Chichester District Council

CORPORATE GOVERNANCE & AUDIT COMMITTEE 25 January 2018

General Data Protection Regulations (GDPR)

1. Contacts

Report Author:
Nick Bennett, Legal and Democratic Service Manager
Tel: 01243 524657 E-mail: nbennett@chichester.gov.uk

2. Executive Summary

The purpose of this report is to give an outline of the imminent General Data Protection Regulations and impact upon governance oversight of operational activities at the Council involving data processing.

This report sets out the key principles of the new regulations and actions that are being taken to ensure effective ongoing implementation.

All activity of the Council will need to be undertaken with manager and member awareness of the further rights of the public generated by this legislation.

3. Recommendation

1) **The committee is requested to consider the report and to raise any issues of concern or comment.**

2) **The committee is requested to note the work being undertaken to ensure that the authority is compliant with the provisions of the General Data Protection Regulations by 25 May 2018.**

4. Background

4.1 The current EU data protection regime is based on the Data Protection Directive (95/46/EC) that was introduced in 1995. Since then, there have been significant advances in information technology, and fundamental changes to the ways in which individuals and organisations communicate and share information.

4.2 With the intention of creating legislation which is "fit for the 21st Century" new legislation has been drafted commonly known as the General Data Protection Regulation (GDPR). All British and European organisations including the Council will have to comply with its provisions by 25 May 2018.

4.3 The GDPR is the core piece of legislation in this area from May, though members should note that several other complementary data protection laws are coming which will impact the Council for specific areas of operation in particular the new Crime directive 2016/680 which gives detailed rules for applying data protection for crime

investigation and community justice work by the authority. However none of the further directives contradict the GDPR and the principles set out below are broadly the same for those areas.

4.4 Compliance with the GDPR is going to require organisation-wide changes, to ensure that personal data are processed in compliance with the GDPR's requirements. Such changes may include redesigning systems that process personal data, renegotiating contracts with third party data processors and restructuring data transfer arrangements. Members should therefore consider that these changes may require a significant amount of time to implement, and plan ahead for all departments. It is intended to develop these changes in conjunction with the other organisational improvement work, as set out within the forward plan. All project governance will need to include consideration of how to ensure appropriate resources necessary to achieve GDPR compliance as a part of its planning.

4.5 Some press reporting has raised questions about whether Brexit may impact the introduction of the GDPR – however the Government has been extremely clear that the GDPR will be introduced and that it has no intention of amending the legislation post Brexit.

5. Outcomes to be achieved

5.1 The purpose of this report is to set out the key demands of the GDPR and explain the impact upon the delivery of services by the Council.

5.2 This will help the Council to deliver its Corporate Plan objectives by building on its legal compliance and ensuring that the above requirements are built into governance of projects.

6. Key concepts

6.1 Steve Wood, Head of Policy Delivery at the Information Commissioner's Office (ICO), in his blog post "A data dozen to prepare for reform" of 14 March 2016, explained that:

"Many of the principles in the new legislation are much the same as those in the current Data Protection Act. If you are complying properly with the current law, then you have a strong starting point to build from. But there are important new elements, and some things will need to be done differently."

6.2 This Council has always worked hard to ensure that information is well managed and treated in a secure and respectful manner, so the "strong starting point" is believed to apply to the authority. However a significant amount of work is underway to ensure this starting point is the foundation for effective information management as required by GDPR builds into a strong structure framed by the necessary principles. This implementation across the authority is referred to in guidance as "Data Protection by design".

6.3 The Information Commissioner has published guidance on preparing for the GDPR and the specific guidance organisations can expect to see in 2018 and it is suggested that members interested in more detail on this subject visit the information

commissioner website (https://ico.org.uk/). This provides a range of documents and guidance on the GDPR.

6.4 The GDPR will introduce several new concepts and approaches, the most significant of which are outlined below. The GDPR is also designed to be more "future-proof" and "forward-looking" than the Data Protection Directive, and to be capable of applying to all technology.

6.5 Some concepts will stay the same. Many of the existing core concepts under the Data Protection Directive will remain unchanged. For example, the concepts of personal data, data controllers, and data processors are broadly similar in both the Data Protection Directive and the GDPR. These issues are not addressed further below.

Greater harmonisation

6.6 The GDPR introduces a single legal framework that applies across all EU member states. This means that businesses will face a more consistent set of data protection compliance obligations from one EU member state to the next. This will mean that some of the confusion caused by different approaches to the law across different legal systems in Europe will be removed.

Increased enforcement powers

6.7 Currently, fines under national law vary, and are comparatively low (for example, the UK maximum fine is £500,000). The GDPR will significantly increase the maximum fines and the Information Commissioner will be able to impose fines on data controllers and data processors on a two-tier basis, as follows:

- Up to 2% of annual worldwide turnover of the preceding financial year or 10 million euros (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default.
- Up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers.

6.8 The investigative powers of the Information Commissioner include a power to carry out audits, as well as to require information to be provided, and to obtain access to premises (in accordance with other legal requirements for warrants etc.).

Consent

6.9 Consent, as a legal basis for processing, will be harder to obtain. The Data Protection Directive distinguished between ordinary consent (for non-sensitive personal data) and explicit consent (for sensitive personal data). The GDPR requires a very high standard of consent, which must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written (including electronic or oral) statement.

- An individual's explicit consent is still required to process special categories of personal data.
- Businesses must be able to demonstrate that the data subject gave their consent to the processing and they will bear the burden of proof that consent was validly obtained.
- When the processing has multiple purposes, the data subject should give their consent to each of the processing purposes.
- The data subject shall have the right to withdraw their consent at any time.
- The execution of a contract or the provision of a service cannot be conditional on consent to processing or use of data that is not necessary for the execution of the contract or the provision of the service.
- Data controllers cannot rely on consent as a legal basis for processing if there is a "clear imbalance" between the parties (for example, the employer and employee relationship) as consent is presumed not to be freely given.

6.10 Each of these changes impact upon the steps which will be required by the Council in carrying out its activities with the express consent of individuals. It is important to note however that the majority of tasks carried out by the Council are ones which do not rely upon consent. Instead the Council will often be entitled (or required) to carry out activity by reason of it having a public duty to carry out that task. Guidance on this topic has been issued to all managers.

The risk-based approach to compliance

6.11 The GDPR adopts a risk-based approach to compliance, under which businesses bear responsibility for assessing the degree of risk that their processing activities pose to data subjects. This can be seen in several of the provisions, for example, the new accountability principle and requirement for data controllers to maintain documentation, privacy by design and default, privacy impact assessments, data security requirements and the appointment of a data protection officer in certain circumstances. Low-risk processing activities may face a reduced compliance burden. Broadly the requirements of this element are to:

- Create awareness among the senior decision makers in the organisation (hence this report and other training and reporting across the organisation to members and strategic officers).
- Audit and document the personal data they hold, recording where it came from and who it is shared with. A significant exercise to complete an audit of all processing has been completed and a final document will be in place by May 2018.
- Review the legal basis for the various types of processing that they carry out and document this. Again this has been considered as part of the audit above.
- Review privacy notices and put in place a plan for making any changes to comply with the GDPR (This is underway with staff in Legal and Procurement reviewing contractual notices with partner bodies).

6.12 The Information Commissioner has published guidelines on data protection officers and draft guidelines on privacy impact assessments and is aiming to publish guidelines on transparency. These will be considered and implemented when available.

Mandatory privacy by design and default

6.13 Having regard to the state of the art and the cost of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk to individuals, the Council will be required to implement data protection by design (for example, when creating new products, services or other data processing activities) and by default (for example, data minimisation), at the time of the determination of the means for processing and at the time of the processing itself. By training key officers in detail on the GDPR and all officers on the principles of GDPR, the Council is working to ensure that this is part of the ongoing improvement and corporate development of the authority.

Mandatory privacy impact assessments

6.14 The Council will be required to perform data protection impact assessments (PIAs) before carrying any processing that uses new technologies (and taking into account the nature, scope, context and purposes of the processing) that is likely to result in a high risk to data subjects, takes place. In particular, PIAs will be required for:

- A systematic and extensive evaluation of personal aspects by automated processing, including profiling, and on which decisions are based that produce legal effects concerning the data subject or significantly affect the data subject.
- Processing of special categories of personal data or data relating to criminal convictions and offences on a large scale.
- A systematic monitoring of a publicly accessible area on a large scale.

6.15 The Council, as a Data controller, can carry out a single assessment to address a similar set of similar processing operations that present similar high risks. The Committee will note that the Council has policies in place relating to CCTV and body worn camera monitoring by parking officers. Guidance has been issued very recently and this will be taken into account by officers revisiting those policies before May. All information policies are being considered.

Registrations and ongoing monitoring

6.16 Instead of registering with the Information Commissioner, the GDPR will require the Council to maintain detailed documentation recording their processing activities and the GDPR specifies the information this record must contain. As set out above, a detailed record is being prepared over the past several months known as the "Register of Processing".

6.17 Data processors must keep a record of the categories of processing activities they carry out on behalf of a controller. The GDPR specifies what this record must contain. Where the Council will act on behalf of other bodies this will be taken into account and again legal officers have received specific training on these requirements and implementing them into relevant contracts or other agreements.

6.18 In addition as a public body covered by the Freedom of Information Act, the Council is expressly required to appoint a data protection officer. This has been done and the Legal and Democratic Services Manager (The Monitoring Officer) has been appointed to this role.

6.19 The current guidance on this area sets out several required steps to prepare for the new inspection regime and the Council must:

- Review our existing compliance programmes, and ensure that those programmes are updated and expanded as necessary to comply with the GDPR.
- Ensure that the Council has clear records of all of their data processing activities, and that such records are available to be provided to the Information Commissioner on request.
- Appoint a data protection officer (particularly, where it is mandatory to do so) with expert knowledge of data protection. That employee has protected employment status in some EU member states. Again the Monitoring Officer has undertaken a relevant qualification on GDPR.

6.20 Section 111 of the UK's Digital Economy Act 2017 provides for the repeal of the notification regime. The government is working on an alternative funding model for the ICO based on fees from data controllers. Section 108 of the Act provides that "the Secretary of State may by regulations require data controllers to pay charges of an amount specified in the regulations to the Information Commissioner". This provision will be brought into force by statutory instrument but no draft legislation is yet available.

New obligations of data processors

6.21 The GDPR introduces direct compliance obligations for processors. Whereas under the Data Protection Directive processors generally are not subject to fines or other penalties, under the GDPR processors may be liable to pay fines of up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros, whichever is greater.

6.22 The Council usually acts as Data Controller but GDPR is likely to substantially impact both processors and controllers that engage processors, in the following ways:

- The increased compliance obligations and penalties for processors are likely to result in an increase in the cost of data processing services.
- Negotiating data processing agreements may become more difficult, as processors will have a greater interest in ensuring that the scope of the controller's instructions is clear.
- Some processors may wish to review their existing data processing agreements, to ensure that they have met their own compliance obligations under the GDPR.
- The Council acting as Data controllers needs to identify our processor agreements early on so that we can review and amend them as necessary. These changes are likely to require time to implement but the work has started by Legal and Procurement officers.

Strict data breach notification rules

6.23 The GDPR requires businesses to notify the Information Commissioner of all data breaches without undue delay and where feasible within 72 hours unless the data breach is unlikely to result in a risk to the individuals. If this is not possible it will have to justify the delay to the Information Commissioner by way of a "reasoned justification".

6.24 If the breach is likely to result in high risk to the individuals, the GDPR, requires businesses to inform data subjects “without undue delay”, unless an exception applies.

6.25 The Council will need to develop and implement its data breach response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling the authority to react more promptly in the event of a data breach. Complying with the data breach reporting obligations in the GDPR will also entail a significant administrative burden, which may increase costs. However the DPO is working with IT officers, in particular the Compliance Officer Mary Barlow. This work will include a review of relevant practices and ensure that the required improvements are in place and demonstrable to the Information Commissioner. Again further guidance on this area is anticipated.

Pseudonymisation

6.26 The GDPR introduces a new concept of “pseudonymisation” (that is, the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual, without additional information). Pseudonymous data will still be treated as personal data, but possibly subject to fewer restrictions on processing, if the risk of harm is low. It requires that the “key” necessary to identify data subjects from the coded data is kept separately, and is subject to technical and organisational security measures to prevent inadvertent re-identification of the coded data.

The right to erasure (”right be forgotten”)

6.27 Individuals will have the right to request that the Council deletes their personal data in certain circumstances (for example, the data are no longer necessary for the purpose for which they were collected or the data subject withdraws their consent). It remains unclear precisely how this will work in practice however it is important to note that the Council will consider that the need for holding data will match the period set out in its own retention policy. That policy considered the period for which information would be required from operational and legal purposes such as the defence of claims for every type of data held by the Council and the new Register of Processing will be integrated with the data retention scheme.

6.28 In general, the rights of data subjects are expanded under the GDPR. As a result, the Council IT team will need to devote additional time and resources to ensuring that these issues are appropriately addressed by all departments. In particular, departments will need to consider how they will give effect to the right to erasure (right to be forgotten), as deletion of personal data is not always straightforward from databases in particular.

The right to object to profiling

6.29 In certain circumstances, individuals will have the right to object to their personal data being processed at all (which includes profiling). Again, normally this will not apply where the Council is relying on a public duty to carry out that type of processing.

6.30 “Profiling” is defined broadly and includes most forms of online tracking and behavioural advertising, making it harder for organisations to use data for these activities. The fact of profiling must be disclosed to the data subject, and a PIA is

required if it is done. The Council does not believe that it carries out profiling in any of its activities but this will be monitored and again managers will be trained to identify potential profiling to ensure that it can be properly managed if it is undertaken.

The right to data portability

6.31 Individuals have a new right to obtain a copy of their personal data from the data controller in a commonly used and machine-readable format and have the right to transmit those data to another controller (for example, an online service provider). In exercising their right, the data subject can request the information be transmitted directly from one controller to another, where technically feasible. This issue will need to be considered where the Council operates in a competitive market scenario but it is considered unlikely that this will apply to most Council activity.

Data subject access requests

6.32 Whilst the Council is already required to respond to requests of this kind, the requirements are now significantly more demanding and the consequences of failure are significantly more serious as set out above. The Council must reply within one month from the date of receipt of a request and provide more information than was required under the Data Protection Directive. The council customer services and legal teams are considering how they will respond to data subject access requests within the new time scale and how they will provide the additional information required. At present it is considered that the existing processes, with some minor amendments, will enable the required delivery of responses in sufficient detail and within time. This will receive ongoing monitoring by the Data Protection Officer.

7 Alternatives that have been considered

7.1 The regulations are directly applicable – this means that the Council is required to ensure that its role is compliant with the requirements set out above.

8 Resource and legal implications

8.1 The process and principles set out in the report will help to guide the management of the Council's information resources into the future.

9 Consultation

9.1 The Corporate Governance and Audit Committee is asked to consider this report and to raise any issues of concern or comment.

10 Community impact and corporate risks

10.1 The Council has taken action to ensure that data is processed legitimately and fairly and that previous Data Protection legislation was properly applied. The GDPR compliance efforts set out above will enable the Council to reduce the risk of enforcement in all areas of activity and maintain the strong public perception of being an authority which uses information thoughtfully and with care.

11 Other Implications

Crime & Disorder:		None
Climate Change:		None
Human Rights and Equality Impact:		None
Safeguarding and Early Help:		None

12 Appendices

12.1 None

13 Background Papers

13.1 None