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs). The latter is likely to apply to some of the larger scale marketing service providers and research organisations, but needs further clarification.

The regulation requires that they have expert knowledge of data protection law and practices. The level of which should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor.

The data protection officer's tasks are also defined in the regulation to include:

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance including managing internal data protection activities, training data processing staff, and conducting internal audits.
- Advising with regard to data protection impact assessments when required under Article 33, Privacy Impact Assessments.
- Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.
- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten and related rights.

Data Protection Officers may insist upon company resources to fulfil their job functions and for their own ongoing training. They must have access to the company's data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line to the highest management level of the company.

Data Protection Officers are expressly granted significant independence in their job functions and may perform other tasks and duties provided they do not create conflicts of interest. The regulation expressly prevents dismissal or penalty of the data protection officer for performance of their tasks and places no limitation on the length of this tenure. The GDPR also allows the data protection officer functions to be performed by either an employee of the controller or processor or by a third party service provider.

Privacy Management

Organisations will have to think harder about privacy. The regulation mandates a "Risk Based Approach:" where appropriate organisation's controls must be developed according to the degree of risk associated with the processing activities.

Where appropriate, privacy impact assessments must be made, with the focus on protecting data subject rights. Data protection safeguards must be designed into products and services from the earliest stage of development.

Privacy-friendly techniques such as using pseudonyms will be encouraged, to reap the benefits of big data innovation while protecting privacy. There is an increased emphasis on record keeping for controllers, designed to help demonstrate and meet compliance with the regulation and improve the capabilities of organisations to manage privacy and data effectively.

Consent

According to the Regulation consent means "any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed." Explicit consent is not generally required.

However although the consent itself need not be explicit, the purposes for which the consent is gained does need to be collected for specified, explicit and legitimate purposes. It needs to be obvious to the data subject what their data is going to be used for at the point of data collection.

Consent should be demonstrable. We need to be able to show clearly how consent was gained and when and consent must be freely given. We cannot insist on data that's not required. Withdrawing consent should always be possible and should be as easy as giving it.

Information Provided at Data Collection

The information that must be made available to a Data Subject when data is collected has been strongly defined and includes:

- The identity and the contact details of the controller and Data Protection Officer.
- The purposes of the processing for which the personal data are intended.
- The legal basis of the processing.
- Where applicable the legitimate interests pursued by the controller or by a third party.
- Where applicable, the recipients or categories of recipients of the personal data.
- Where applicable, that the controller intends to transfer personal data internationally.

- The period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period.
- The existence of the right to access, rectify or erase the personal data.
- The right to data portability.
- The right to withdraw consent at any time.
- The right to lodge a complaint to a supervisory authority.
- Importantly where the data has not been obtained directly from the data subject, perhaps using a 3rd party list, the list varies and includes:
- From which source the personal data originate.
- The existence of any profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

There are some exceptions, notably where the effort would be disproportionate (although this is unlikely be a good justification in day to day circumstances) and, importantly, where the information has already been provided to the data subject. This is likely to cause many headaches to marketers, rather than local authorities, using multiple sources of third party data.

Profiling

The regulation defines profiling as any automated processing of personal data to determine certain criteria about a person. In particular to analyse or predict aspects concerning that natural person' s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

This will impact some marketing processes and services, although the extent of this impact is yet to be understood. It is not clear where profiling will finish and selection starts. Full personalisation and other ad serving techniques, for example, rely on a degree of selection normally built on profiles of behaviour or purchase. It would appear that explicit consent for something like this would be required.

Individuals have the right not to be subject to the results of automated decision making, including profiling, which produces legal effects on him/her or otherwise significantly affects them. So, individuals can opt out of profiling. But, individuals have no right to opt-out of profiling if they have already explicitly consented to it, or if profiling is necessary under a contract between an organisation and an individual, or if profiling is authorised by EU or Member State Law.

Legitimate Interests & Direct Marketing

The regulation specifically recognises that the processing of data for direct marketing purposes can be considered as a legitimate interest. Legitimate interest is one of the grounds, like consent, that an organisation can use in order to process data and satisfy the principle that data has been fairly and lawfully processed.

The act says that processing is lawful if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Direct Marketing has not been defined, so consideration needs to be given to the precise nature of the marketing activity proposed to be covered by this ground for

processing. This could mean that a simple mailing of similar goods and services to existing customers and prospects is completely legitimate without direct consent, but it does not include “Profiling” for marketing purposes which does require consent.

Breach & Notification

According to the regulation a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. It is important to note that the wilful destruction or alteration of data is as much a breach as theft.

In the event of a personal data breach data controllers must notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. If notification is not made within 72 hours, the controller must provide a reasoned justification for the delay. Notice is not required if the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.

When a data processor experiences a personal data breach, it must notify the controller but otherwise has no other notification or reporting obligation. Should the controller determine that the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, it must also communicate information regarding the personal data breach to the affected data subjects. Under Article 32, this must be done without undue delay.

The GDPR provides exceptions to this additional requirement to notify data subjects in the following circumstances:

- The controller has implemented appropriate technical and organisational protection measures that render the data unintelligible to any person who is not authorised to access it, such as encryption.
- The controller takes actions subsequent to the personal data breach to ensure that the high risk for the rights and freedoms of data subjects is unlikely to materialise.
- When notification to each data subject would involve disproportionate effort, in which case alternative communication measures may be used.

Data Subject Access Requests

Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. Where requests to access data are manifestly unfounded or excessive, we will be able to charge a fee for providing access.

Data Subject Access Requests must be executed without undue delay and at the latest within one month of receipt of the request. The current rules stipulate 40 days. Subject access requests must also give all the information relating to purposes that should have been provided upon collection.

The Right to Data Portability

This part of the regulation seeks to drive automated transfers of data (using a common format yet to be defined) between services which primarily process customers automatically. This could include utilities, banks, telecoms and internet service providers.

Retention & the Right to be Forgotten

Data Controllers must inform subjects of the period of time, or reasons why, data will be retained on collection. Should the data subject subsequently wish to have their data removed and the data is no longer required for the reasons for which it was collected then it must be erased.

There is a responsibility for data controllers to take reasonable steps to notify processors and other data recipients of such requests. This area of the regulation is likely to need further clarification.