AUDIT & GOVERNANCE COMMITTEE – 10 January 2018

Implementation of General Data Protection Regulations

Report by Director of Law & Governance

Introduction

1. On 25 May 2018 the European Union General Data Protection Regulation (GDPR) will come into effect and will replace the Data Protection Act 1998 (DPA). Despite leaving the EU in 2019 the UK will still adopt the GDPR.

2. This report provides a high-level overview of the changes in the GDPR, the actions planned to implement and progress against those plans.

Background

3. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the Data Protection Act came into force in 1998. Although the key principles of data privacy still hold true, the new regulation reflects advances in technology, and represents a step increase in responsibilities for safeguarding personal data, and maintaining audit trails of what has been done with personal information, when it was done and why.

4. The main changes are as follows:

5. Consent: The conditions for consent have been strengthened, and organisations will no longer be able to use long illegible terms and conditions full of legalese. The request for consent must use clear and plain language, and be distinguishable from other matters. It must be as easy to withdraw consent as it is to give it.

6. The default age at which a person is no longer considered a child is 16, but GDPR allows member states to adjust that limit to anywhere between 13 and 16. Data controllers therefore must know the age of consent and cannot seek consent from anyone under that age. Instead, they must obtain consent from a person holding parental responsibility. They must also make "reasonable efforts" to verify that the person providing that consent is indeed a parental figure

7. Breach Notification: Breach notification is mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach.

8. Right to Access: Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.

9. Right to be Forgotten: Also known as Data Erasure, the right to be forgotten entitles the data subject to have their personal data erased, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. The exception to this right is if the personal data belonging to the data subject is related to the delivery of a statutory service.

10. Data Portability: Data portability is the right for a data subject to receive the personal data concerning them, which they have previously provided, in a "commonly use and machine readable format" and have the right to transmit that data to another controller.

11. Privacy by Design: Privacy by design requires the inclusion of data protection from the onset of the design of systems or process, rather than as an addition; i.e. think about data protection at the beginning and throughout the design process. Organisations should only process the data that is necessary for the completion of its duties, as well as limiting the access to personal data to those needing to act out the processing.

12. Penalties: Under GDPR organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements, e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines, e.g. an organisation can be fined 2% for not having their records in order, not notifying the supervising authority and data subject about a breach or not conducting an impact assessment.

13. Data Protection Officers: It is mandatory to appoint a Data Protection Officer.

14. Increased Territorial Scope: The extended jurisdiction of the GDPR mean that it applies to all organisations processing the personal data of data subjects residing in the Union, regardless of the organisation's location.

15. The implementation of the GDPR at Oxfordshire County Council is being coordinated centrally, but privacy and data protection will be everyone's responsibility. Support will be given to staff through a range of tools, including guidance, toolkits, templates and training, in order to help them engage with the changes and implement them in their service areas

16. The Information Commissioner's Office (ICO) published guidance - "Preparing for the General Data Protection Regulations (GDPR) 12 steps to take now" – has been used as the basis for the implementation plan and this report.

Preparation for the General Data Protection Regulations – ICO guidelines

17. Below are the ICO guidelines used as the basis for the implementation plan and the current progress against each one.

Awareness

18. CLT have been briefed and agreed to provide their support.

19. Two half day key stakeholder workshops were held on 14th November; this was aimed at service manager level. The workshop covered the fundamentals of the GDPR; the plan for implementation and progress against the plan as well as workshops covering Privacy notices and Consent, and Security Incidents.

20. There was a GDPR stand at the staff conference. Materials were prepared covering the ICO 12 steps, individual rights, consent, privacy notices and privacy by design as well as a GDPR quiz, a 'guess the ICO fine' competition and a countdown clock showing how many days, hours and minutes until 25th May 2018.

21. Members training will be held in February 2018.

22. A series of monthly GDPR intranet headlines starting in May 2017 up to May 2018; each with a different GDPR related subject.

23. Regular posting on the GDPR Yammer group.

24. A series of site surgeries were held at Speedwell, Abbey House, Samuelson House, Knights Court, County Hall, Mount House and Nash Court between 20th November and 7th December. The materials produced for the staff conference were also distributed at the site surgeries.

25. Following the stakeholder workshop and site surgeries there are a series of targeted briefings to individual teams; these briefings cover the basics but are also tailored to each team.

26. The data protection e-learning course is being revamped and will include GDPR updates. The plan is to launch this at the end of January/beginning of February and for it to be mandatory for all staff. It will be modular so that there will be sections that everyone has to complete and other more specific e.g. consent that only certain groups of staff will need to complete.

27. There will be a set of Information Security videos coming out in January; one of these will be GDPR specific.

28. A GDPR toolkit is being devised and content released as it is available; this will eventually replace some of the Information Management intranet content.

Information you hold

29. The identification of all business information, however it is held, is being gathered and recorded in the Information Asset Registers for all service areas. These registers will identify all the information we hold across the council and some of the information about that asset e.g. how and where it is shared, what records retention is applied, what consent is sort, what format it is e.g. database, excel etc, what types if information is held in the asset.

30. There are approximately 55 interviews in total. Once each one is complete it is analysed to identify areas of concern e.g. no sharing agreement, no consent etc. and marked for action. The aim is for all Information Asset Registers to be complete by the end of January 2018

31. Once a group of registers are complete for a service area an action plan will be developed to address the areas of concern and to create a data map and information process map for that service area. Following this the security of processing and legality of processing will be assessed, and changes made as needed.

32. It is also intended for these to be used to identify information for individual rights post go-live.

Communicating privacy information

33. A standard privacy notice has been created. It has been designed to contain all that is needed but to be generic and not service specific. The reasoning behind this is that we will have one privacy notice on the website that can be used by all services rather than different privacy notices with different wording which could cause confusion. It will also mean that if it needs to be changed we only have to change in one place.

Individuals' rights

34. As previously stated we will use the Information Asset Registers to identify where we hold personal data.

35. The work to create the processes for data portability, data correction and the right to be forgotten has started.

Subject access requests

36. The Subject Access Request process has been revised to account for the reduced time period of 30 days.

Lawful basis for processing personal data

37. The privacy notice includes the lawful basis for processing data.

38. The processing of data by the council and on the council's behalf will be audited and assessed for legality.

Consent

39. The consent processes and notices are being reviewed.

40. The design of the process and system to collect and record consent is in progress.

Children

41. This is included in the other consent work.

Data breaches

42. The security breach procedure has been revised to reduce the timings for initial breach reports to be returned to the Information Management team within 1 working

day. The Information Management team will assess whether this should be passed onto legal for consideration of reporting the breach to the ICO.

43. The new procedure went live on the 8th September to allow time for it to be refined if needed before May 2018.

Data Protection by Design and Data Protection Impact Assessments

44. The digital platform team and the Project Management Office have been made aware of the requirements for Privacy by Design for any new systems or processes.

45. Privacy by Design was discussed at the stakeholder workshop, site surgeries and team specific briefings.

46. Privacy by Design guidance will be included in the GDPR toolkit.

47. Data Protection Impact Assessment templates and guidance have been produced and are being used.

Data Protection Officers

48. The Data Protection Officer role will be allocated to an individual within the council.

International

49. We do not have to do anything with this requirement.

Other Work

50. All Information Governance/Management policies are being reviewed to include relevant GDPR content. The opportunity is being taken to consolidate policies where relevant.

51. All providers and suppliers are being contacted to request evidence of their compliance with GDPR, and a variation to contract applied where appropriate.

52. Information Governance requirements for tenders and contracts is being revised

53. Information Management Risk Assessments have been revised to include GDPR

Issues

54. Information from the ICO is still being released; therefore, some assumptions have to be made until the information from the ICO is clearer. This issue is being mitigated by gathering information and advice through networking with other local authorities and partner organisations, attending conferences, engaging with webinars and attending workshops.

55. At this stage it is not known what the impact of the new regulations will be post go-live. There is the potential for an increase in demand regarding the new and enhanced individual rights that may result in the need for additional resource to be allocated to managing the requests.

56. With the hard deadline and a lot of work to be done there is a possibility we may not be fully compliant by 25 May 2018. However, there is an action plan in place to deliver by May and progress is being made to the expected deadlines.

Summary

57. Good progress has been made in some areas but there is still a lot of work to do.

58. This is a good opportunity to review the council's policies, processes, consent and sharing agreements, and data management; and renew and consolidate where appropriate. The result will be a more streamlined and transparent governance of data within the organisation.

RECOMMENDATION

59. The Committee is RECOMMENDED to

a) note the contents of the report; and

b) advise of areas of concern.

Nick Graham
Director of Law & Governance

Contact Officer: Caroline Parker
December 2017