North Somerset Council 6

REPORT TO THE COMMUNITY AND CORPORATE ORGANISATION POLICY & SCRUTINY PANEL

DATE OF MEETING: 11 JULY 2017

SUBJECT OF REPORT: GENERAL DATA PROTECTION REGULATION (GDPR)

TOWN OR PARISH: ALL

OFFICERS PRESENTING: MIKE RIGGALL & LYNSEY WILSON, CORPORATE SERVICES

KEY DECISION: NO

RECOMMENDATIONS

That the Panel notes the progress being made by the authority in preparing for the implementation of new data protection legislation in May 2018, and takes the opportunity to ensure that members are aware of how their own information management responsibilities will change.

1. SUMMARY OF REPORT

1.1. This report provides a summary of the changes to data protection legislation that will be introduced through the General Data Protection Regulation (GDPR) which will come into effect in May 2018.

1.2. The report also provides an insight into the council's GDPR implementation plan and the progress being made by the council in preparing to meet the requirements of the new legislation.

2. POLICY

2.1. Ensuring organisational readiness for GDPR is an objective of the 2017/18 Corporate Services Directorate statement and is delivered under an enabling ambition of the corporate plan, viz. *A transformed council – modern, innovative and accessible*.

- Ensure that compliance with the General Data Protection Regulation is embedded throughout the organisation and with partners;
- Provide good quality, timely advice and professional support to aid in the delivery of a range of major and minor projects across the organisation;
- Ensure we make best use of our data by improving data/intelligence sharing with partners and following a 'collect once, use lots of times' principle.

3. DETAILS

Background

3.1. On 27 April 2016 the European Parliament created regulation 2016/679 otherwise known as the General Data Protection Regulation (GDPR). The regulation replaced Directive 95/46/EC which gave rise to the Data Protection Act (1998) in the UK. Whilst the regulation was written into EU law in 2016, its effects are not enforceable until 25 May 2018.

3.2. The GDPR strengthens the protection afforded to personal data processed by organisations and affords new rights of access for individuals to their data. A summary of the differences between the existing Data Protection Act and the new GDPR will be presented later in this report.

3.3. The new legislation is designed to reflect the significant advances in technology since the original directive was passed in 1995, addressing weaknesses in existing approaches and attitudes to information governance created by the global, digital economy. It is also designed to bring a consistency to information management across the European Union which currently sees very different approaches between member states.

3.4. In spite of the UK's impending exit from the EU, UK organisations must still prepare to comply with the new legislation. There are two good reasons for this:

3.4.1. The UK will not leave the EU before the GDPR comes into effect in May 2018.

3.4.2. Once the UK finally leaves the EU, there will still be a requirement for UK companies to trade with companies in Europe. In order for European companies to be able to send personal information outside the EU border to the UK, it will be necessary for the UK to be able to demonstrate that it has suitable data protection legislation in place. The easiest way for the UK to seek this 'safe harbour' status is to enshrine the GDPR into UK law.

3.5. The Queen's speech in Parliament on 21 June contained the following statement:

A new law will ensure that the United Kingdom retains its world-class regime protecting personal data, and proposals for a new digital charter will be brought forward to ensure that the United Kingdom is the safest place to be online.

The expectation is that the new law referred to in the Queen's speech will be the existing GDPR although it is anticipated that it will contain some minor variations designed to clarify a number of issues arising from the wording of the current regulation.

Effects of Non-Compliance

3.6. For breaches of the existing Data Protection Act, the Information Commissioner is currently able to issue fines of up to £500k. Income raised from such fines is received by the Treasury.

3.7. Under the new legislation, the Information Commissioner is empowered to issue fines for less-damaging breaches of the GDPR of up to €10M, or 2% of global annual turnover depending on whichever is greater value. For more significant breaches of the GDPR, the Information Commissioner may issue fines of up to €20M, or 4% of global annual turnover. Under the new legislation, income from fines will be retained by the regulator.

3.8. Whilst fines of €20M will be reserved for the most severe of data breaches comparable to the massive data losses recently experienced by Talk-Talk and

Yahoo, the authority must be mindful that it processes a lot of personal information, some of which represents the most sensitive, personal information it is possible to handle; the risk of a significant fine should not be under-estimated.

3.9. Under existing legislation, the Information Commissioner is only empowered to levy fines against a *data controller*, i.e. the registered "owner" of the data who determines the purpose and manner in which information is processed. By comparison a *data processor,* an individual or organisation which undertakes the processing of personal information under the instruction of a data controller, is not liable for fines even if a data breach arises as a result of a direct action of the data processor. Private sector partners such as Agilisys, Liberata and BIFFA who deliver services on behalf of the council are data processors.

Key Changes in Legislation

Basis on which to Process Personal Data

3.10. Currently, for an organisation to process an element of personal information, it must be able to demonstrate a valid basis on which to do so by satisfying at least one of the following six conditions:

3.10.1. Consent has been given by data subject

3.10.2. Necessary for performance of a contract to which data subject is a party

3.10.3. Necessary for compliance with a legal obligation

3.10.4. Necessary to protect the vital interests of the data subject

3.10.5. Necessary for the administration of justice

3.10.6. Legitimate interests pursued by the data controller

The council currently relies heavily on having the consent of the data subject to process their personal information; this is particularly the case in both adult and children's social care.

3.11. Under the new legislation, local authorities are not allowed to use the condition of *legitimate interests pursued by the data controller* in order to process personal information.

3.12. In addition, local authorities are strongly discouraged from relying on the consent of the data subject to process personal information and instead should seek to satisfy one of the other four conditions described in 3.10.2 – 3.10.5 above. The rationale for this is that, where it is used, consent must be freely and willingly given, and the legislation does not accept that this condition can be satisfied in situations where local authorities are in a position of control over a data subject.

3.13. Where the council is forced to rely on consent to process personal information, that consent must be unambiguous and must be provided on an opt-in basis. Pre-ticked boxes are not acceptable.

3.14. Reliance on consent to process personal information also has significant implications for another of the new data subject access rights, the *Right to be Forgotten*, which is discussed in 3.21.

3.15. It is a requirement of the legislation that the condition on which the council relies to process personal information must be clearly recorded for every business process.

Subject Access Rights

3.16. The definition of personal data has been extended to include location data, such as computer IP addresses, and biometric information such as retina scans and fingerprints.

3.17. The time within which an organisation must complete a subject access request has been reduced from 40 calendar days to one month, although the definition of *one month* is still to be clarified. For manifestly difficult subject access requests, under GDPR, organisations will have the right to apply a one month extension thereby giving them more time to complete the request.

3.18. Organisations may currently charge for processing a subject access request (the current limit is £10). Under GDPR, it is not permissible to charge for processing such a request.

3.19. When processing a subject access request, an organisation currently is only obliged to provide the information that it holds. Under GDPR, an organisation must, for each piece of information it discloses, provide additional details related to that information which includes:

3.19.1. The basis on which the council processes the information;

3.19.2. The purpose for which the information is used by the council;

3.19.3. A list of partners with which the information is shared;

3.19.4. The length of time for which the information is retained;

3.19.5. The details of any privacy impact assessment that the council has undertaken in respect of the information

3.20. In the event that the council has recorded an element of personal information incorrectly, under GDPR the council will be obliged to correct any errors without the need for the data subject to obtain a court order. (Where a data subject disputes an opinion, it is sufficient for the council to record alongside that opinion that the data subject disputes its accuracy).

3.21. Where an organisation relies on the consent of the data subject to process their personal information, the data subject has the right to withdraw consent at any time. Under GDPR, where consent is withdrawn, the data subject has the right to be forgotten. The implication for the council is that it would then need to identify and remove all elements of personal information relating to the data subject from any and all systems in which the information is recorded, including both electronic and manual records, including backups.

3.22. The right to be forgotten only applies in cases where an organisation relies on consent to process personal information. It is not possible, for example, for a resident to ask the council to remove all of their personal details from the Revenues system as the council has a statutory responsibility to collect council tax. The basis for processing this information is therefore provided by the fact that it is *necessary for compliance with a legal obligation,* as described in 3.9.3 above and it does not need the consent of the data subject to do so.

Record Keeping

3.23. For each high risk data processing activity undertaken, the authority will be obliged to complete a mandatory privacy impact assessment. Whilst the strict definition of a high risk data processing activity has yet to be agreed, it will inevitably include those activities that involve processing large numbers of data records, particularly sensitive

personal information of one or more individuals, or records which are likely to cause significant distress to a data subject in the event of accidental disclosure.

3.24. In addition to carrying out the privacy impact assessments, the council will also be obliged to publish a list of processing activities that require a privacy impact assessment to be undertaken.

3.25. Fundamental to both existing and future data protection legislation is the requirement to ensure that data subjects are aware of the precise extent of personal information that is processed. The standard instrument for delivering this obligation is the fair processing notice (FPN). The mandatory content of a FPN changes under GDPR and therefore requires the council to review and revise all such notices.

3.26. Under existing legislation, where information is shared with partner organisations for whatever reason, a data sharing agreement must exist, signed by both parties. The data sharing agreement lists the conditions and constraints under which the data may be processed by the partner. The content of every existing information sharing agreement will need to be reviewed and revised to ensure compliance with the new requirements of the GDPR.

3.27. All organisations that process personal information must be able to produce an information asset register on demand by the Information Commissioner. The register provides a central record of all sources of personal information managed by an organisation. For each source the register must indicate:

- The precise composition of the data record
- Why we hold the information
- The basis under GDPR on which we hold the information
- How we use the information
- With whom we share it
- Where we store the information
- How long we retain it
- The details of any Fair Processing Notice and privacy impact assessment associated with the information

Data Profiling

3.28. It will become unlawful for organisations to undertake automated profiling on the personal information supplied by a data subject. This means that the outcome of an application for a council service may not be fully automated and must have a human intervention at some point in the decision making process. Some council services currently make use of profiling techniques. Housing Benefit applications for example are currently initially assessed using *risk based profiling* and this will need to be reviewed.

Compliance

3.29. Under GDPR, the Information Commissioner will have the authority to issue a fine for non-compliance against a data processor as well as a data controller. Contractors may therefore seek to mitigate these new risks indirectly through the re-negotiation of existing contracts.

3.30. Under GDPR there is a mandatory requirement for organisations to report any major data security breaches “as soon as reasonably possible,” but in any case within a maximum period of 72 hours. Additionally, data subjects must also be notified within the same timeframe in the case of high risk processing activities. Failure to observe the reporting requirements is likely to result in the Information Commissioner issuing a fine which will be in the higher threshold.

3.31. It is important for the council and its contractors to review and agree breach procedures; the Information Commissioner must be able to see a joined-up and consistent approach.

3.32. In order to demonstrate compliance with the regulation, an organisation must be able to show that it has embedded the basic concepts of good information management practice at all levels. Throughout the guidance documents this is referred to as *Data Protection by Default and by Design*. This means that we need to emphasise the importance of good information management in our procurements and our contracts. It also means that we will need to ensure that our induction processes for new members of staff and agency workers stress the necessity of good information management practices and that this applies to each and every officer and member in the organisation.

Governance

3.33. The General Data Protection Regulation requires that every organisation designates a role of Data Protection Officer (DPO). Whilst the DPO does not need to be an officer dedicated to the role, they must report to the highest level of management and be able to fulfil their information governance duties free of any conflict of interest or interference from the organisation.

3.34. A Data Protection Officer holds the organisation to account for all activities associated with the processing of personal information. The contact details of the DPO must be provided with the disclosure of every subject access request.

3.35. Subject to formal process and approval by Corporate Management Team, the role of Data Protection Officer within the council is likely to be fulfilled by the Head of Legal Services, Nick Brain.

Implementation Plans

3.36. The council's GDPR implementation plan has been split into three phases:

- Raising awareness
- Information audit and analysis
- Implementation

3.37. Raising awareness throughout the organisation of the impending change to the legislation commenced in January 2017. The information governance team is currently working with services at either a service, team, or an individual officer level depending on the nature and quantity of personal information being processed. This level of support will continue to be provided right the way through to May 2018 and beyond.

3.38. A series of sessions designed to highlight the specific issues relevant to councillors will be offered in September 2017.

3.39. Mandatory training in Information Security and Information Governance is being updated to reflect the changes required by GDPR and a two year training refresh requirement will be enforced.

3.40. The key output from the briefing sessions is the knowledge to allow the information governance team to create the information asset register described in 3.27. Once the basis of the register has been created, the information governance team will then be in a position to identify the changes that are required to ensure compliance with GDPR. This information audit and analysis phase needs to be completed by September 2017.

3.41. The information governance team will work with services across the council between September 2017 and May 2018 in the implementation phase to review existing processes and procedures and implement all of the required changes that were identified in the preceding analysis phase. Reviews of third party contracts and discussions with contractors will take place during this time.

4. CONSULTATION

4.1. The preparation for the implementation of the General Data Protection Regulation has been discussed widely across the organisation, including:

- CMT
- Directorate Management Teams of P&C, D&E and Corporate Services
- ICT Architecture Board
- Service Managers' meetings in all directorates
- Team meetings in all directorates

4.2. A Knowledge Special was produced in May and further articles have been prepared for the run up to May 2018. Once we move into the implementation phase of the plan, the organisation will begin to see a GDPR countdown appearing in regular communications such as The Knowledge.

4.3. The information governance team is cooperating with other public sector bodies across the Bristol, North Somerset and South Gloucestershire (BNSSG) region, building on the relationships forged through complex information sharing projects such as Connecting Care. This ensures that a level of consistency towards GDPR is maintained across the data flows between the council and colleagues in health organisations.

5. FINANCIAL IMPLICATIONS

5.1. Unlike many other organisations in the region, the authority is managing the preparation for GDPR within existing resources and budgets.

5.2. The council may see a future indirect rise in the cost of third party contracts where contractors acting as data processors seek to offset the risk of fines imposed by the Information Commissioner for non-compliance.

5.3. As described previously in sections 3.6 - 3.9 the potential fines for non-compliance with the new legislation are significant. Whilst the council obviously strives hard to minimise the number of accidental disclosures of information, incidents do happen.

6. RISK MANAGEMENT

6.1. The council has not engaged additional resources in preparing for GDPR. Whilst minimising cost, this places a significant burden on officers to implement the action plan alongside normal duties and it is conceivable that not all preparation activities will be complete before May 2018.

6.2. Much of the specific detail of the GDPR has yet to be produced. We do not yet know the definition of "one month" to complete a subject access request, nor how we define a "high risk processing activity". Similarly, whilst we are aware of the implementation of new UK data protection legislation from the Queen's Speech, any variations between this new legislation and GDPR is not yet understood.

6.3. The consensus of opinion is that organisations such as local authorities are likely to see a significant rise in the number of requests made as a result of the extended

access rights afforded by GDPR once the legislation comes into effect. Coupled with the reduced timeframes and higher penalties for non-compliance, there is a risk that this will create a significant, but short-term demand on resources.

6.4. The council has established a GDPR project board to provide governance for the implementation plan and manage the associated risks. The project sponsor is the Head of Legal Services who is ideally placed to keep CMT informed of progress.

7. EQUALITY IMPLICATIONS

7.1. The introduction of the new legislation creates no new equality implications. It is still a requirement that subject access requests are submitted in writing, and suitable identification is provided.

7.2. The maximum £10 charge for processing a subject access request is removed under GDPR thereby removing any financial barrier for those on low incomes.

7.3. In line with all such changes, the information governance team will undertake an equality impact assessment as part of the preparation phase of the implementation plan.

8. CORPORATE IMPLICATIONS

8.1. There are significant implications for all services across the council involved in the processing of personal information. In this context, *processing* can simply mean the recording and storing of personal information, and *personal information,* is any element of data which, on its own or in conjunction with other records held by the data controller, enables the identification of a living individual.

8.2. Creation of the information asset register is reliant on officers being able to identify locations where personal information is recorded and describe the business processes that make use that personal information.

9. OPTIONS CONSIDERED

9.1. The role of Data Protection Officer can be fulfilled by a resource shared between multiple organisations, or be secured on a contractual basis from a third party. Whilst the authority has considered these options it feels that the duties and independence required by the role are aligned closely with the role of the Monitoring Officer and that it is most appropriate to fulfil this role from within the council.

9.2. Whilst the council could engage the services of additional resources to assist with the delivery of the implementation plan, this will not obviate the need for the involvement of officers from across the council who are best placed to understand the nature of data processing that takes place within service teams and identify the locations of personal information.

AUTHOR

Mike Riggall, Client ICT Manager, Support Services Partnership. Tel: 01934 42**6385**

BACKGROUND PAPERS

http://www.eugdpr.org/ - Home Page of the EU GDPR

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
Overview of the GDPR by the Information Commissioner's Office

https://youtu.be/vI39FRkM3DA
Statement on GDPR by the Information Commissioner

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
Home page of the Article 29 Working Party, the body designed to provide the clarification documents that support the GDPR.

B:\CSU\Client Team\f. Information Governance\Team Plan\GDPR Action Plan.xlsx
Summary of the council's GDPR implementation plan.