

General Data Protection Regulation

REPORT TO AUDIT AND STANDARDS COMMITTEE



DATE	10/01/2018
PORTFOLIO	Resources and Performance Management
REPORT AUTHOR	Ian Evenett
TEL NO	01282 425011 Ext 7175
EMAIL	ievenett@burnley.gov.uk

PURPOSE

1. To inform members of the requirements and progress on meeting the General Data Protection Regulation

RECOMMENDATION

2. The Committee considers the progress report and comments on its contents.

REASONS FOR RECOMMENDATION

3. Members can monitor the management of the risk and the control arrangements.

SUMMARY OF KEY POINTS

General Data Protection Act Regulation (GDPR)

4. The GDPR has been in discussion in the European Union for several years. This must be implemented in the UK by May 2018, this will be before the UK leaves the EU and so are enforceable. The Government is progressing a bill through Parliament to implement aspects of the GDPR (the Directives) to apply in the UK (The Data Protection Bill). This bill also addresses some other related areas of Data Protection.
5. The regulation directly replaces the Data Protection Act 1998 and update this area of legislation for the changes information uses which have evolved.
6. Once the UK has left the EU it will be up to the Government as to how it will legislate in this area. The stated intention is to follow the new requirements.
7. The objectives of the GDPR is to achieve a consistency of Data Protection (DP) legislation across the EU and a wider scope to wherever EU citizens data is processed. It aims to clarify the meanings of consent (the agreement of the data subject to allow their data to be processed. It increases the rights for data subjects over their data. It requires data systems to have data protection incorporated into them and the impact of new systems to be assessed. There are higher penalties for non-compliance, and a requirement to report data breaches. It also requires the appointment of Data Protection

Officers for some organisations.

8. The Information Commissioner (ICO) has provided some useful guides to prepare for the GDPR (<https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>) , a guide to the GDPR (<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>) and the Data Protection Bill (<https://ico.org.uk/for-organisations/data-protection-bill/>). The 12 points of preparing for the GDPR are covered below.

Awareness

9. The first step in the process has been to make sure that key officers are aware of the GDPR. The Council has had in place a team of officers to plan the Council's response to the GDPR based on the advice and guidance which has been provided from various sources. The team has been meeting since May 2016, when the bill was passed in the EU and includes a member of Management Team.
10. The team has been monitoring the development of the GDPR guidance and planning the main elements of the responses.
11. Early changes were the incorporation of the GDPR requirements into the Council's IT Strategy and policy changes to incorporate the requirements of Data Protection by design.
12. In May 2017, the team of information governance officers across the Council and Liberata was briefed on the GDPR and the progression of the first steps. This team lead in services addressing Freedom of Information and Data Protection Issues.
13. In October 2017 a revamped Data Protection Awareness course was launched as mandatory training for colleagues.
14. A GDPR e-learning course is being prepared for wide use.

Information Held

15. The GDPR team decided that we needed to more about all the information that the council held. This information would be gathered by an on-line survey.
16. The objective of the survey is to record key data protection elements about the data we hold. This would provide the basis for further progress towards meeting the GDPR.
17. A GDPR survey was devised and launched in June 2017. It was hoped that this could be completed quickly but we do not expect completion until Dec 2017.

Communicating Privacy information

18. The Council's current privacy notice was reviewed quite recently so met the then current ICO guidance on Privacy Notices. The team's view is that the GDPR will need to be far more specific about what data is held, why it is held and how it is processed. The information for most of these details is being gathered as part of the survey.

Individuals Rights

19. There are some new rights provided to data subjects under the GDPR which need to be incorporated into Council data systems. For example, the deletion of a data subjects' information. Many of the Council's systems do not permit the deletion of data, the survey is gathering data on this. Many of the Council's data systems require data to be held and will be exempt from this provision but others will need to be adapted to cope with this.

Subject Access Requests

20. The Council receives and deals with Subject Access Requests on a periodic basis for a minimal charge. Under the GDPR these requests will become free and so it is anticipated that the number and frequency of requests will increase. We will also have less time to respond to these requests. Whilst the Council has a system part of the survey is do the

data systems have ways to deal with subject access requests.

Lawful basis for Processing Personal Data

21. This is altered under the GDPR. Key information systems are held by the Council as a legal requirement, others are held to deliver services in the public interest. It is important that the Council records and explains the lawful basis for processing the personal data and this then addresses some of the rights and exemptions which apply linked to that basis. For example the right to deletion for Council Tax is not applicable as this is a legal requirement.

Consent

22. This is where a data subject agrees to the processing and this is a legal basis for processing the data. The Council is reviewing where it collects consent to processing the data, too ensure that these consents meet the updated requirements and that these consents are retained.

Children

23. The survey is identifying where the data may relate to children and if consent is required then is the appropriate parental consent obtained.

Data Breaches

24. The Council has existing policies and procedures to address Data Breaches and these are being reviewed to consider the requirements to quickly detect, report and investigate serious Data Breaches.

Data Protection by Design and Data Protection Impact Assessments

25. As stated earlier we have already incorporated designing in data protection into our policies and procedures. The council has been following the ICO's code of practice on impact assessments for a few years now so this should require minimal adjustments.

Data Protection Officers

26. A public authority like the Council is required to have a Data Protection Officer. This is already covered in the Constitution as the Head of Governance, Law, Property and Regulation. However, given the new requirements of the role, this is being reviewed.

International

27. The Council only operates in the UK so this will not be a major issue and we will be covered by the Information Commission's Office (ICO) for compliance. However, the Council does process some data from EU citizens which will have implications after the UK leaves the EU. Where the Council holds data in cloud facilities, the locations of the data servers will need to be established.

Fines

28. Part of the legislation increases the maximum fines imposable for non-compliance with the GDPR. All the actions we are taking are working toward reducing the risk of fines and data breaches which would impact on the Council's reputation.

FINANCIAL IMPLICATIONS AND BUDGET PROVISION

29. It is intended to incorporate any changes within existing budgets although income from fees for subject access requests will need to be removed.

POLICY IMPLICATIONS

30. Further changes will be incorporated into the Councils IT security Policies. A specific Data protection policy to assist the process would be useful

DETAILS OF CONSULTATION

31. None

BACKGROUND PAPERS

32. None

FURTHER INFORMATION**PLEASE CONTACT:**

**Ian Evenett (Internal Audit Manager) Ext
7175**

ALSO:

Nadeem Ukadia (Senior Auditor) Ext 3150