What does GDPR mean to the public sector?

The Information Commissioner’s Office (the ICO) currently enforces the Data Protection Act, and has powers to impose fines of up to £500,000. GDPR is a significant change to the regulation, and the ICO will be empowered to impose fines of up to 4% of global revenue or 20 million euros. The regulation applies to the processing of individuals’ personal data in the EU when offering goods and services or monitoring their behaviour. As was the case with the Data Protection Act, all public sector organisations have a fiduciary duty to understand and comply with GDPR.

As a public sector organisation, you are likely to hold and process large amounts of sensitive information on individuals, including confidential details such as financial data, medical records and general contact information.

You might rely on third-party organisations to provide services, such as the provision of care to vulnerable members of the public, or you might have outsourced ICT support providing a managed service, including the hosting of servers. In both situations, responsibility falls on you to ensure compliance with GDPR.

What do you need to do?

GDPR brings the Data Protection Act into the 21st century by seeking to protect data subjects from the inappropriate or unauthorised sharing of their data. The new regulation makes a number of activities mandatory for all organisations, such as:

- The requirement to update policies and processes to reflect the requirements of GDPR. As an example, it will require changes to how organisations obtain and use consent and also how they store information.
- Providing new and existing staff with suitable training and awareness, as well as additional sources of guidance and support when required.
- Conducting Data Protection Impact Assessments (DPIA) in order to design data privacy into any new systems and processes. This is of particular importance if new technology is being deployed, where there is processing on a large scale of the special categories of data, or if profiling operations are being performed which are likely to have an impact on individuals.
- Notifying the ICO within 72 hours of a data breach.
- Holding those at executive management and board level accountable for compliance, requiring them to produce and maintain documents that demonstrate what actions have been taken to achieve compliance.

There are some important caveats and derogations regarding consent, data retention and the right to be forgotten that apply to government bodies and public sector organisations. Largely, the key changes are as follows:

- The requirement to appoint a Data Protection Officer (DPO) for certain types of organisations, who will be responsible for communications between the organisation and the ICO and for enforcing the mandatory processes mentioned above. This is likely to apply to most public bodies.
• Data subjects have to explicitly ‘opt in’ to allowing their data to be shared, and it must be made clear what manner of data sharing they are opting into. Consent, however, is not always required when processing data to fulfil a task which is in the public interest. This is something public bodies need to consider carefully.

• Data should only be held for the purposes it was gathered and be deleted when it is no longer needed. Individuals also have the right to request that they be provided with all their data in order to move it to another organisation (data portability) and the right to be forgotten (data erasure). If data is retained following such a request, an explanation has to be provided to the individual explaining the grounds for this decision. Public sector bodies, however, can retain data if there is a public interest rationale for doing so, even if individuals have requested it be removed.

• If sharing data with organisations outside the EEA, you are required to ensure adequacy decisions or appropriate privacy safeguards are in place, such as binding corporate rules and the use of the EU-US Privacy Shield. This will have a particular impact on the provision of cloud and outsourced services.

Recent breaches of data protection to learn from

You will have seen news headlines exposing breaches of data protection with eye-watering fines for the organisation at fault. GDPR means the scrutiny, and penalties, are set to intensify. Recent breaches include:

- **Nursing home fined £15,000 for failing to look after sensitive personal details after an unencrypted laptop was stolen during a burglary, containing information on 29 residents and 46 employees.**

- **GP practice fined £40,000 after revealing confidential details about a woman and her family to her estranged ex-partner, despite being asked not to inform him of their whereabouts.**

- **Council fined £150,000 for publishing sensitive personal information on a family in online planning application documents, including medical details and the names, ages and addresses of family members.**

- **County council fined £60,000 after leaving files that included sensitive information about children in a cabinet sent to a second hand shop.**

In addition to responding to reports of any breaches and imposing fines, the ICO also carries out a programme of audit activities across the public sector. These audits are designed to enable and support organisations in their efforts to be compliant by providing feedback on their current processes and controls.
How we can help you

Our GDPR health check is a facilitated self-assessment, which is most effectively administered in a workshop environment. Our team facilitate the assessment, and present and explain the questions and the scoring system used. Their knowledge of GDPR helps the participants explore and challenge their self-assessment, and support consistency of interpretation across the different areas of the questionnaire.

The workshop usually takes between one and two hours. Prior to the session, we would hold an opening meeting with yourself at which we will introduce you to the questionnaire and the scoring process. We will also provide participants with guidance materials in advance to help them prepare.

After the workshop, we will provide a standard report which will show your self-assessed maturity against the different areas of GDPR. We will then work with you to develop an action plan to address any areas of weakness.

Our team will provide independent input and challenge, both during the workshop and after it, to support you in considering all relevant aspects across the activities of a client and in interpreting the requirements of GDPR. This exercise does not provide independent audit or validation of the information provided by participants.

Get in touch

We have helped a number of our clients with their GDPR requirements, ensuring they are in a strong position by May 2018. If you’d like our team to come out and conduct a GDPR health check on your organisation, please get in touch.

Fraser Nicol  
Partner, Glasgow  
E fraser.nicol@scott-moncrieff.com  
T 0141 567 4500

Liz McLean  
IT Audit Manager, Glasgow  
E Elizabeth.mclean@scott-moncrieff.com  
T 0141 567 4500