Central Bedfordshire Council

AUDIT COMMITTEE 27 September 2017

Update On The General Data Protection Regulation

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 overview of the General Data Protection Regulation (GDPR) and the Council's plans for compliance.

RECOMMENDATIONS
The Committee is asked to:

i. Note the position with the GDPR.

Overview and Scrutiny Comments/Recommendations

2. This is a report to update the committee on the GDPR. No decision is necessary and the report has not been considered by the Overview & Scrutiny Committees.

Introduction

3. At the Audit Committee meeting of 29 June 2017 Members considered the position with the GDPR and asked for a report from the Chief Information Officer to update Members.

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 to be considered by parliament in September to incorporate the requirements of the GDPR into UK legislation. It is anticipated that this will ensure that the GDPR requirements are still 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. The Council will be able to rely on consent, compliance with a legal obligation, protection of the vital interests of a data subject or another person and performance of a task carried out in the public interest or in the exercise of official authority vested in it.

    b. Consent and Privacy Notices

    The definition of consent under the GDPR is more strictly defined than under the DPA. It must be a freely given, specific, informed and an unambiguous indication of the individual's wishes. There must be a positive opt-in - consent cannot be inferred from silence, pre-ticked boxes or inactivity. 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.

LGSS and the Information Security Manager are developing consent templates and privacy notices that can be used across the Authority.

c. Children's personal data

The GDPR contains new provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, the Council must ensure that any privacy notice is written in a clear, plain way that a child will understand.

Specialist advice from Children's Services will be obtained to help with the drafting of the consent and privacy notice templates.

d. Individual's Rights

The GDPR both strengthens existing rights under the DPA and creates new rights for individuals. GDPR provides the following rights for individuals:
The right to be informed
The right of access
The right to rectification
The right to erasure
The right to restrict processing
The right to data portability
The right to object
Rights in relation to automated decision making and profiling.

Whilst the Council may not currently carry out activities which are affected by some of these rights the position will be monitored.

e. Accountability and Governance

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

New requirements will include records of processing activities, privacy impact assessments, privacy by design and the appointment of a Data Protection Officer.

The Council must also be able to show that the requirements are being complied with. The Council's governance measures will be reviewed and updated to take account of any requirements not already in place.

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. The Council will need to clarify how this applies to information held in "the cloud" and ensure appropriate safeguards are in place.

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 the Council's current position.

15. As detailed above a template is being drafted which will allow all departments to create/update their privacy notices or consents. 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.

17. A more detailed Action Plan is also to be developed. It is anticipated that any areas of weakness identified by Internal Audits, the privacy notices or consents and/or drop in sessions will feed into both the Action Plan and the new data protection training where appropriate.

Council Priorities

18. 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

19. 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)

20. There are none.

Legal Implications

21. 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

22. 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

23. None arising directly from this report.

Conclusion and next Steps

24. 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

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