Report to:	**Overview and Scrutiny Panel**
Date:	**9 November 2017**
Title:	**General Data Protection Regulation – Readiness Update**
Portfolio Area:	**Support Services**
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:	**Neil Hawke**	Role:	**Support Services Specialist Manager**

Contact: **Neil.hawke@swdevon.gov.uk**

RECOMMENDATION

That the Overview and Scrutiny Panel support the approach to GDPR readiness ahead of its implementation in May 2018.

1. Executive summary

1.1 From May 2018, new regulations come into force in respect of Data Protection. Known as the General Data Protection Regulation.

1.2 This report outlines the changes that the Council will need to implement in order to achieve compliance with the General Data Protection Regulation (GDPR) by 25 May 2018

1.3 The GDPR places great emphasis on the documentation that the Council must maintain in order to demonstrate accountability. Compliance within all areas listed in this report will require that the Council reviews our approach to information governance and how we manage data protection as a corporate issue.

2. Background

2.1. The General Data Protection Regulation is an EU regulation drafted to be fit for purpose in the digital age. The GDPR will replace the UK's existing Data Protection Act which was developed in 1995. The Government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2.2. The 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.

2.3. The Information Commissioners Office has set out a 12 point plan for preparing for GDPR as follows;

2.3.1. **Awareness** - Implementing the GDPR at the last minute will leave organisations at risk of non-compliance. At this stage it is important that key individuals in the organisation are aware of the requirements and what the Council is required to do in order to maintain compliance.

2.3.2. **Information you hold** – The GDPR requires that we maintain records of our processing activities. It updates rights for the new digital era. In order to comply, we are undertaking an information audit and assigning Information Asset Owners (which will be members of the Extended Leadership Team). These measures are important to ensure that we comply with the GDPR's accountability principle which requires organisations to be able to show how they comply with the data protection principles (so having effective policies and procedures in place)

2.3.3. **Communicating privacy information** – We are required to review our current privacy notices and put a plan in place for making any necessary changes for May 2018. Currently our privacy notice has to state our identity and how we intend to use the information. From May 2018 they must contain

- The name and contact details of the controller and the data protection officer
- The legal basis for the processing
- The legitimate interests of the controller
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfer to other countries (not likely to be an activity for us)
- The retention period for the information
- The existence of each of the data subjects rights
- The right to withdraw consent at any time
- The right to lodge a complaint with a supervisory authority (such as ICO)
  The source the personal data originated from and whether it came from publically accessible sources

2.3.4. **Individuals' rights** - the rights of individuals under the GDPR will largely remain the same as under the existing Data Protection although there are some significant enhancements.

- 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

2.3.4.1. 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.

2.3.5. **Subject Access Requests** – 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.

2.3.6. **Lawful basis for processing personal data** – For each processing activity that the Council undertakes, we need 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.

2.3.7. **Consent** – We must review how we seek, record and manage consent. Consent for us 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.

2.3.8. **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

2.3.9. **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.

2.3.10. **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.

2.3.11. **Data Protection Officers** – as a Local Authority, we are 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 set out

that the Group Manager, Business Development be appointed to this role.

2.3.12. **International –** Only applicable to organisations operating in more than one Country

2.4. 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.

2.5. In order to ensure that the Council is compliant, the Information Governance Group have commissioned an external "readiness" audit. A GDPR specialist visited the Council and interviewed key officers in order to ascertain priority areas for consideration. As a result we now have an action plan for the next 6 months (Appendix 1) to this report.

2.6. 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.

2.7. Work has already commenced on addressing the areas identified under the assessment and will continue to be monitored by the Information Governance Group.

3. Outcomes

3.1. Ensuring that the Council is compliant with the General Data Protection Regulation is a legal requirement that seeks to enhance the protections to individuals in how the Council processes their personal data.

3.2. By May 2018 the Council will;

3.2.1. Have a compliant General Data Protection Regulation Policy (currently under development)
3.2.2. Delivered online training on the new regulations to all employees
3.2.3. Delivered face to face training sessions for Information Asset Owners
3.2.4. Completed its information asset register for all processing activities and identified the lawful basis for that processing
3.2.5. Updated its Privacy Notices to be compliant with the new regulation
3.2.6. Addressed the high priority actions from the Action plan in Appendix 1

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, 9 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 3.2 of this report

6. 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. Our existing Data Protection policy requires updating in order to be compliant.
Financial	Y	There are no significant financial implications from obtaining compliance however there is risk of significant financial penalties for non-compliance.
Risk	Y	There is a significant amount of work to be undertaken in ensuring compliance with the regulations. An action plan is however in place and will be monitored throughout the next 6 months. Training will be arranged for individuals at an appropriate level based on their role in the organisation to ensure awareness of the new regulation.
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
Community Safety, Crime and Disorder	N	None
Health, Safety and Wellbeing	N	None
Other implications	N	None

Supporting Information

Appendices:
Appendix A – GDPR Action Plan

Background Papers:
None