The Vale of Glamorgan Council

Cabinet Meeting: 5 February, 2018

Report of the Leader

Data Protection Changes

Purpose of the Report

1. To advise of the new Data Protection legislation and its impact upon the Council and to authorise the necessary actions in order to ensure compliance.

Recommendations

1. The contents of this report are noted.
2. The Council's Data Protection Policy and procedures be updated to take into account the new legislative provisions.
3. The Data Protection Training / Awareness Courses be updated to reflect the new statutory provisions.
4. The Information Commissioners document "Preparing for the General Data Protection Regulation (GDPR)" be utilised as an action plan for implementation.
5. The Information Manager (Lawyer) be designated the Data Protection Officer under the terms of the GDPR.
6. A further report to be brought to Cabinet to update on progress in relation to the implementation of GDPR.

Reason for the Recommendations

1-6. To ensure compliance with the law.

Background

2. The current legislative regime in relation to data protection stems from the Data Protection Act 1998 which implemented European Directive 95/46/EC in the UK. This regime has been operational in the UK since 1st March, 2000. As part of its membership of the European Union, the UK was party to and subject to a new EU inspired Data Protection Law, the General Data Protection Regulation (GDPR) Regulation EU2016/679 which is currently due to come into force in the UK upon 25th May, 2018. The intention is that this legislation will come into effect immediately on this date, there will be no transitional periods.

3. The GDPR has similarities with the existing UK Data Protection Act (DPA), however it has several new features, which includes extending the existing principles thus placing additional obligations upon organisations regarding how information is processed and stored, recording keeping and accountability. It introduces mandatory data breach reporting, stronger penalties for breaches and non-compliance, enhanced rights for individuals and data portability provisions together with an obligation to have a designated Data Protection Officer. Generally the provisions will tighten up the existing regulatory regime. There is work to be undertaken across the Council, both at policy level and implementation level, in order to comply with the Regulation.

4. The Government has also introduced a new Protection Bill. The Data Protection Bill will replace the 1998 Act to provide a comprehensive legal framework for Data Protection in the UK, supplemented by the GDPR until the UK leaves the EU. While the UK remains a member of the EU all the rights and obligations of EU membership will remain in force. When the UK leaves the EU the GDPR will be incorporated into UK domestic law under the European Union Withdrawal Bill. The Bill and the GDPR apply substantively the same standards to the majority of data processing in the UK in order to create a clear coherent Data Protection regime. It also sets out certain delegations that provide exemptions from the GDPR in order to deal with aspects relating to areas specific to domestic arrangements within England and Wales..

5. Therefore until the UK leaves the EU the GDPR will operate in tandem with the Bill. When the UK leaves, the Government will restore to a wholly domestic regime for our Data Protection laws but the Bill allows for continued application of GDPR standards. Accordingly both the bill and the GDPR will apply to the UK.

Relevant Issues and Options

6. The key changes under the GDPR are as follows:

Accountability Principle

7. The most significant change is how organisations show they are compliant with the law. In this respect it introduces a new accountability principle in Article 5.2 which provides "The controller shall be responsible for, and be able to demonstrate, compliance with Paragraph 1(the principles) ". This is a fundamental change to the existing regime.

8. To comply with this the Council will need to document the decisions we take on processing and review governance arrangements. The Information Commissioner's guidance on this matter has advised that you organisations be required to make these records available for the purposes of an investigation. Therefore there will be a greater responsibility on the Council to retain records as to how it processes and reviews its processing arrangements.

9. This includes an obligation upon organisations to maintain a "record of processing activities" also known as a data register, which must be made available to the regulator (the Information Commissioner in the UK) on request, and producing much more detailed privacy notices. Details regarding this are referred to below.

Application

10. The GDPR applies to personal data, however the definition is more detailed and provides for a wide range of personal identifiers, including IP addresses. It applies to automated personal data and manual filing systems.

Principles

11. Like the DPA, the GDPR's data protection principles set out the main responsibilities for organisations in relation to Personal Data. These are:

    Personal data shall be:

    (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

    (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

    (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

12. There are two classes of personal data:- ordinary personal data and special category personal data. Special category personal data is high risk personal data and includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, offences or alleged offences, physical or mental health, genetic data, biometric identification data, sexual life, sexual orientation.

Lawful Processing

13. Organisations need to identify the legal basis for processing personal data before they can process it and this needs to be documented.

14. The Commissioner's guidance on implementation provides "You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it".

15. Accordingly, each area of processing in each Department will need to undertake an audit of what personal data is processed and why, consider which legal grounds are relied upon, consider if the data falls within one of the special categories of data, whether or not the personal data relates to criminal convictions and offences and then draft a privacy notice which will encompass all of these aspects and will have to be checked for compliance.

16. Organisations can now be fined for breach of this provision.

Consent

17. Consent is one of the legally permissible reasons where data can be processed and retained. Under the GDPR this will require some form of clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute consent. Consent must be verifiable. This means that some form of record must be kept of how and when consent was given. Implementation of the GDPR will require a review of consent mechanisms to ensure that they meet the standards required under the legislation.

18. The ICO advise that consent should be the last basis utilised and that the other options should be considered. The other legally permissible reasons for processing ordinary personal data are:-

- Necessary for the performance of a contract with a Data Subject;
- Necessary for a legal obligation;
- Necessary to protect the vital interests of a data subject or another person;
- Necessary for the performance of a task in the public interest or in the exercise of official authority;
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

19. The legal basis for processing special categories of personal data are:-

- Explicit consent;
- Preventing or detecting crime/preventing fraud;
- Regulatory activities;
- Public functions;
- Employment law, social security law or law relating to social protection;
- Employment benefits (life insurance/pensions);
- Monitoring equal opportunities (race, disability, sexual orientation and religion)

20. Organisations can be fined for breach of this provision.

Children's Personal Data

21. The GDPR contains new provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, organisations must ensure that the privacy notice is written in a clear, plain way a child understands. This may affect the Council in terms of the provisions of play groups and youth initiatives.

Individual Rights

22. The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. Individual Rights will include :-

- A right to be informed;
- A right to access;
- A right to rectification;
- A right to erasure
- A right to restrict processing;
- A right to data portability;
- A right to object;
- Rights in relation to automated decision making

23. Privacy Notices were a requirement under the DPA but have been extended in terms of contents under the GDPR as originally they contained four points now under the GDPR there are 13 points to consider and adhere to. A privacy notice explains to individuals details of the information you hold and how you use that information. The GDPR states that the information you provide to individuals about how you process their personal data must be concise, transparent, intelligible and easily accessible. It should be written in clear and plain language, particularly if addressed to a child and free of charge.

The Right of Subject Access

24. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of processing. Differing from existing Subject Access, organisations must now provide a copy of the information free of charge. Organisations will have less time to comply. Information must be provided without delay and at the latest within one month of receipt.

25. It is likely that the Council will see an increase in Subject Access Requests as a result. These are often extremely time intensive and accordingly is likely to represent a significant new demand on officer time. Social Services have traditionally received a large number of requests and this will no doubt increase under the new regime. The GDPR also introduces a new best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which will provide an individual with direct access to his or her information.

Right to Rectification

26. Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete. Further, if organisations have disclosed or shared personal data with

third parties, they must inform them of the rectification where possible and also inform the individuals about the third parties to whom the data has been disclosed.

The Right to Erasure

27. This is known as the right to be forgotten. It is not an absolute right. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Under the DPA the right of erasure is limited to processing which causes unwarranted and substantial damage or distress. Under the GDPR this threshold is not present, however, if the processing does cause damage or distress this is likely to make the case for erasure stronger.

28. If processing personal data of children, organisations need to pay special attention to existing situations where a child has given consent and they later request the erasure of the data. This is particularly relevant in relation to social networking sites and internet forums. Again, if information is disclosed or shared, organisations must inform them about the erasure of the personal data.

Right of Data Portability

29. The right of data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data from one IT environment to another in a safe, secure way without hindrance to usability.

Other Rights

30. The DPA currently provides rights in relation to the individual in respect of objecting or stopping processing. However, the new GDPR builds upon these, introducing new rights to restrict processing where an individual contests the accuracy of the personal data or where an individual objects to the processing when the processing is unlawful. Under the GDPR individuals have the right to object to processing where it is based on legitimate interests or the performance of the task in the public interest, direct marketing and processing for purposes of scientific / historical research. Article 82 also provides a right to compensation where any person has suffered material or non-material damage as a result of the infringement of the regulation.

31. The GDPR provides safeguards to individuals against the risk that a potentially damaging decision is taken without human intervention. Accordingly, individuals have the right not to be subject to a decision when it is based on an automated process. If it produces a legal effect or similar significant effect on the individual. Profiling is defined under the GDPR as automated processing intended to evaluate certain personal aspects of an individual, in particular:

- Performance at work
- Economic situation
- Health
- Personal preferences
- Reliability
- Behaviour
- Location
- Movements.

32. Accordingly, privacy notices would require us to advise as to the logic involved as well as the significance and envisaged consequences upon individuals.

Accountability

33. The new accountability principle requires organisations to demonstrate they comply with the Principles, in particular they must:

- Implement appropriate technical and organisational measures. This will include Data Protection Policies, staff training, internal audits and reviews, maintenance of relevant documentation on processing activities, appoint a Data Protection Officer. They must have professional experience and knowledge of data protection law. They must inform and advise organisations and its employees about their obligations to comply with the GDPR and other data protection laws, monitor compliance with the GDPR and be the first point of contact with supervisory authorities.
- Further organisations must implement measures to meet the principles of data protection by design and data protection by default. Measures include:
  - data minimisation
  - pseudo anonimisation
  - transparency
  - allowing individuals to monitor progress
  - creating and improving security features on an ongoing basis.

Data Protection Impact Assessments

34. Data Protection Impact Assessments (DPIAs), also known as Privacy Impact Assessments (PIAs), are a tool which can help organisations identify the most effective way to comply with their data protection obligations and to meet individuals' expectations of privacy.

35. Organisations must carry out DPIAs when:

- using new technology and the processing is likely to result in a high risk to the rights and freedoms of individuals
- systematic and extensive processing activities, including profiling
- large scale processing of special categories
- large scale systematic monitoring of public areas (CCTV).
- The potential fine for non-compliance in this area is up to €10m.

Codes of Conduct and Certification Mechanisms

36. The GDPR endorses the use of approved Codes of Conduct and Certification Mechanisms to demonstrate compliance. Whilst signing up to a Code of Conduct or Certification Scheme is not obligatory, if an approved Code of Conduct or Certification Scheme covers the processing activities, organisations are advised that it is worth working towards these as a way of demonstrating compliance Breach Notification

37. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of or access to personal data. This means that a breach is more than just losing personal data. You must notify the Information Commissioner's Office (ICO) of a breach where it is likely to result in a risk to the

rights and freedoms of individuals. This has to be assessed on a case by case basis. You must also inform the individuals where the breach is likely to result in a high risk to the rights and freedoms of the individual. A notifiable breach has to be reported to the ICO within 72 hours. If the breach is sufficiently serious to warrant notification the organisation must do so without undue delay.

Transfer of Data

38. The current 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 for individuals afforded by the GDPR is not undermined.

39. According the the Department for Digital, Culture, Media and Sport the main elements of the Data Protection Bill are as follows:

- Implement GDPR standards across all general Data Protection processing
- Provide clarity on the definitions used in the GDPR in the UK context
- Ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health and safeguarding situations can be maintained
- Provide appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification including for national security purposes
- Set the age from which parental consent is needed to process data online at the age of 13.

40. As set out above, the Data Protection Bill and the GDPR will operate in tandem until the UK leaves the EU. There is still a degree of uncertainty in this instance as at the date of writing the Data Protection Bill was going through Parliament and maybe subject to amendment.

41. As a public authority, the Council is required to appoint a Data Protection Officer and the individual should report to the highest management level of the organisation. It is proposed that this role is taken on by the current Information Manager (Lawyer). The ICO guidance confirms that the DPO reports to the highest management level of the organisation, is permitted to operate independently and is not dismissed or penalised for performing their tasks, and has adequate resources provided to him/her to enable the DPO to meeting their GDPR obligations.

42. The DPO's minimum tasks are defined below:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

43. The ICO have prepared an Implementation Guide in preparing for the General Data Protection Regulation and the 12 steps to be undertaken. Attached at Appendix A is a copy of that document. As can be seen, it suggests implementation in respect of the following:

1. Awareness
2. Information You Hold
3. Communicating privacy information
4. Individual Rights
5. Subject Access
6. Legal basis for processing of personal data
7. Consent
8. Children
9. Data Breaches
10. Data Protection by design and Data Protection Impact Assessments
11. Data Protection Officers
12. International.

44. The Council needs to work through that Guidance to ensure compliance. This work is being overseen via the Corporate Information Governance Group which has cross Directorate representation.

45. An action plan to implement GDPR is attached at Appendix B

Resource Implications (Financial and Employment)

46. The implementation of the new Regime will have an implication upon the Council's resources, most notably in terms of officer time in changing policies, assessing the Council's current position, amending notices and information to be given out and altering policies and procedures and training staff in relation to same.

47. On-going it will result in officer time in processing subject access requests, which are likely to increase. Equally in determining and complying with the rights of erasure, rectification and objecting to processing will take officer time on a case by case basis. Where information sharing has taken place the duty to inform other organisations of the change will again take officer time.

48. The level and how often fines will be issued to organisations is too early to be assessed but the power is in place and there is no reason to doubt that the UK regulators will not use these powers to ensure compliance. The level of fine would have a substantial affect upon departmental budgets. The issue of compensation for material and non-material damage would have an ongoing effect on Council finances however at this stage it is too early to predicate what this will translate into.

Sustainability and Climate Change Implications

49. None directly related to this report.

Legal Implications (to Include Human Rights Implications)

50. The legal implications are set out within this report.

Crime and Disorder Implications

51. None directly applicable.

Equal Opportunities Implications (to include Welsh Language issues)

52. None directly applicable.

Corporate/Service Objectives

53. To ensure that the Council is in compliance with the new legislative regime and does not render itself liable to fines.

Policy Framework and Budget

54. This is a matter for executive decision by Cabinet.

Consultation (including Ward Member Consultation)

55. No Ward Member consultation has taken place in relation to this matter. DPA training was provided to elected members following the May 2017 election and will be refreshed prior to May 2018.

Relevant Scrutiny Committee

56. Corporate Performance and Resources

Background Papers

The Data Protection Act 1998
EU Directive 95/46/EC
The General Data Protection Regulation (GDPR) EU 2016 / 679
ICO Overview of the General Data Protection Regulation (GDPR)
Preparing for the General Data Protection Regulation (GDPR): 12 Steps to Take Now - Information Commissioner's Office
Data Protection Bill HLBill 66
Data Protection Bill HL (Explanatory Notes)

Contact Officer

Tim Cousins, Information Manager - Lawyer

Officers Consulted

The Information Governance Board
Insight Board
Corporate Management Team

Responsible Officer:

Carys Lord