| | |
|---|---|
| Report to: | **Audit Committee** |
| Date: | **22 March 2018** |
| Title: | **General Data Protection Regulation (GDPR) – Readiness & Impact** |
| Portfolio Area: | **Strategy & Commissioning, Cllr K Wingate** |
| Wards Affected: | **All** |
| Relevant Scrutiny Committee: | **N/A** |
| Urgent Decision: | **N** Approval and clearance obtained: **N/A** |
| Date next steps can be taken: | **N/A** |


Author: **Darren Arulvasagam** Role: **Group Manager, Business Development & Data Protection Officer**

Contact: **Darren.Arulvasagam@swdevon.gov.uk or 01803 861222**


**RECOMMENDATION**

**That the Committee note the impacts and support the approach to GDPR readiness ahead of its implementation in May 2018.**

## 1. Executive summary

1.1 From 25th May 2018, new regulations come into force in respect of Data Protection – this is known both as the General Data Protection Regulation (GDPR - EU regulation) and the Data Protection Act 2018 (UK Law).

1.2 This report provides an overview of the key requirements of the GDPR, outlines the approach that the Council is implementing in order to achieve compliance and the tasks that lay ahead

1.3 GDPR places great emphasis on the documentation that the Council must maintain in order to demonstrate accountability. Compliance requires a detailed review of our approach to information governance, data protection and how we collect and process data.

## 2. Background

2.1 Data protection law is changing from 25th May 2018. The current law has been in place for twenty years - since before the use of the internet, emails and cloud storage services. The General Data Protection Regulation (GDPR) is an EU regulation drafted to be fit for purpose in the digital age.

2.2 GDPR is an EU sourced regulation. In the UK, the existing Data Protection Act which was developed in 1995 will be updated to adopt many of the GDPR requirements (there will be some derogations) and will be known as the Data

Protection Act 2018. This move will ensure that 'Brexit' will not lead to later changes in the law.

2.3 The new regulation enhances the rights of data subjects and gives them more control over what happens with their data. It also allows for financial penalties to be imposed on any organisation that breaches those rights or does not comply with the accountability principle.

2.4 Organisations need to put technical and organisational measures in place to protect data from loss, unauthorised access, etc. and to ensure the rights of data subjects are protected.

2.5 The six general principles under the new legislation are very similar to the current law:

2.5.1 Personal information shall be processed lawfully, fairly and in a transparent manner.

2.5.2 Personal information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

2.5.3 Personal information shall be adequate, relevant, and limited to what is necessary.

2.5.4 Personal information shall be accurate and, where necessary, kept up-to-date.

2.5.5 Personal information shall be retained only for as long as necessary.

2.5.6 Personal information shall be processed in an appropriate manner to maintain security.

2.6 Personal data under GDPR includes:

- an identifier, e.g. a name, email address, phone number
- personal identification numbers, e.g. bank account or national insurance numbers
- factors specific to an individual's physical, physiological, genetic, mental, economic, cultural or social identity. This would include anything relating to a disability
- location data - data that has any kind of geographic position attached to it, e.g. data collected by wireless networks, swipe cards and smart mobile devices that provide location tracking
- online identifiers, e.g. mobile device IDs, browser cookies, IP addresses

2.7 Special Categories of Data are those which are particularly sensitive, e.g. race, ethnicity, political opinion, genetic or health related data and sexual orientation.

2.8 GDPR applies to 'controllers' and 'processors' – the controller says how and why personal data is processed and the processor acts on the controller's behalf. In most cases, SHDC (officers and Members) is the controller and processor, in others data is processed by third parties.

2.9 The rights of individuals under the GDPR will largely remain the same as under the existing Data Protection law although there are some significant enhancements. From May, individuals will have:

- 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; and
- the right not to be subject to automated decision-making including profiling

2.10 The biggest change that the Councils will need to implement in this respect is the ability to locate and delete individual's data across all of the Councils systems. Many customer records are now held in W2 which would make the information relatively easy to delete.

2.11 **Subject Access Requests** (SARs) – The new regulations mean that we cannot charge for complying with SAR's and we have to comply with the request within a month rather than the current 40 days allowed. During the last 12 months that Council has handled 4 SARs. The current legislation allows for a fee of £10 to be levied.

2.12 **Lawful basis for processing personal data** – For each processing activity that the Council undertakes, the Council needs to identify the lawful basis for the processing. It is important to assess this particularly in light of the right for data to be deleted – if the only lawful basis for processing is 'Consent' then the information must be deleted on request. The lawful basis for processing the information must also be included within the Privacy Notice.

2.13 **Consent** – The Council must review how it seeks, records and manages consent. Consent for the Council processing data must be freely given, specific, informed and unambiguous. Consent can also not be inferred. Consent for data processing must be separate for any other terms and conditions in documents, web pages or other data capture means.

2.14 **Children** – For the first time, the GDPR will bring in special protection for children's personal data. If the Council obtains personal data in respect of Children, the privacy notice must be written in a language that Children will understand

2.15 **Data Breaches** - The GDPR introduces a duty to report certain types of data breach to the ICO, and in some cases, to individuals. The Council will only have to report a breach to the ICO where it is likely to result in a risk to the rights and freedoms of individuals. Additionally, where there is a high risk to these rights and freedoms, resulting in potential for discrimination, reputational damage, financial loss, loss of confidentiality, etc. there is an additional requirement for the individual concerned to be notified. There has been some misleading press articles stating that all breaches will need to be reported to the ICO.

2.16 **Data Protection by design and Data Protection Impact Assessment** – The GDPR makes privacy by design an express legal requirement. It also makes Privacy Impact Assessments mandatory where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals or where there is processing on a large scale of the special categories of data.

3. **Outcomes**

3.1 Under the GDPR, the Council is required to appoint a Data Protection Officer. The regulation states that the appointment must be made on an individuals' professional qualities and expert Data Protection knowledge, laws and practices. They must also be a direct report to the senior tier of management and able to act independently of the Council. The Senior Leadership Team have appointed the Group Manager, Business Development to this role and that specific training has been given to ensure compliance.

3.2 The Council have formed an Information Governance Group which is responsible for ensuring the Councils are compliant with all information regulation and laws (Data Protection Act, Freedom of Information Act, and Environmental Information Regulations) as well as ensuring that suitable good practice advice and training is in place for staff. This group of officers meets monthly to monitor progress against plans.

3.3 In order to ensure that the Council is compliant, the Information Governance Group commissioned an external "readiness" audit. A GDPR specialist visited the Council and interviewed key officers in order to ascertain priority areas for consideration. Overall the independent assessment considered that while there is a lot of work required for South Hams District Council to be compliant with the GDPR, the Council is reasonably well placed to move to compliance before the regulations takes full effect on 25th May 2018.

3.4 The Action Plan (Appendix A) denotes the actions required to address the points raised in the readiness audit. The first actions completed have been to appoint a Data Protection Officer (the author of this report) and to instigate a review of all of the Council's data protection policies and procedures. This review will be completed by the end of April 2018.

3.5 **Outline Impact for Council Members**

Each Member is registered with the Information Commissioner's Office / ICO. Members should already be doing the following in respect of personal data:

3.5.1 Keep personal data secure

3.5.2 Only use their official Council email address to respond to constituent queries

3.5.3 Be careful with whom they share personal data

3.5.4 Only keep information for no longer than necessary

3.5.5 Be careful if you work in public areas so that you are not overlooked or overheard

3.5.6 Not leave documents or computers/ipads on whilst you are out of the room

3.5.7 Require a password to access any computer file containing personal data

3.5.8 Ensure any device that you use is is password protected / encrypted and is stored securely when not in use

3.5.9 When emailing you should always check who you are sending information to is who you intend to be sending information to – and include the minimum amount of personal data necessary in order to make sense and avoid references to other identifiable people where possible

3.6 The new Act places a duty on Members to keep certain records as it is their duty to show that they are complying with the law.

3.7 New requirements applicable to Members as a result of GDPR:

3.7.1 Keep a record of all processing activities, to show compliance with the legislation

3.7.2 Give a more detailed Privacy Notice when personal data is collected

3.7.3 Tell subjects their rights

3.7.4 Delete 'old' data when it is no longer needed

3.7.5 Report any breaches within 72 hours to the ICO

3.8 By May 2018 the Council will have:

3.8.1 A compliant General Data Protection Regulation Policy (currently under development)

3.8.2 Delivered online training on the new regulations to all employees

3.8.3 Delivered face to face training sessions for Information Asset Owners (60 staff already received training, with regular updates to the ELT and SLT)

3.8.4 Prepared an information asset register for all processing activities and identified the lawful basis for such processing

3.8.5 Prepared an information / training checklist for Members to advise how they should deal with personal data

3.8.6 Updated its Privacy Notices to be compliant with the new regulation & prepared a data protection impact assessment for all relevant areas of data processing

3.8.7 Appendix A details the actions being undertaken.

## 4 Options available and consideration of risk

4.1 Although the regulations continue to be interpreted and clarifications provided by the Information Commissioners Office, the Council must aim to be compliant by 25th May 2018 to avoid the risk of substantial fines and reputational damage.

4.2 The new regulations allow the ICO to impose up to £17m fine per breach although the ICO have confirmed that fines will be the last resort (of the 17,300 cases reported to the ICO last year, 16 of them resulted in a fine to the organisations concerned).

4.3 So far for 2017/18, 10 Data Protection complaints have been made to the Council, two of which have been referred to the ICO for investigation.

## 5 Proposed Way Forward

5.1 To continue to deliver against the action plan as set out in Appenidx A & section 3 of this report.

## 6.0 Implications

| Implications | Relevant to proposals Y/N | Details and proposed measures to address |
|---|---|---|
| Legal/Governance | Y | Compliance with the regulations is critical in ensuring that the reputation of the Council is upheld and that the rights of individuals are protected.<br><br>Our existing Data Protection policy requires updating in order to be compliant – this work is underway. |
| Financial | Y | There are no significant financial implications from obtaining compliance however there is risk of significant financial penalties for non-compliance. At present, resources have been absorbed / pooled from Support Services, Customer First and Strategy & Commissioning to prepare for the implementation of the new regulations, with no new budget pressure. |
| Risk | Y | There is a significant amount of work to be undertaking in ensuring compliance with the regulations. An action plan is in place and is monitored regularly. A project team has been formed which meets regularly, with oversight by the Information Governance CoP, the Data Protection Officer and SLT.<br><br>Training has been and will be arranged for individuals at an appropriate level based on their role in the organisation to ensure awareness of the new regulation & the impact that this has on their activities. |
| Comprehensive Impact Assessment Implications | | |
| Equality and Diversity | N | There are no Equality and Diversity implications. The regulations apply to all individuals equally. |
| Safeguarding | N | None – Compliance with GDPR has implicit improvement impacts on safeguarding |
| Community Safety, Crime and Disorder | N | None |
| Health, Safety and Wellbeing | N | This is implicit with GDPR and will be dealt with through compliance and revised policies. |
| Other implications | N | Policies will be updated as a result of compliance with GDPR |

**Supporting Information**

**Appendices:**
Appendix A – GDPR Action Plan

**Background Papers:**
None