Section 2:
Overview

This section provides an overview of the relationship between the GDPR and the UK Data Protection Act 2018 and explains significant changes in key data protection concepts.

2.1 Relationship between GDPR and DPA 2018

The General Data Protection Regulation (GDPR) comes into effect in all EU Member States on 25 May 2018. It is directly applicable in all EU Member States without any further implementing domestic law.

After the UK formally leaves the European Union the provisions in the GDPR will continue to apply in line with the manner that they are set out in the UK Data Protection Act 2018 (DPA 2018). In addition to restating the provisions of the GDPR, the DPA 2018 also sets out tailored national exemptions (in areas allowable under the GDPR) and provides a legal framework for data protection in criminal justice and law enforcement. It also replaces the Data Protection Act 1998 (DPA 1998).

In this Guidance references to the GDPR should be interpreted as references to the GDPR as implemented by the DPA 2018. References are made to the articles of GDPR and sections of the DPA 2018 as appropriate. The Guidance reflects the UK national implementation of the GDPR. Differences in the data protection framework as a result of specific national rules in the UK implementing legislation are generally highlighted in the text.

2.2 New and significantly changed concepts between DPA 1998 and GDPR/DPA 2018

The GDPR introduces new concepts and rules and significantly changes core provisions in the existing data protection framework. The changes of greatest relevance to researchers are:-

- **Wider definition of personal data** – The GDPR expands on the definition of personal data in the DPA 1998 to explicitly acknowledge that online identifiers such as cookies and similar technology such as IP addresses can be personal data.[4] It also expands the category of special category data (previously known as sensitive personal data) to include sexual orientation, biometric data used for identification purposes and genetic data.
- **New concepts of accountability and data protection by design and default** – Data controllers are accountable and must be able to demonstrate compliance with the data protection principles and use appropriate organisational and technical measures to ensure compliance. Additionally, the concept of data protection by design and default requires data controllers to ensure that data subjects' privacy is considered from the outset of each new processing, activity or development of

[4] The text in a cookie often consists of a string of numbers and letters that uniquely identifies a computer, but it can contain other information as well. Cookies are often used by web pages to help users navigate their websites efficiently and perform certain functions within pages or logins.

new products, services or applications. It also means that, by default, only the minimum amounts of personal data as necessary for specific purposes are collected and processed. This also means that techniques such as pseudonymisation must be effectively utilised.

- **Statutory liability of data processors** - Data processors and data controllers are both directly liable through statutory obligations in contrast to the previous regime which placed liability only on data controllers. Data processors are jointly and severally liable with data controllers for compensation claims from data subjects.
- **Mandatory appointment of Data Protection Officer (DPO)** – DPOs are mandatory in certain circumstances. DPOs are required for public bodies, and for organisations whose core activities either require regular and systematic monitoring of data subjects on a large scale or involve large scale processing of special category data and data relating to criminal convictions. Appointment of a DPO is likely to be a requirement for most research suppliers.
- **Higher standard of consent** –GDPR requires unambiguous consent that is freely-given, specific, informed and evidenced by clear affirmative action or statement (silence or pre-ticked boxes are not evidence of consent). Consent must also be verifiable with higher standard of explicit consent required to process special category data.
- **Mandatory notification of personal data breaches** – Data breaches must be notified to the ICO without undue delay and within 72 hours of becoming aware of the breach where there is a likelihood of risk to data subjects. Notification must also be made to affected data subjects where there is a high risk the data breach is likely to cause harm.
- **Territorial scope**– The GDPR applies to organisations outside the EU who are offering goods or services to or monitoring data subjects resident in the EU. These organisations will generally need to appoint a representative based in the EU. In light of this, it is also important to note that when the UK is no longer a member of the EU, UK-based organisations monitoring EU citizens will be subject to the GDPR and any tailored national provisions in individual Member States.

For further information see:

- MRS GDPR In Brief (No.1): Changes in UK Data Protection Framework (Member Content)
- ICO Guide to the GDPR **https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/**