The GDPR

1. Introduction

The General Data Protection Regulation (GDPR or The Regulation) was published in May 2016 and will come into force in effective in May 2018. As a regulation it is direct law in all member states. The ICO has advised it will apply in the UK and businesses need to prepare for it. It replaces the existing Data Protection Directive 95/46/EC (DP Directive) and the E-Privacy Directive 2002/58/EC (Privacy Directive). Much of the Regulation as well as its structure and content, is familiar from and follows the scheme of the DP Directive. At the core of the GDRP are the Principles governing collection and processing, see arts. 6 & 7 GDPR.

2. Main new elements

2.1. Territorial jurisdiction

The DP Directive had a place of establishment and location of equipment test for its application. However the Regulation bites when EU citizens' data is processed to sell to or monitor them—regardless of the location of the actors. That is, when EU citizens are targeted, the Regulation is likely to apply.

2.2. Improved consent

The concept of consent is improved by the express clarification that it be informed and revocable and affirmative (including the rejection of silence) as well as severable and unbundled. See art.7 GDPR.

2.3. RTBF

The right to be forgotten/erasure from *Google Spain v Costeja* and related rights to revoke and rectify are codified and strengthened in arts 16 to 18. This can extend to hosts and social media as well as search engines. If the Data Controller made the data public, it must take all reasonable steps to inform others and obtain their erasure, subject to Freedom of Expression, legal obligations, public interest and public health and archives and legal proceedings etc, see art. 17.

2.4. Data Portability

This is a new right in art 20 for data subjects to obtain a copy of their data in machine readable format --- or the transfer of it directly from A to B where technically feasible.

2.5. Data Breach Notification

This duty to notify a breach has become statutory and extends to all breaches after 72 hours --unless unlikely to be a risk for individuals. See arts. 33-34 GDPR.

2.6. Automated decision-making and profiling

Data Subjects have a right to object to this and not to be subject to it, see arts 21 & 22.

2.7. Privacy by design

This is also new and mandatory. Data controllers must have regard to the state of the art in privacy and its costs and implement technical and organizational measures accordingly, see art.25.

2.8. Transfers

EU data can only be transferred abroad where there is an "adequate" level of similar protection in the destination country. The US had avoided this issue with its safe harbor, but that fell following the CJEU decision in *Schrems* in 2014 and was replaced with the untested privacy shield.

3. Media issues

Art.9 has a general prohibition on processing special data –previously understood as sensitive personal data. This category maps to data protected by the law of privacy and will include gender, opinions, beliefs, health and sexual and intimate relations information and financial information. This is subject to many exemptions including (a) consent and (e) where the data has been made publically available by the data subject and (g) public interest. These will form the basis of defences for the media.

Article 85 of the GDPR requires national governments to reconcile the right to protection of personal data with that of freedom of expression and information. A familiar balance for those working in privacy and data protection. Journalistic purposes and the purposes of academic, artistic or literary expression are all specifically referenced in Article 85. The UK Government has not yet brought forward legislation for this purpose and is consulting with industry and the public.

4. Action point

4.1. Prepare. Data Controllers and processors should review their arrangements, policies and

processes and conduct an "Impact Assessment" if they have high risk data. This is advisable in any case in light of the new Regulation. Businesses should bench mark best practices and ideally have a third party professional conduct an audit for privacy by design.