Central Bedfordshire Council

AUDIT COMMITTEE 8 JANUARY 2018

UPDATE ON PREPARATIONS FOR THE GENERAL DATA PROTECTION REGULATION (GDPR)

Advising Officer: Stephan Conaway, Chief Information Officer (Stephan.conaway@centralbedfordshire.gov.uk)
Contact Officers: Sean Dykes, Information Security Manager (sean.dykes@centralbedfordshire.gov.uk)
Maria Damigos, Corporate Lawyer, LGSS Law Ltd

Purpose of this report

1. The report seeks to provide an update on preparations for the General Data Protection Regulation (GDPR) and the Council's plans for compliance.

RECOMMENDATIONS
The Committee is asked to:

i. Note the progress regarding preparations for the GDPR.

Overview and Scrutiny Comments/Recommendations

2. This report is to update the committee on preparations for the GDPR following the last Audit Committee on 27 Septempber 2017. No decision is necessary and the report has not been considered by the Overview & Scrutiny Committees.

Introduction

3. At the Audit Committee meeting of 27 September 2017, Members were briefed on the GDPR and the Council's preparations. This brief is to update on those preparations.

Background

4. How personal data is dealt with in the UK is currently governed by the Data Protection Act 1998 (DPA) which was enacted to bring the

European Union (EU) Data Protection Directive 1995 into UK law.

5. The GDPR is an EU Regulation by which the European Parliament, the Council of the European Union and the European Commission intended to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulations within the EU.

6. The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 after a two-year transition period. It does not require any enabling legislation to be passed by national governments and is thus directly binding and applicable whilst the UK is a member of the EU. The UK government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

7. A Data Protection Bill is currently progressing through Parliament which will incorporate the requirements of the GDPR into UK legislation. It is likely that the GDPR requirements will be applicable after the UK leaves the EU.

Summary of Changes

8. The GDPR extends the rights and responsibilities contained in the DPA. Apart from private use, it will apply to all individuals and organisations storing or using personal data and will include a 'data processor' (someone who acts on a data controller's behalf).

9. Under the DPA the data controller was responsible for the data. Data processors will now have specific obligations in relation to record keeping and processing and will have more legal liability in the event of a breach.

10. The key areas of change are:

    a. Lawful processing

    For processing to be lawful under both the DPA and the GDPR, a lawful basis must be identified. The requirements for lawful processing under GDPR will change slightly.

    b. Consent and Privacy Notices

    The definition of consent under the GDPR is more strictly defined than under the DPA. . Simple procedures for withdrawing consent must be in place.

    The Council as a public authority and an employer will need to take particular care to ensure that consent is freely given (or rely on another basis for processing).

Where consent is not given or required individuals must be provided with a notice detailing what information is held and why, what will be done with the information and the persons rights in respect of that data.

c. Children's personal data

The GDPR contains new provisions intended to enhance the protection of children's personal data.

d. Individual's Rights

The GDPR both strengthens existing rights under the DPA and creates new rights for individuals.

e. Accountability and Governance

The GDPR includes specific provisions that promote accountability and governance which complement the GDPR's transparency requirements.

f. Breach Notification

The GDPR will introduce a duty to report all incidents where there has been a significant breach to the ICO within 72 hours. The Council already has a successful reporting system in place which will only need minor updates to comply with the timescale for reporting.

g. Transfers of personal data to third countries or international organisations

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

11. The GDPR also significantly increases the maximum fine for a data protection breach which can be imposed from £500,000 to either 10 million euros or 20 million euros (or 2% or 4% of global turnover in the preceding financial year respectively) depending on the type of breach.

Current Position

12. A GDPR Working Group has been set up to monitor and implement the requirements of the GDPR within the Council. The group is made up of the Information Security Manager, LGSS Corporate Lawyer, Head of Internal Audit, Deputy Chief Information Officer, Records and Risk Officer and Information Request Officer. Updates are provided to the

Monitoring Officer, SIRO/Chief Information Officer, CMT and the Information Assurance Group (IAG) as necessary.

13. The IAG includes senior officers from Human Resources, Internal Audit, IT, Children's Services, Adult Services and the Caldicott Guardian and can provide further support, initial approval and sense checking of proposed draft documents and procedures.

14. Appendix A sets out the ICO Recommended Actions and updates the Council's status as regards those actions as at 13 December 17.

15. The template for consent and privacy notices has been completed and we are about to begin the build of an electronic version of this form prior to testing. Once rolled out, it is proposed that drop in sessions will be available for queries.

16. The Council's data protection training is to be reviewed and revised early 2018 and this will also take account of the new requirements of the GDPR. This will commence in January 2018.

17. At the last Audit Committee various comments were made regarding compliance, planning and training and these have been fed into the work plan and will be incorporated into preparations.

18. Council Priorities

19. Compliance with legal obligations ensures that Council delivers it priorities and contributes to the achievement of all the Council's priorities.

Corporate Implications

Risk Management

20. Failure to implement the requirements of the GDPR would be a breach of the law. This is already identified as a significant governance issue within the draft Annual Governance Statement for 2016/17. It is however anticipated that all requirements will be met or implemented.

Staffing (including Trades Unions)

21. There are none.

Legal Implications

22. The GDPR will become law in the UK on 25 May 2018. The Council will need to comply with the GDPR and any other applicable legislation.

Financial Implications

23. Although this report has no financial implications, resources will be required for implementation of, and compliance with, the GDPR which will either be met from existing budgets or will be the subject of further reports to the appropriate committee or Executive.

Equalities Implications

24. None arising directly from this report.

Conclusion and next Steps

25. Development of a detailed Action Plan with ongoing awareness raising for all staff. Drop in sessions to assist departments with specific queries are also to be arranged and delivered.

Appendices

The following Appendices are attached:

Appendix A – ICO Recommended Actions – Current Position Dec 17

Further information can be obtained from:
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/