Update on Progress Towards Meeting the General Data Protection Regulation (GDPR) and Data Protection Matters

Director: *Netta Meadows, Strategy and Commissioning*
Lead Officer: *Lynda Creek, Legal Specialist*
Contact Details: *Lynda.creek@southsomerset.gov.uk or 01935 462204*

Purpose of the Report

1. To update members on
    - progress towards the Council meeting the General Data Protection Regulation (GDPR) requirements which comes into effect on 25th May 2018 and;
    - The Information Commissioner's requirement for councillors to be registered as individual data controllers and the implications of this decision in terms of the personal responsibility of members to meet the requirements in their dealings as Ward members.

Public Interest

2. The General Data Protection Regulation (GDPR) fundamentally changes the way organisations must handle personal data they obtain from individuals including an obligation to be more transparent about how such data will be used and with whom it might be shared. Under the Regulation, organisations must design their systems and processes to minimise the data collected and ensure it is protected from unlawful and authorised loss, damage, disclosure, alteration etc. The General Data Protection Regulation (GDPR) puts the individual 'data subject' at the centre of the process and gives more rights and powers to data subjects to control how their personal data is used.

    Organisations have until 25th May 2018 to get their systems, processes and procedures aligned to meet these more exacting requirements. The Information Commissioner (ICO) is likely to use a 'light touch' on enforcement, in the period immediately after May 2018, although they will expect significant progress to have been made and for plans to be in place to put the full requirements in place within a reasonable timescale.

    The financial penalties and other sanctions have been significantly enhanced so it is important that organisations take this issue seriously. There is also reputational risk where data is not handled with privacy issues in mind and the Council is committed to ensuring it protects the personal data of citizens.

Recommendations

3. That Audit Committee note the contents of the report.

Background

4. The Council needs to meet the key requirements for the General Data Protection Regulation (GDPR) by May 2018 and a plan is in place to meet them. Members asked at the last Audit Committee meeting for an update on progress towards General Data Protection Regulation (GDPR) compliance in February 2018.

    A full update and report on the current position went to Senior Leadership Team on the 6th February 2018. The Senior Leadership Team are clear that requests for information, or action, as

part of the General Data Protection Regulation (GDPR) preparation should be treated as important and given appropriate priority. To this end a project work stream will be created as part of the Transformation programme, which will focus on the wider issues of how we effectively manage information and data, as well as the implementation of the General Data Protection Regulation. This work stream will form part of the governance structures within the Transformation programme and progress will be reported regularly as part of normal Transformation monitoring.

Report Detail

5. The Information Commissioner (ICO) published 12 steps to follow to meet the General Data Protection Regulation (GDPR) requirements and progress towards meeting these steps is set out below under the appropriate heading

Step 1 Awareness – ensuring the key decision makers are aware of the changes in data protection requirements and their implications.

As outlined above, SLT have been briefed and a verbal update on their response can be provided at the meeting as required.

With regards to step 1 specifically; as well as face to face awareness sessions at Team Meetings and at Full Council, we have acquired an e-learning module which allows awareness for staff and Members to be tailored to the different levels within the organisation so differing needs are recognized and knowledge is increased in manageable chunks. We are at the test stage for this system and will shortly be planning a rollout across the council.

Steps 2, 6, 7 and 8 Information Asset Review (IAR) – essentially this process involves auditing the types of information we hold, its source, the legal basis for holding it and with whom it is shared etc.

We have completed roughly half of these reviews, although some key areas are outstanding e.g. planning matters. Appointments have been made to progress these ones and so reviews will be completed before the General Data Protection Regulation (GDPR) starts.

We know from the review already completed that they sometimes throw up other work which needs to be resolved – especially around the legal basis for processing as some of the 'gateways' under the General Data Protection Regulation (GDPR) are not available to public authorities like South Somerset District Council. We are therefore noting in the Information Asset Register when consent has been used in the past and if it is still a valid gateway we will be ensuring it meets the new requirements.

All tasks identified during the Information Asset Review are added to the work plan and the exercise has been very useful in identifying gaps in compliance as well as assurance where information systems meet the General Data Protection Regulation (GDPR) requirements.

Step 3 Communicating privacy information – this is the information that we are required to give to the individual 'data subject' when we obtain any personal information from them or from any third parties. The requirements are more extensive and stringent under General Data Protection Regulation (GDPR).

Some ad hoc work has been completed with teams as part of the Information Asset Review however it is hoped that a significant part of this requirement can be addressed through the Civica Workflow 360 system and we will work with the Build Team as part of Transformation to achieve this result. The key aim is to standardise as many aspects of the Privacy Notice as possible and

then work to ensure we deal, efficiently, with the parts that need to be tailored to the particular requirements, through the new agile framework.

Steps 4 and 5 Individuals' rights – including Subject Access Rights (essentially the right to have information about the personal data held about you and obtain a copy) - are greater in number and have more exacting requirements compared to the Data Protection Act 1988 (DPA). The General Data Protection Regulation (GDPR) includes a requirement to promote these rights.

We are awaiting guidance from either the Information Commissioner (ICO) or the Article 29 Working Party (29WP) - who advise the European Commission on such matters. Ideally these issues will be picked up by the Business Analysts (BAs), the Lead Specialist for IT and the Civica Build Team to see how the new technology can support and deal with these requests as part of Transformation. The timescales may not align so this needs to be kept under review but a simple booklet has been produced giving an overview of the changes and has been used in staff awareness session.

Step 9 Data breaches – new requirements and timescales around reporting breaches of the General Data Protection Regulation (GDPR) to both the Information Commissioner's Office (ICO) and Data Subject depending upon the significance of the breach and the contingent risks.

We have, currently, a good system for reporting breaches and then mitigating any possible damage flowing from it. The work will focus, therefore, on ensuring the time scales and additional requirements are met and that appropriate systems for detecting breaches, including raising staff and member awareness of what might constitute a breach, are in place.

Step 10 Data Protection by Design and Data Protection Impact Assessments (DPIAs). These are concepts/tools which have been around a number of years and were recommended as good practice but have now given a statutory footing.

The essence of the former is to ensure when building any 'system' that we implement organisational and technical measures which support the data protection principles such as collecting the minimum personal data needed; pseudonymising personal data wherever possible etc. The latter tool relates to a formal assessment of the impact of some planned new system/process to ensure that any privacy risks are identified and addressed.

We have been carrying out Data Protection Impact Assessments (DPIAs) for the past year and have taken account of the Information Commissioner's Code of Practice in doing so. Where they have been used they have proved a very useful tool in directing minds towards privacy issues. The key issue is that they are drawn up at an early stage before plans have been firmed up.

The key focus going forward will be on continuing to raise awareness of the value of Data Protection Impact Assessments (DPIAs) and where, under the General Data Protection Regulation (GDPR), they will become a statutory. The other tasks is ensuring that once drawn up the actions are implemented and signed off at the appropriate level

Step 11 Designation of the Data Protection Officer (DPO) which is a statutory role responsible for data protection compliance.

Netta Meadows, Director Strategy and Commissioning is considering the options for how we deliver this responsibility, as it does not necessarily need to be provided in-house in the form of a specific post. Other options exist including a shared role (with another Local Authority) or even "buying in" the service from an external organization.

Step 12 – International – special rules apply where personal data is transferred or processed outside of the European Economic Area (which includes the European Union countries plus Norway, Iceland and Liechtenstein).

During the Information Asset Review we are identifying where there may be any overseas transfers as sometimes use of particular websites will involve overseas storage of data, and in such cases the rules are engaged. This issue is not a major concern for South Somerset District Council.

Individual registration of Members

The Information Commissioner contacted the Council in November 2017 to advise that, in relation to the work undertaken by Councilors as Ward Members, it considered those Members should individually register as data controllers. This view was because, in these situations, the individual Councillor controls what personal data they collect from their ward constituents and how it is used and these rather than it being laid down by the Council as a body and this equates with the definition of a Data Controller.

Under the Data Protection Act 1998 (DPA), it is a criminal offence not to register with the Information Commissioner (ICO) if you are a Data Controller. In view of the Information Commissioner's contact (and that we are out of line with many other councils), it was decided that we should register each member with the Information Commissioner (ICO), to ensure their legality under the Data Protection Act 1998 (DPA) and the cost has been met from Council budgets.

It does mean, however, that individual Members are personally responsible for ensuring personal data, derived from their Ward matters is protected. Support in understanding and meeting these requirements can be offered to ensure members know their responsibilities and duties via the e-learning modules, mentioned above, and by face to face advice on request.

Financial Implications

6. None

Council Plan Implications

7. Compliance with the General Data Protection Regulation (GDPR) and other data protection requirements will help ensure the Council achieves its aim for 'high-quality and cost effective services', and will be an integral part of our focus on 'transforming customer services through technology'.

Carbon Emissions and Climate Change Implications

8 None

Equality and Diversity Implications

9. *None*

Privacy Impact Assessment

10 None

Background Papers

11

- Link to the General Data Protection Regulation https://gdpr-info.eu/X
- Link to Data Protection Bill https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/18153.pdf
- Link to the Information Commissioner's advice for Elected and Prospective Councillors https://ico.org.uk/media/for-organisations/documents/1432067/advice-for-elected-and-prospective-councillors.pdf.