

GDPR: Overview of Changes		
	Change	Does the change require action by the SSSC?
1	Data Protection Impact Assessments (DPIA) Introduces a requirement that DPIAs are undertaken when data processing presents a high risk.	Yes The current system provides for the optional completion of privacy impact assessments out where appropriate. This is not something that the SSSC regularly undertakes. We will require a new process for officers to ensure they are considering the need for a DPIA at appropriate times.
2	Data Protection Officers (DPOs) Introduces a requirement that data controllers must designate a DPO if they are a public authority or their core activities relate to processing of certain types or scale of data. The DPO must report to the most senior level of management.	No The Head of Corporate Governance and Hearings role has responsibility for data protection and reports to the Chief Executive.
3	Demonstrating administrative compliance Introduces a general obligation to maintain documentation and demonstrate compliance with the legislation. <ul style="list-style-type: none"> Records of data breaches and remedial action taken Undertaking DPIAs Implementing data security requirements. 	Yes We already have an embedded system of procedures, compliance checks, training and data breach recording. This system will need reviewed in light of other changes.
4	Abolishing Notifications Abolishes the current system of	No There is other legislation which

	registration with the ICO to reduce the administrative burden, particularly on organisations operating cross-border.	requires those processing data to pay the ICO a fee, so there will still be a form of registration and payment to the ICO.
5	Subject Access Requests (SAR) Abolishes the power to charge a subject for a copy of their data and reduces the time to respond from 40 days to a month. Also introduces a requirement to provide additional information when responding to SARs.	Yes We will need to refresh our procedures. We will consider the resource implications of responding within a shorter time-period.
6	Data Portability Introduces a new right for data subjects to receive their personal data in a structured, commonly used and machine-readable format and for one data controller to transmit that data to another data controller.	No The focus of this provision is to enable people to change service provider more easily by requiring, for example, one utility company to pass data directly (in electronic fashion) to another utility company. It will not be hugely relevant for us. However we can already provide data in a way that meets the legislation if required.
7	Right to Erasure Expands the right to be forgotten. Currently the law focusses on whether the existence of the data is likely to cause substantial damage or distress. That will change to require data controllers to erase data when consent is withdrawn.	Yes This will not affect data held in fulfilment of our core regulatory function, as our reason for retaining the data will not be based on the consent of the individual. We will review whether we need to improve our erasure process for other personal data that we hold.
8	Data Breach Notification Introduces a requirement to inform the ICO within 72 hours (where feasible) of all personal data	Yes We already have a process of recording data breaches and notifying

	breaches that are likely to result in a risk to the rights and freedoms of natural person.	<p>the ICO when necessary.</p> <p>We will review the process to ensure we can meet the new timescale.</p>
9	<p>Administrative Sanctions</p> <p>New sanctions available to the ICO including increased powers to inspect and increased fines of up to £17.7 million.</p>	No