Item 5.2

Report

Data Protection Reform

Edinburgh Integration Joint Board

2 March 2018

Executive Summary

1. From 25 May 2018, the existing Data Protection Act 1998 will be replaced by new legislation in the form of the EU General Data Protection Regulation (GDPR), and a new Data Protection Act. This report sets out the main features of the legislation and its likely impact, and details the current approach to ensuring compliance.

Recommendations

2. The Integration Joint Board is asked to:

   i. note legislative developments concerning the introduction of GDPR and a new Data Protection Act, and their significance for integrated services and the Edinburgh Integration Joint Board (IJB)

   ii. note a Memorandum of Understanding has been signed by NHS Lothian and the Council which provides a framework for promoting compliance with data protection legislation

   iii. note the statutory role of Data Protection Officer (DPO)

   iv. to delegate authority to the Interim Chief Officer to appoint a DPO for the IJB.

Background

3. From 25 May 2018, the existing Data Protection Act 1998 will be replaced by new legislation in the form of the GDPR and a new Data Protection Act. Together these measures are referred to as “Data Protection Reform” for the remainder of this report.

4. The overall aim of the legislation is to establish a harmonised data protection framework across the EU, and to update the approach to the processing of

personal data in the digital age. It imposes new obligations on organisations and expands and strengthens the rights of individuals.

5. The UK Government has confirmed that the European Union (Withdrawal) Bill will bring the GDPR onto the UK statute books after the UK has left the EU. The new Data Protection Act sets our further details of how GDPR will apply in the UK.

6. Data Protection Reform makes some significant changes to the rules governing the processing of personal data, for which organisations must plan and prepare. This report highlights the key features of the new legislation and sets out developments (to date) to promote compliance.

Main report

7. A report was presented to the IJB on 16 June 2017 on its statutory responsibilities in relation to information governance. It confirmed that under data protection legislation, the IJB is a joint data controller with the City of Edinburgh Council ("the Council") and NHS Lothian, in relation to the joint processing of personal data for the delivery of delegated functions.

8. To achieve appropriate governance, the report in June 2017 also confirmed that the IJB is a signatory to the Pan-Lothian Information Sharing Protocol, and a Memorandum of Understanding (MoU) was being drafted to ensure that responsibilities in relation to the processing of personal data are set out and understood between the IJB, the Council and NHS Lothian.

9. The MoU will be supplemented by local documentation which will address and set out operational arrangements around information compliance and management. The MoU also introduces the concept of a "Lead Data Controller" to take responsibility in ensuring information governance standards are met and followed. The Lead Data Controller will be the Council or NHS Lothian and generally dependent on whether the function is predominately social care or health focused.

10. The MoU has now been signed off and provides the framework to ensure compliance with Data Protection Reform. The remainder of this report highlights the key features of the new legislation and current issues, which require further consideration.

Transparency

11. Transparency is a central feature of the new legislation. Under the current Data Protection Act, organisations should let people know how their personal data is managed and processed, through a "privacy notice". Under Data Protection Reform, there is a requirement to provide greater transparency through more

details regarding how personal data is used, shared and stored. Privacy notices will need to ensure people are told about processing in sufficient detail, and include several mandatory elements.

Governance and accountability

12. The new legislation includes provisions that promote accountability and governance. These complement the greater transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, Data Protection Reform elevate their significance.

13. Organisations are expected to put in place comprehensive but proportionate governance measures, including data protection policies, procedures, training and audits of processing activities. The Council and NHS Lothian have established information governance frameworks and the MoU will help to demonstrate good governance and on-going accountability in these areas.

14. The new legislation makes provision for several good practice tools that are currently not mandatory, but will be legally required in certain circumstances. One such provision is “Privacy by Design”, where organisations must consider privacy and data protection implications when initiating new projects, decisions or information systems that involve the processing of personal data. It will become mandatory to complete a Data Protection Impact Assessment (DPIA) for such projects, to ensure that privacy issues are considered and documented. The Lead Data Controller will take responsibility for the DPIA for integrated services.

15. The legislation also introduces a new statutory duty to report certain types of data breaches to the UK Information Commissioner, and in some cases to the individuals affected. A notifiable breach must be reported within 72 hours of the organisation becoming aware of it. The MoU sets out that the Lead Data Controller will be responsible for monitoring and reporting breaches, as appropriate.

Rights of individuals

16. Data Protection Reform creates some new rights for individuals, as well as strengthening some of the rights that exist under current legislation. New rights include a “Right to be Forgotten” (that is, for an individual to have their personal data destroyed in certain circumstances) and a “Right to Data Portability” (that is, for an individual to have their personal data transferred from one service provider to another).

17. Changes to existing rights include a revised timescale for Subject Access Requests (where an individual requests access to the personal data held about

them), which must be answered within one month (but with the possibility of extending the deadline by a further 2 months), rather than 40 days under existing legislation.

18. Arrangements and practical considerations for upholding the information rights of individuals will be the responsibility of the Lead Data Controller.

Register of processing

19. Organisations need to compile a register of data processing, which documents each process involving personal data – setting out the purpose of processing; condition(s) relied upon to make processing lawful; privacy notices issued to data subject; how data is stored used and how long it is kept; and with whom it is shared. The register must be made available to the public.

20. The Council and NHS Lothian will have their own registers as part of their compliance arrangements. These are likely to capture data processing activities in relation to delegated functions. However, to promote transparency and accountability, it would be helpful if the Edinburgh Health and Social Care Partnership (HSPC) maintained a register that captured all delegated function processing activities. The small amount of processing that the IJB has direct responsibility for (e.g. complaints management) must also be recorded and could form part of this register.

21. The register of processing is an effective way of assessing compliance of each process against the requirements of data protection legislation. Typical actions arising might involve: revising privacy notices; making sure a lawful condition for processing has been identified and documented; ensuring there are agreements in place with other people and organisations to share personal data; and ensuring that there are retention rules in place for all personal data held; and that these rules are routinely implemented.

22. The Lead Data Controller will be responsible for identifying and mitigating risks identified through this process and maintaining a risk-based approach to processing activities.

Data Protection Officer

23. Data Protection Reform introduces a statutory role of Data Protection Officer (DPO), which is mandatory for public authorities. The DPO will be responsible for assuring compliance with data protection legislation, and must have a direct reporting route to senior management.

24. The DPO will be expected to have sufficient professional knowledge to inform and advise the organisation, and to act independently with sufficient authority to identify, report and rectify risks relating to the processing of personal data. The DPO must be in post by 25 May 2018.

25. The DPO function can be a shared role with other public authorities. The IJB should consider approaching its partners to discuss this option. The DPO would be expected to provide regular reports to the IJB and engage with the Edinburgh Health and Social Care Partnership on a regular basis.

Preparing for data protection reform

26. The Information Commissioner's Office (ICO) has stated that GDPR is an evolution in data protection, not a revolution. While organisations need to do more in terms of accountability regarding their use of personal data and respecting the rights of individuals, they do so on foundations already in place for the last 20 years through the current Data Protection Act. For organisations that comply with the Act and have effective information governance arrangements in place, Data Protection Reform is something to plan for rather than fear.

27. In relation to integrated services, services will have to assign and commit resources to implement any improvement actions, and ensure that identified risks are managed. To facilitate this process, a Data Protection Reform readiness questionnaire has been circulated to integrated teams to highlight areas for improvement and associated risks. The Council and NHS Lothian information governance teams will support integrated services and the Operations Manager (Risk, Information, and Compliance) in making any required changes.

Key risks

28. The MoU will provide the framework for governing information compliance arrangements at a strategic and operational level. The MoU was signed-off on 15 February to ensure appropriate levels of compliance.

29. Failure to prepare for Data Protection Reform could have a serious impact on the IJB's ability to meet its statutory obligations under data protection legislation leading to major financial and legal penalties, as well as significant reputational damage for the organisation.

Financial implications

30. Failure to comply with the Data Protection Reform requirements could lead to significant financial penalties.

Implications for Directions

31. None.

Equalities implications

32. There are no equalities issues arising from this report.

Sustainability implications

33. There are no sustainability implications arising from this report.

Involving people

34. Data Protection Reform upholds and strengthens the information rights of individuals and ensures that their personal data is processed appropriately and lawfully.

Impact on plans of other parties

35. The Joint Information Governance Group discuss information governance arrangements and issues to ensure a consistency of approach between NHS Lothian, the Lothian councils, and Lothian Integration Joint Boards.

Background reading/references

Guide to the General Data Protection Regulation – UK Information Commissioner

Draft Data Protection Bill – UK Information Commissioner

EU Working Party Guidelines – Role of the Data Protection Officer

Report author

Michelle Miller

Interim Chief Officer, Edinburgh Health and Social Care Partnership

Contact: Kevin Wilbraham, Information Governance Manager (CEC)

E-mail: | kevin.wilbraham@edinburgh.gov.uk Tel: 0131 469 6174

Appendices

None