Veritau
Assurance Services for the Public Sector

Data Protection Reform

New data protection legislation comes into effect on 25 May 2018. It includes rights for data subjects, duties on data controllers (similar to the now-familiar principles), and exemptions from both rights and duties. There are some small but noteworthy changes to all three but there is also a new emphasis on

- assessing and mitigating risk
- structures within organisations to ensure compliance
- taking a more organised, proactive approach to Data Protection
- **demonstrating** compliance and accountability

The UK Data Protection Bill

The Data Protection Bill incorporates into UK law the requirements of two new pieces of EU legislation: the General Data Protection Regulation and the Law Enforcement Directive (which governs processing of information for crime related purposes). It seeks to ensure the UK can demonstrate an adequate level of privacy protection, in order to promote continuing trade (and also crime prevention and security cooperation) with the EU and will still have effect after Brexit.

The Bill is currently passing through the House of Commons so the final details have yet to be established. However broadly speaking most of the requirements of the new legislation have been recommended best practice for some time and will already be in place to some degree in most councils.

The ICO has cited the first step to compliance as the completion of a comprehensive information asset register and the details requirements are listed below:

Notification

The requirement for all data controllers (including local authorities, schools, registrars, councillors and coroners) to pay an annual fee to the Information Commissioner (ICO) is not carried over. Instead the Digital Economy Act 2017 introduces a requirement to pay a fee for processing personal data. The proposal is for a three tier fee system, rather than the current two.

The new fee system will be implemented on 1 April 2018 and fees will continue to be collected by the ICO. Organisations should renew their notification as usual: the fee charged will be that in force at the renewal date.

Current	**Proposed**
£35	£55 - Tier 1: Staff Headcount under 250 and number of records under 10,000
£500 if: turnover of £25.9M **and** more than 249 members of staff; or if you are a public authority with more than 249 members of staff	£80 - Tier 2: Staff Headcount under 250 and number of records over 10,000
	Up to £1000 Tier 3: Staff Headcount over or equal to 250

NB public authorities will be categorised based on headcount and records alone.

Organisations which engage in direct marketing will be required to pay an additional £20.

Privacy notices

The Bill introduces a quite lengthy list of information with which an organisation must provide data subjects about the processing of their personal data and requires the information to be written in a way which is:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

This is called a privacy notice and must be provided at the time the information is collected from the data subject, or within a reasonable period of the information is obtained indirectly.

Consent

In a significant change to current practice, public authorities may not, in most circumstances, be able to rely on consent to process personal data.

Public authorities will instead be able to justify most processing by virtue of a legal duty, a contract, or their "public task", which necessitates processing. Consequently, in many services, detailed privacy notices will replace consent forms.

Public Task means all those things which an organisation does because it is a public authority. It includes all the organisation's legal duties, its optional powers if any, and things it does through custom and practice.

In cases where it is necessary to use consent, the consent must be freely given, specific, informed and unambiguous. If consent is relied on, the organisation must be able to evidence that it is valid. There must have been a positive indication of consent – so no more pre-ticked boxes, or inference from a lack of objection. Consent may be partial or conditional, and may be withdrawn by the data subject at any time.

There are two final justifications which a public authority can rely on: where the processing is necessary to protect vital interests or the processing is in an organisation's legitimate interests, and it does not infringe the rights and freedoms of a data subject.

Data Protection by Design & Data Protection Impact Assessments

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. A Data Protection Impact Assessment (DPIA) - formerly known as a Privacy Impact Assessment – is a mandatory tool for assessing privacy risks in certain circumstances.

Under the Bill, a DPIA is mandatory if the project will be likely to result in "a high risk to the rights and freedoms of individuals." For example data matching or profiling, or if using special category data of a large number of individuals, or large scale CCTV monitoring.

Data Protection Officers have a significant role in mandatory DPIAs, including advising when a DPIA should be conducted, what safeguards to apply and whether a DPIA has been carried out correctly.

In controversial cases, DPIAs may need to be referred to the Information Commissioner before processing can begin.

The Bill also requires an organisation to maintain documentation on its processing activities – these are largely the same as information which is currently included in the notification to the ICO.

Data Protection Officer

All public authorities, as defined in the Freedom of Information Act, must appoint a Data Protection Officer (DPO). This obligation will therefore apply to LEA-maintained schools, and town and parish councils.

The DPO can be a living individual or an organisation. A DPO should have expert knowledge of data protection law and practices, and have an understanding of information technologies, information security and other critical business continuity issues around the holding and processing of personal and sensitive data.

The DPO must be independent, and is to be protected from undue interference or obstruction, or dismissal. Organisations must ensure their DPO is adequately resourced.

NB liability remains with the data controller, not the data protection officer.

Reporting data breaches

Each data controller will be obliged to notify the ICO of serious data security incidents without undue delay, and within 72 hours of the controller becoming aware of the breach. Breaches do not need to be reported if they are unlikely to result in a risk to the rights and freedoms of data subjects.

The data subjects concerned should also be notified, if the breach is likely to result in a high risk to their rights and freedoms.

Thresholds for these reporting requirements haven't yet been clearly established - we are hoping to get more guidance at the Data Protection conference in April.

Sanctions

The following sanctions can be imposed by ICO:

- a written warning in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;

- a fine of up to £17m (ie €20m) (an increase from the current £500k) for a range of infringements of the Bill (not just data breaches)

Data Processors

The Bill requires contracts with data processors to include specific clauses. These include the requirement for data processors to inform the data controller of a breach on becoming aware of it. Liability for data breaches will still lie with the data controller but may also extend to that data processor if it is at fault. Outsourced ICT systems, including cloud-based systems will be affected by this.

Subject Access Requests

Subject access requests must now be answered within **one month** – although for complex or bulky requests an organisation may apply an extension of a further two months. No charge may be made. In some cases organisations may refuse a request or request a fee if the response is considered excessive, repetitive, or manifestly unreasonable. It should be noted however that it is thought the ICO will rarely approve of such reasoning.

The data controller should provide the information electronically if the request was made electronically.

Right to be forgotten

A data subject may require erasure of some or all of his or her personal data, unless there are legitimate grounds for it to be kept. The new legislation reverses the burden of proof so that the data controller must demonstrate that it must retain the data, rather than the data subject showing how the processing is causing him or her harm.

Right to Data Portability

This is the right of a data subject to transfer personal data easily from one IT environment and is designed to assist consumers when switching between data controllers who provide a commercial service. However the definition may apply to some HR and payroll data and may therefore impact public authorities as well.

This only applies if the information was provided by the data subject, is processed by automated means, and is processed based on consent or the performance of a contract.

Social media

The new legislation provides that when using social media once a child reaches 13 he or she will have the capacity provide consent themselves. Below that age the child's parent or guardian must consent.

However for all other child DP issues, the current position remains – that is, once a child has the capacity to decide on privacy matters for him or herself, then it should be the child whose consent is sought, rather than the parents. The rule of thumb that a child of 12 has such capacity will continue to apply.

Retention

There are no new requirements around retention of information – an organisation should always have had a retention schedule and deleted/destroyed information in accordance with that schedule.

However it is our experience that this has rarely been the case. The new legislation has the same requirements in relation to records retention (but greater penalties for non compliance and retention periods must now be communicated to data subjects on privacy notices) and so should be used as a catalyst for organisations to address this as a priority.

Processing personal information for crime related purposes

The Data Protection Bill includes separate rules for 'competent authorities'. These are services with statutory functions for any law enforcement purposes including prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security - generally these are services which have the power to prosecute and conduct interviews under caution, such as trading standards and social housing. Youth offending teams are also defined as competent authorities.

Most of these are the same rules which govern any personal information but there are some specific new requirements which apply to these services:

For more information about data protection reform please contact the information governance team at Veritau at:
information.governance@veritau.co.uk