# Data governance: Landscape Review

June 2017

THE ROYAL SOCIETY

BRITISH ACADEMY
*for the humanities and social sciences*

# Contents

CHAPTER 1

# Introduction

This review was undertaken as part of joint work between the British Academy and the Royal Society on data governance. The final report *Data management and use: Governance in the 21st century* was published in June 2017.

This review does not represent the view of either of the Academies.

This review aims to:

- provide a general understanding of the data governance framework;
- help identify and understand the complexity and challenges with current governance landscape;
- help map the types of powers and functions currently being used with a view to using this to inform what maybe missing or needed.

The review presents a summary of the main regulations. It is not meant to be a comprehensive review of all the data governance regulations or bodies.

**Acknowledgments**

The British Academy and the Royal Society are grateful for the contribution of Fernanda Ribas in the production of this review. We would also like to thank expert reviewers:

- Iain Bourne – Information Commissioner's Office
- Marion Oswald – University of Winchester
- Professor Roger Brownsword – King's College London

CHAPTER 2

# Main regulations

| | | |
|---|---|---|
| EU regulations | EU Data Protection Directive (1995) | It regulates the processing of personal data within the European Union. It is based on a set of rights for individuals – for example access rights - and a series of principles that organisations must follow – for example transparency and data security. |
| | The Database Directive (1996) | Created a new exclusive "sui generis" right for database producers to protect their investment of time, money and effort, irrespective of whether the database is in itself innovative ("non-original" databases). The Directive also harmonised copyright law applicable to the structure and arrangement of the contents of databases ("original" databases). |
| | The ePrivacy Directive (2002) | Sets out rules on how providers of electronic communication services should manage their subscribers' data. It also guarantees rights for subscribers when they use these services, for example, control over electronic marketing. |
| | The General Data Protection Regulation (GDPR) (2016) | The new EU data protection regime will build on existing rights and principles, but will bring in a stronger accountability principle, strengthen existing rights and introduce some new ones – for example, 'data portability'. It also seeks to harmonise the data protection regime across the EU. |
| | Digital Single Market Strategy (2015) | The Digital Agenda's main objective is to develop a digital single market to generate smart, sustainable and inclusive growth in Europe. A Digital Single Market (DSM) is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. |
| UK regulations | Data Protection Act (1998) | The Data Protection Act (DPA) is the current UK law on the processing of personal data. It is the main piece of legislation that governs the protection of personal data in the UK. It implements the 1995 EU Data Protection Directive. |
| | The Freedom of Information Act (2000) | The Freedom of Information Act provides public access to information held by public authorities. It does this in two ways: public authorities are obliged to publish certain information about their activities and members of the public are entitled to request information from public authorities. |
| | The Privacy and Electronic Communications Regulations (PERC) (2003) | The Privacy and Electronic Communications Regulations give people specific privacy rights in relation to electronic communications. There are specific rules on: marketing calls, emails, texts and faxes; cookies (and similar technologies); keeping communications services secure; and customer privacy about traffic and location data, itemised billing, line identification, and directory listings. |
| | The Environmental Information Regulations (2004) | The Environmental Information Regulations provide public access to environmental information held by public authorities. The Regulations do this in two ways: public authorities must make environmental information available proactively; and members of the public are entitled to request environmental information from public authorities. |
| | INSPIRE Regulations (2009) | The INSPIRE Regulations derive from a European Directive (INSPIRE Directive 2007/2/EC) and create a right to discover and view spatial datasets. They enable the sharing of environmental spatial information among public sector organisations and better facilitate public access to spatial information across the EU. |
| | Re-use of Public Sector Information Regulations (RPSI) (2015) | RPSI is intended to encourage re-use of public sector information and is about permitting re-use of information and how it is made available. |
| | Investigatory Powers Act (2016) | It provides a new framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies. |
| | The Digital Economy Bill (2017) | The Digital Economy Bill will implement several government commitments on the digital economy made in the Conservative Party Manifesto, such as: new and simpler planning rules for building broadband infrastructure; rules concerning data sharing and statistical data; a new statutory code of practice for direct marketing, etc. |

CHAPTER 3

# EU data regulation

This section sets out the main elements of the governance framework for data in the EU.

### 3.1 The 1995 EU Data Protection Directive[1]

The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union (EU) directive which regulates the processing of personal data within the European Union. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data[2]. It encompasses all the key elements from Article 8 of the European Convention on Human Rights[3] whose purpose is to ensure respect for the right of privacy in personal and family life, as well as in the home and in personal correspondence. The respect to privacy is however subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society".

This Directive applies to data processed by automated means and data contained in or intended to be part of a non-automated filing system. It does not apply to the processing of data:

- by a natural person in the course of purely personal or household activities;
- in the course of an activity which falls outside the scope of Community law, such as operations concerning public security, defence or State security. However, these activities are covered by the UK's domestic data protection law.

The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down criteria for ensuring processing is lawful and setting out the data protection principles.

The principles of data quality, which must be implemented for all lawful data processing activities, are the following:

- personal data must be processed fairly and lawfully, and be collected for specified, explicit and legitimate purposes. They must also be adequate, relevant and not excessive, accurate and, where necessary, kept up to date, must not be stored for longer than necessary and solely for the purposes for which they were collected (all subject to relevant national exemptions);

1 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; EUR-Lex - 31995L0046.
See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. (accessed 1 June 2017).

2 Protection of personal data; EUR-Lex - l14012 - EN - EUR-Lex.
See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012 (accessed 1 June 2017).

3 ECHR. European Convention on Human Rights - Official texts, Convention and Protocols.
See http://www.echr.coe.int/Pages/home.aspx?p=basictexts&c= (accessed 1 June 2017).

- special categories of processing: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life. This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis.

The person whose data are processed, the data subject, can exercise the following rights[4]:

- the right to obtain information: the controller must provide the data subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data etc.);
- the data subject's right of access to data: every data subject should have the right to obtain his or her data from the controller;
- the right to object to the processing of data: the data subject should have the right to object, on legitimate grounds, to the processing of data relating to him/her. He/she should also have the right to object, on request and free of charge, to the processing of personal data that the controller anticipates being processed for the purposes of direct marketing. He/she should finally be informed before personal data are disclosed to third parties for the purposes of direct marketing, and be expressly offered the right to object to such disclosures.

Data processing must have a legal basis. These include where the:

- data subject has given his consent; or
- processing is necessary for the performance of a contract to which the data subject is party; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or
- processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

Other relevant issues for data processing:

- exemptions and restrictions from data subject's rights: the scope of the principles relating to the quality of the data, information to be given to the data subject, right of access and the publicising of processing may be restricted in order to safeguard interests such as national security, defence, public security, the prosecution of criminal offences, an important economic or financial interest of a Member State or of the European Union or the protection of the data subject;
- the confidentiality and security of processing: any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller. In addition, the controller must implement appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access;

4 Protection of personal data; EUR-Lex - l14012 - EN - EUR-Lex. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012 (accessed 1 June 2017).

- the notification of processing to a supervisory authority: the controller must notify the national supervisory authority before carrying out any processing operation – subject to certain exemptions. Prior checks to determine specific risks to the rights and freedoms of data subjects may be carried out by the supervisory authority following receipt of the notification. Measures are to be taken to ensure that processing operations are publicised and the supervisory authorities must keep a register of the processing operations notified.

Every person shall have the right to a judicial remedy for any breach of the rights guaranteed by national law applicable to the processing in question. In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered.

Transfers of personal data from a Member State to a third country with an adequate level of protection are authorised. However, although transfers may not take place when an adequate level of protection is not guaranteed, there are a number of exceptions to this rule listed in the Directive, e.g. the data subject agrees to the transfer, in the event of the conclusion of a contract, it is necessary on public interest grounds, or if Binding Corporate Rules or Standard Contractual Clauses have been authorised by the Member State.

The Directive aims to encourage the formulation of national and Community codes of conduct intended to contribute to the proper implementation of the national and Community provisions.

Each Member State must set up a supervisory authority[5]. According to Article 28 of the Directive, each Member State shall establish in its territory at least one data protection authority, which shall be endowed with investigative powers, effective powers of intervention, and the power to start legal proceedings when data protection law has been violated. A data protection authority is an independent body which is in charge of:

- monitoring the processing of personal data within its jurisdiction (country, region or international organisation);
- providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data;
- hearing complaints lodged by citizens with regard to the protection of their data protection rights.

A Working Party on the Protection of Individuals with regard to the Processing of Personal Data has been set up, composed of representatives of the national supervisory authorities, representatives of the supervisory authorities of the Community institutions and bodies, and a representative of the Commission[6].

The General Data Protection Regulation, adopted in April 2016, will supersede the Data Protection Directive and be enforceable starting on 25 May 2018. The UK government has confirmed that the country's decision to leave the EU will not affect the commencement of the GDPR[7].

5 Glossary - European Data Protection Supervisor. See https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/74

6 Protection of personal data; EUR-Lex - l14012 - EN - EUR-Lex. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012 (accessed 1 June 2017).

7 Overview of the GDPR - Introduction. See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/introduction/

### 3.2 The database directive[8]

The Directive on the legal protection of Databases was adopted in February 1996. The Directive created a new exclusive "sui generis" right for database producers, valid for 15 years, to protect their investment of time, money and effort, irrespective of whether the database is in itself innovative ("non-original" databases). It also harmonised copyright law applicable to the structure and arrangement of the contents of databases ("original" databases). The Directive's provisions apply to both analogue and digital databases[9].

The Directive constitutes a noteworthy event in the evolution of database protection worldwide[10]. It arose from the differing levels of legal protection that existed in the various Member States for databases. In response, the European Commission aimed to harmonise EU law among all Members through the adoption of uniform provisions for the protection of databases. Moreover, in the context of the internal European market, the Commission has sought greater protection for the capital investment required for database production and continued profit incentive for the producers.

The Recitals of the Directive offered several justifications for the harmonisation measure. To begin with, existing legislation in the Member States was deemed insufficient to protect databases, and even where such protection existed, it had different attributes. Additionally, the Recitals noted that such differences could become more pronounced through Member States' independent legislative acts. Furthermore, unharmonized intellectual property rights with respect to differences in scope and conditions of protection were considered a barrier to the free movement of goods and services within the Community. The Directive was also a response to advances in digital technology.

**Sui Generis Protection under the Directive:**

The Directive requires Member States to provide a new proprietary right for the protection of database contents. In order to obtain this sui generis right, a database maker must show that there has been a "substantial investment" in either the obtaining, verification, or presentation of the contents. In contrast to copyright protection, the Directive prescribes a "sweat of the brow" approach to allocating the sui generis right. Rather than defining what constitutes a "substantial investment," however, the Directive says little more than that this determination is to be made qualitatively and/or quantitatively. The sui generis right applies irrespective of the database's eligibility for copyright or other protection. The right is also transferable, assignable, and may be granted under contractual license.

Sui generis protection under the Directive gives the database maker the right "to prevent extraction and/or re-utilization of the whole or of a substantial part" of the database contents. Actions relating only to insubstantial parts are therefore non-infringing. An "extraction" involves either the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form. Even the viewing of database contents on-screen constitutes an action subject to authorisation by the rightsholder because it involves the transfer of all or a substantial part of the contents to another medium. "Reutilization" means any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, or by other forms of transmission, including on-line. However, the first sale of a copy of the database by the rightsholder exhausts the right to control resale of that copy within the Community. Furthermore, public lending is specifically excluded from definitions of either extraction or re-utilization.

8 DIRECTIVE 96/9/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL- EUR-Lex - 31996L0009 - EN - EUR-Lex." 2017. Accessed April 27. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31996L0009. (accessed 1 June 2017).

9 Protection of Databases - European Commission. See http://ec.europa.eu/internal_market/copyright/prot-databases/index_en.htm (accessed 1 June 2017).

10 Schneider M. The European Union Database Directive. Berkeley Technol Law J. 1998;13(1):551.

The term of protection for the sui generis right begins when the database is completed and ends fifteen years from the first of January following the date of completion. If the database is made available to the public before the fifteen-year term expires, then a new fifteen-year term begins from the first of January following the date that the database was first made available to the public. Any substantial change to the contents of the database that constitutes a "substantial new investment" entitles the database to a new fifteen-year term of protection. Depending on what level of investment is ultimately required to be "substantial," the provision for a renewable sui generis right could last in perpetuity if the contents are regularly updated[11].

### 3.3 The ePrivacy directive[12]

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), known as the ePrivacy Directive, sets out rules on how providers of electronic communication services, such as telecoms companies and Internet Service Providers, should manage their subscribers' data. It also guarantees rights for subscribers when they use these services. These are the main requirements imposed by the Directive[13]:

1. Confidentiality of communications: EU Member States must ensure the confidentiality of communications over public networks, in particular by prohibiting the listening into, tapping and storage of communications without the consent of the users concerned.
2. Security of networks and services: a provider of a public electronic communications service has to take appropriate measures to safeguard the security of its service.
3. Data breach notifications: if a provider suffers a breach of security that leads to personal data being lost or stolen, it has to inform the national authority and, in certain cases, the subscriber or individual.
4. Traffic and location data: this data must be erased or made anonymous when no longer required for communication or billing purposes, except if the subscriber has given consent for another use.
5. Spam: subscribers must give their prior consent before unsolicited commercial communications ("spam") are addressed to them. This also covers SMS text messages and other electronic messages received on any fixed or mobile terminal.
6. Public directories: subscribers' prior consent is required in order for their telephone numbers, e-mail addresses and postal addresses to appear in public directories.
7. Calling-line identification: subscribers must be given the option not to have their telephone number disclosed when they make a call.

The European Commission has reviewed the Directive to align it with the new data protection rules. In the past years, the Commission has started a modernisation process of the data protection framework, which culminated in the adoption in May 2016 of the new General Data Protection Regulation. The ePrivacy legislation needs to be adapted to align with these new rules.

The new proposal for a regulation on high level of privacy rules for all electronic communications includes[14]:

- Ensuring that privacy rules will in the future also apply to providers of electronic communications services such as WhatsApp, Facebook Messenger and Skype. This will ensure that these popular services guarantee the same level of confidentiality of communications as traditional telecoms operators.
- Stronger rules: all people and businesses in the EU will enjoy the same level of protection of their electronic communications through this directly applicable regulation. Businesses should also benefit from one single set of rules across the EU.

11 Schneider M. The European Union Database Directive. Berkeley Technol Law J. 1998;13(1):551.

12 Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) EUR-Lex - 32002L0058; See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (accessed 1 June 2017).

13 The ePrivacy Directive. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive (accessed 1 June 2017).

14 Proposal for an ePrivacy Regulation. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (accessed 1 June 2017).

- Communications content and metadata: privacy is guaranteed for communications content and metadata, e.g. time of a call and location. Metadata have a high privacy component and are to be anonymised or deleted if users did not give their consent, unless the data is needed for billing.
- New business opportunities: once consent is given for communications data - content and/or metadata - to be processed, traditional telecoms operators will have more opportunities to provide additional services and to develop their businesses. For example, they could produce heat maps indicating the presence of individuals; these could help public authorities and transport companies when developing new infrastructure projects.
- Simpler rules on cookies: the cookie provision, which has resulted in an overload of consent requests for internet users, will be streamlined. The new rule will be more user-friendly as browser settings will provide for an easy way to accept or refuse tracking cookies and other identifiers. The proposal also clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history) or cookies used by a website to count the number of visitors.
- Protection against spam: this proposal bans unsolicited electronic communications by emails, SMS and automated calling machines. Depending on national law people will either be protected by default or be able to use a do-not-call list to not receive marketing phone calls. Marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call.
- More effective enforcement: the enforcement of the confidentiality rules in the Regulation will be the responsibility of data protection authorities, who will already be in charge of the rules under the General Data Protection Regulation[15].

### 3.4 The General Data Protection Regulation (GDPR)[16]

On 25 January 2012, the European Commission (EC) announced it would unify data protection law across the European Union via the General Data Protection Regulation (Regulation (EU) 2016/679). The GDPR will be directly applicable in all EU Member States from 25 May 2018 and aims to strengthen the rights individuals have over their data and make companies take the issue of data protection more seriously, as well as simplifying the regulatory environment. The data protection principles are revised but are broadly similar to the principles set out in Directive 95/46/EC (the "Data Protection Directive"): fairness, lawfulness and transparency; purpose limitation; data minimisation; data quality; security, integrity and confidentiality. A new accountability principle makes controllers responsible for demonstrating compliance with the data protection principles[17].

#### 3.4.1 Key changes to previous laws

**The scope (Article 3)**

The proposed new EU data protection regime extends the scope of the EU data protection law to data controllers or processors outside the EU if offering goods or services (including free goods or services) to EU data subjects or if monitoring behaviour (within the EU) of EU data subjects. Under the GDPR, data processors have direct obligations for the first time.

**A single set of rules**

The proposed new EU data protection regime provides for a harmonisation of data protection law throughout the EU. Each member state will establish an independent Supervisory Authority (SA) to hear and investigate complaints, sanction administrative offences, etc. SAs in each Member State will cooperate with other SAs, providing mutual assistance and organising joint operations. Where a business has multiple establishments in the EU, it will have a single SA as its "lead authority", based on the location of its "main establishment" within the EU. The lead authority will act as a "one-stop shop" to supervise all the processing activities of that business throughout the EU.

15 Digital privacy. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/online-privacy (accessed 1 June 2017).

16 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). EUR-Lex - 32016R0679. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC (accessed 1 June 2017).

17 Bird & Bird GDPR guide PDF. Bird & Bird. See https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic (accessed 1 June 2017).

A European Data Protection Board (EDPB) will coordinate the SAs. EDPB will replace the Article 29 Working Party[18]. The Article 29 Working Party is composed of representatives of the national data protection authorities (DPA), the European Data Protection Supervisor (EDPS) and the European Commission. The Information Commissioner's Office (ICO) is an active member of A29 WP. "When the UK exits the EU, it appears to be likely that the ICO will lose its place on the EDPB, as a full member with decision making powers, unless a special status for the ICO can be negotiated. Loss of EDPB membership means the ICO would be unable to vote on guidelines, opinions and binding decisions in cross border enforcement matters"[19].

**Principles[20]**

The principles under the GDPR are broadly similar to those in the Data Protection Directive, but there are some new elements.

- Lawfulness, fairness and transparency: Personal data must be processed lawfully, fairly, and *in a transparent manner in relation to the data subject*.
- Purpose limitation: Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for *archiving purposes in the public interest*, or scientific and historical research purposes or statistical purposes shall not be considered incompatible with the original processing purposes. However, conditions in Article 89(1) (which sets out safeguards and derogations in relation to processing for such purposes) must be met.
- Data minimization: Personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed.
- Accuracy: Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Storage limitation: Personal data must be kept in a form *which permits identification of data subjects* for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for *archiving purposes in the public interest*, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1) and subject to implementation of appropriate technical and organisational measures.
- Integrity and confidentiality: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Accountability: The controller shall be responsible for and be *able to demonstrate* compliance with these principles[21].

18 Opinions and recommendations - European Commission. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (accessed 1 June 2017).

19 Brexit: future trade between the UK and EU in services publications. UK Parliament. See https://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-internal-market-subcommittee/inquiries/parliament-2015/brexit-future-trade-in-services-inquiry/brexit-future-trade-between-the-uk-and-eu-in-services/ (accessed 1 June 2017).

20 Bird & Bird GDPR guide PDF . Bird & Bird. See https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic (accessed 1 June 2017).

21 Bird & Bird GDPR guide PDF . Bird & Bird. See https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic.

**Lawful processing**[22]

For processing to be lawful under the GDPR, an organisation needs to identify a legal basis before they can process personal data. These are often referred to as the "conditions for processing" under the Data Protection Act. This becomes more of an issue under the GDPR because an organisation's legal basis for processing has an effect on individuals' rights.

Lawfulness of processing conditions:

- 6(1)(a) – Consent of the data subject;
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract;
- 6(1)(c) – Processing is necessary for compliance with a legal obligation;
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person;
- 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- 6(1)(f) – Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (not applicable to processing by public authorities in the performance of their tasks).

The GDPR allows member states to introduce more specific provisions in relation to Articles 6(1)(c) and (e).

Processing of special categories of personal data listed in Article 9(1) (racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data; and biometric data where processed to uniquely identify a person)[23] is prohibited unless one of the conditions in Article 9(2) applies:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law;
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;
- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
- 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent;

22 Overview of the General Data Protection Regulation (GDPR). 2017 Apr 6 ; See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

23 Bird & Bird GDPR guide PDF . Bird & Bird. See https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic

- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject;
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards;
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices;
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

**Further processing**

The GDPR also sets out the rules (at Article 6(4)) on factors a controller must take into account to assess whether a new processing purpose is compatible with the purpose for which the data were initially collected. Where such processing is not based on consent, or on Union or Member State law relating to matters specified in Article 23 (general article on restrictions relating to the protection of national security, criminal investigations etc.), the following factors should be taken into account in order to determine compatibility[24]:

- any link between the original and proposed new purposes;
- the context in which data have been collected (in particular the relationship between subjects and the controller);
- the nature of the data (particularly whether they are sensitive data or criminal offence data);
- the possible consequences of the proposed processing; and
- the existence of safeguards (including encryption or pseudonymisation).

Recital 50 indicates that further processing for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes should be considered as compatible processing[25].

24 Bird & Bird GDPR guide PDF . Bird & Bird. See https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic (accessed 1 June 2017).

25 Bird & Bird GDPR guide PDF. See https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic (accessed 1 June 2017).

**Responsibility and accountability**

According to the ICO's report 'Overview of the General Data Protection Regulation'[26], the GDPR's most significant addition in relation to the 1998 Data Protection Act[27] is the accountability principle. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR makes accountability an express legal requirement for the first time. The GDPR requires organisations to put into place comprehensive but proportionate governance measures. Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data.

The new accountability principle in Article 5(2) requires an organisation to demonstrate that it complies with the principles and states explicitly that this is their responsibility. Article 5(1) of the GDPR sets out the 'Principles relating to processing of personal data' and requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles." To demonstrate that they comply, organisations must:

- implement appropriate technical and organisational measures that ensure and demonstrate that they comply;
- maintain relevant documentation on processing activities;
- where appropriate, appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default (Article 25). Measures could include: Data minimisation; Pseudonymisation; Transparency; Allowing individuals to monitor processing; and creating and improving security features on an ongoing basis; and
- use data protection impact assessments where appropriate.

26 Overview of the General Data Protection Regulation (GDPR). 2017 Apr 6. See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ (accessed 26 April 2017).

27 Data Protection Act 1998; See http://www.legislation.gov.uk/ukpga/1998/29/contents (accessed 1 June 2017).

Organisations can also adhere to approved codes of conduct and/or certification schemes established pursuant to Article 42[28]. Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers an organisation's processing activity becomes available, they may wish to consider working towards it as a way of demonstrating that they comply. Governments and regulators can encourage the formulation of codes of conduct and certification schemes. Codes and certification schemes must be approved by the relevant supervisory authority; and where the processing is cross-border, the European Data Protection Board (the EDPB). Existing codes can be amended or extended to comply with the requirements under the GDPR.

**Consent[29]**

The GDPR has references to both 'consent' and 'explicit consent'. The difference between the two is not clear given that both forms of consent have to be freely given, specific, informed and an unambiguous indication of the individual's wishes (Article 4(11)). Recital 32 states that silence, pre-ticked boxes or inactivity should not constitute consent, although the Recital continues that consent can be shown through 'another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.' Explicit consent however may require a positive opt-in or declaratory statement.

Consent must be verifiable. This means that some form of record must be kept of how and when consent was given. Individuals have a right to withdraw consent at any time (Article 7(3)).

When assessing whether consent is freely given, account should be taken of whether the performance of a contract is conditional on consent to processing personal data that is not necessary for the performance of that contract (Article 7(4)). This is particularly relevant to e-commerce transactions where consent for an additional purpose may be required prior to being able to use a service.

Organisations can rely on alternative legal bases to consent – for example, where processing is necessary for the purposes of an organisation's or a third party's legitimate interests. Where an organisation already relies on consent that was sought under the Data Protection Act or the 1995 Data Protection Directive, they will not be required to obtain fresh consent from individuals if the standard of that consent meets the new requirements under the GDPR. If consent is being relied on, then implementation of the GDPR will require a review of consent mechanisms to ensure they meet the standards required under the legislation.

**Children's personal data[30]**

The GDPR contains new provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, organisations must ensure that a privacy notice is written in a clear, plain way that a child will understand (Article 12(1)). There are still alternatives to consent when processing a child's personal data – for example 'legitimate interests'. Under Article 8, if an organisation offers an 'information society service' at children, the child's consent cannot be valid. If consent is to be relied on, the consent must be of the child's parent or guardian – rather than the child him or herself. The GDPR states that if consent it being relied on, parental/guardian consent for access to information society services is required for children aged 16 and under – but it does permit member states to provide for a lower age in law, as long as it is not below 13. Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

28 Article 42(1): "The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account".

29 Overview of the General Data Protection Regulation (GDPR). 2017 Apr 6; See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ (accessed 26 April 2017).

30 Overview of the General Data Protection Regulation (GDPR); See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ (accessed 1 June 2017).

**Transfer of data[31]:** The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR. Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection. Under Article 46, adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses authorised by the competent supervisory authority; or
- provisions inserted in to administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations (Article 49). A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed explicit consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

31 Overview of the General Data Protection Regulation (GDPR); See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ (accessed 1 June 2017).

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU. However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

**Data Protection Officer**

In certain cases, a Data Protection Officer (DPO) must be designated by a data controller or processor including where processing is by a public authority. A person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with the GDPR. The DPO's minimum tasks are defined in Article 39:

1. To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
2. To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
3. To be the first point of contact for supervisory authorities including prior consultation obligations.

**Data protection by design and by default**

Under the GDPR, organisations have a general obligation to implement technical and organisational measures to show that they have considered and integrated data protection into their processing activities. Under the Data Protection Act, privacy by design has always been an implicit requirement of the principles – e.g. relevance and non-excessiveness.

**National derogations**

Article 23 enables Member States to introduce derogations to the GDPR in certain situations. These are similar to the existing exemptions from rights and duties in the DPA.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

- freedom of expression and freedom of information;
- public access to official documents;
- national identification numbers;
- processing of employee data;
- processing for archiving purposes and for scientific or historical research and statistical purposes;
- secrecy obligations; and
- churches and religious associations.

**Data breaches**[32]

The GDPR (Article 33) introduces a duty on all organisations to report certain types of data breach to the relevant supervisory authority within 72 hours, and in some cases to the individuals affected. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Organisations only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must notify those concerned directly (Article 34). A breach notification must contain the following information:

- The nature of the personal data breach.
- The name and contact details of the data protection officer or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows organisations to provide information in phases.

**Sanctions**

There is a tiered approach to fines up to 4% of annual worldwide turnover or EUR 20 million whichever is higher.

### 3.4.2 Individual rights under GDPR – Chapter III[33]

1. **The right to be informed (Articles 13 and 14)**
   It encompasses the obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for fairness and transparency over how the organisation uses personal data.

The GDPR sets out the information that organisations should supply and when individuals should be informed. When and how organisations supply information is determined by whether or not they obtained the personal data directly from individuals. The information organisations supply about the processing of personal data must be: concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

32 Overview of the General Data Protection Regulation (GDPR). 2017 Apr 6 ; See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ (accessed 26 April 2017).

33 Individuals' rights. 2017 Apr 6 ; See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/ (accessed 26 April 2017).

2. **The right of access (Article 15)**[34]
   Individuals have the right to obtain confirmation that their data is being processed; access to their personal data; and other supplementary information including the existence of automated decision-making, including profiling and meaningful information about the logic involved and the significance and consequences for data subjects (Article 15(1)(h)). These are similar to existing subject access rights under the Data Protection Act. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

Organisations will have less time to comply with a subject access request under the GDPR than under the Data Protection Act. Information must be provided without delay and at the latest within one month of receipt (which can be extended by two further months where necessary, Article 12(3)). Where requests are manifestly unfounded or excessive, in particular because they are repetitive, organisations can charge a reasonable fee taking into account the administrative costs of providing the information; or refuse to respond. Where an organisation refuses to respond to a request, they must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month (Article 12(4)).

The GDPR introduces a new best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

3. **The right to rectification (Article 16)**
   Individuals are entitled to have personal data rectified or completed if it is inaccurate or incomplete.

If an organisation has disclosed the personal data in question to third parties, they must inform recipients of the rectification where possible. Organisations must also inform the individuals about the third parties to whom the data has been disclosed where appropriate. Where an organisation is not taking action in response to a request for rectification, it must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

4. **The right to erasure (Article 17)**[35]
   Also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data are no longer necessary in relation to the purpose for which they were originally collected/processed.
- When the individual withdraws consent and where there are no other legal grounds for processing.
- When the individual objects to the processing and there is no overriding legitimate ground for continuing the processing.
- The personal data were unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data must be erased in order to comply with a legal obligation.
- The personal data are processed in relation to the offer of information society services to a child.

Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

34 See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/ (accessed 26 April 2017).

35 Individuals' rights. 2017 Apr 6;
See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/ (accessed 26 April 2017).

An organisation can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- for archiving purposes in the public interest, scientific or historical research or statistical purposes; or
- for the establishment, exercise or defence of legal claims.

There are extra requirements when the request for erasure relates to children's personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments. If an organisation processes the personal data of children, it should pay special attention to existing situations where a child has given consent to processing and later requested erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should take reasonable steps to inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question (Article 17(2)).

5. **The right to restrict processing (Article 18)**[36]
   Individuals have a right to obtain from the controller restriction of processing of personal data. When processing is restricted, organisations are permitted to store the personal data, but not further process it unless the data subject consents or for legal claims, the protection of another's rights or for important public interest reasons.

An organisation will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, the organisation should restrict the processing until they have verified the accuracy of the personal data.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If an organisation no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the organisation is considering whether its legitimate grounds override those of the individual.

An organisation may need to review procedures to ensure that they are able to determine where they may be required to restrict the processing of personal data.

6. **The right to data portability (Article 20)**
   The right to data portability allows individuals to receive his/her personal data, which he/she has provided to a controller, in a structured, commonly used and machine readable format and the right to transmit those data to another controller without hindrance[37].

The right to data portability only applies: to personal data an individual has provided to a controller; where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means.

If the individual requests it, organisations may be required to transmit the data directly to another organisation if this is technically feasible. However, they are not required to adopt or maintain processing systems that are technically compatible with other organisations.

36 Individuals' rights. 2017 Apr 6 ;
See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/ (accessed 1 June 2017).

37 Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits. See: Individuals' rights;
See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/ (accessed 1 June 2017).

7. **The right to object (Article 21)**
   Individuals have the right to object (on grounds based on his/her particular situation) to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling). An individual also has the right to object to processing for direct marketing (including profiling); and to object (on grounds based on his/her particular situation) to processing for purposes of scientific/historical research and statistics.

An organisation must stop processing the personal data on legitimate interest/public task grounds unless: it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims. An organisation must stop processing personal data for direct marketing purposes as soon as they receive an objection (Article 21(3)). There are no exemptions or grounds to refuse. They must deal with an objection to processing for direct marketing at any time and free of charge and must inform individuals of their right to object "at the point of first communication" and in the privacy notice. These requirements are similar to existing rules under the DPA.

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes. If an organisation is conducting research where the processing of personal data is necessary for the performance of a public interest task, they are not required to comply with an objection to the processing.

8. **Rights in relation to automated decision making and profiling (Article 22)**[38]
   The GDPR provides a right for individuals not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects significantly affecting him or her. These rights work in a similar way to existing rights under the DPA.

Individuals have the right not to be subject to a decision when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

Organisations must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

The right does not apply if the decision:

- is necessary for entering into or performance of a contract between an organisation and the individual;
- is authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or
- based on explicit consent. (Article 9(2)).

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

38 Individuals' rights. 2017 Apr 6 ;
See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/ (accessed 26 April 2017).

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

When processing personal data for profiling purposes, organisations must ensure that appropriate safeguards are in place. They must:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) must not:

- concern a child; or
- be based on the processing of special categories of data unless:
- an organisation has the explicit consent of the individual; or the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

### 3.4.3 Challenges

1. **General challenges**

The general challenge in data governance is to construct an adequate regulatory environment for the collection, processing and use of data. The environment will not be adequate unless:

- the formal legal framework is reasonably well connected to the underlying technologies for collecting, processing and using data;
- the regulatory objectives are clear and coherent (i.e. regulators have a clear and coherent sense of what they are trying to do); and
- the public have trust and confidence in the regulatory environment—implying that the public believe that regulators are trying to do the right thing and that they are doing so reasonably effectively.

Although perfection is not expected, the regulatory environment will not suffice unless it scores reasonably well in relation to these criteria.

39 For a critique, see: None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive | Brookings; 2012. See https://www.brookings.edu/events/none-of-your-business-world-data-flows-electronic-commerce-and-the-european-privacy-directive/ (accessed 1 June 2017).

The first criterion is extremely demanding. Information and Communication Technologies (ICTs) and digital technologies have moved very quickly. The Data Protection Directive and the UK implementing legislation were already way behind the state of the technology when they were enacted (see challenge 2 below). They were never adequately connected . It is unlikely that the GDPR is better connected to the technology. There have been huge leaps forward in machine learning and artificial intelligence (AI) as this Regulation has been going through and, although attempts have been made to make some connection, the challenge for the UK is not to try to keep pace (that's almost impossible); rather the challenge is to be smart enough to get ahead of the technology.

The second criterion is less demanding, however, the Data Protection Directive tried to bring together freer flowing data (across borders) with privacy. The tension in this project is that privacy is about stopping data flowing rather than freeing it up to flow. The EU Charter gives some assistance to easing the tension by differentiating explicitly between the right to privacy and the right to data protection. However, the GDPR, now in the context of the digital Europe programme tries to reinforce privacy while embedding the protection in a data protection regime.

Issues with pseudonymisation (see challenge 4 below) and then data transfer (see challenge 5) can both be seen as issues for the third criterion. If the regulatory environment is predicated on the assumption that pseudonyimisation of data covers all objections, it will not be acceptable to those who think that they have a right to control the processing of their data (pseudonymised or not); and, as pseudonymisation can be cracked, a lack of confidence in the regulation will spread. As for data transfer, it reminds us that we live in a global village but with the EU and UK districts unable (whatever the rhetoric) to prevent the inward flow of spam and malware that compromises the infrastructure. Regulators are poorly resourced to deal with violations at home and in no shape to deal with violators who are based out of the jurisdiction.

So, the challenge is not to try to find the perfect form of legislative words. It is to find a way of getting ahead of the technology, anticipating the risks, drawing the red lines (especially around privacy), helping the public to take care of themselves in the digital world (especially when, before long, every home will have its own digital assistant), and putting more resource into compliance and preventing cybercrime.

2. **Big data, artificial intelligence and machine learning:** According to the ICO's report on Big data, artificial intelligence, machine learning and data protection[40], the use of big data analytics has several implications for data protection and privacy rights but various tools and approaches are available to help with compliance. Rather than restricting the use of big data analytics, these tools can encourage innovation and support delivery of the benefits that flow from big data. However, the ICO recognises the emerging view that the data protection principles, as embodied in UK and EU law, were never designed to deal with the entirety of the big data world. The World Economic Forum characterised the "traditional data protection approach" as one where "the individual was involved in consenting to data use at the time of collection. The organisation that collected the data then used it for a specified use, based on user consent, and then deleted the data when it was no longer needed for the specified purpose[41]." It is this model that critics of data protection have in mind.

40 Big data, artificial intelligence, machine learning and data protection. 2017 Mar 3; See https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (accessed 1 June 2017).

41 World Economic Forum Unlocking the value of personal data; from collection to usage. WEF, February 2013.

The complexity of big data analytics, artificial intelligence and machine learning can mean that the processing is opaque to citizens and consumers whose data is being used. It may not be apparent to them that their data is being collected, how it is being processed or what the personal and broader societal consequences are. Similarly, it may be unclear how decisions are being made about them. The opacity can also lead to a lack of trust that can affect people's perceptions of and engagement with the organisation doing the processing. This can be an issue in the public sector, where lack of public awareness can become a barrier to data sharing. Inadequate provision of information to the public about data use has been seen as a barrier to the roll-out of the care.data project in the NHS[42].

This so-called 'notice and consent' model has been criticised on the grounds that users lack the time, willingness or ability to read lengthy privacy notices or sets of terms and conditions; consequently, even if they give consent on this basis it is effectively meaningless. However, the notice and consent model is a fundamental facet of the data protection principle of transparency. The legal situation is therefore complex. Data protection law generally requires telling people who is collecting their data and why. Yet, it does not always require people to be given a choice over this.

Criticism of the notice and consent model is mirrored by wider criticism of the role of transparency in the evolving world of big data analytics. The GDPR does address significant problems with profiling, interpretation, and data processing[43] by providing users with the ability to challenge decisions based on algorithmic processes[44]. On top of that, the law generally provides an alternative to consent as the legal basis for processing personal data. It is generally a policy-call for an organisation as to whether to offer people a choice on how their personal data is collected and used. Some suggest, however, that the concept of transparency plus consent is inadequate when it comes to the complex and opaque nature of algorithms and that it can lead to "gaming of the decision-making process"[45].

In addition to arguments about the limitations of transparency, there is a view that the problems of big data analytics, artificial intelligence, and machine learning arise not specifically from how the data is collected but from how it is used. An increased focus on the use of data has led to the championing of accountability as

42 The UK government's care.data initiative was a programme intended to enable sharing of anonymised primary care health records with "researchers and organisations outside the NHS" for research and service improvement. In her review, Dame Fiona Caldicott recommended the Government consider the future of the care.data programme, as the consent and opt-out model proposed by the review goes further than the approach that was planned for care.data and its pathfinder areas. The programme was paused in 2014 due to a loss of public trust. Reasons cited for this loss of public trust included concerns that personal health care data might be used inappropriately, e.g., sharing with insurance companies or being sold for profit, as well as lack of clarity as to how patients should opt out.

43 (71)" The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her".

44 The Limits of Parental Consent in an Algorithmic World. Media Policy Project. 2016;
See http://blogs.lse.ac.uk/mediapolicyproject/2016/11/28/the-limits-of-parental-consent-in-an-algorithmic-world/ (accessed 1 June 2017).

45 Kroll JA, Huey J, Barocas S, Felten EW, Reidenberg JR, Robinson DG, et al. Accountable Algorithms. 2016 Mar 2;
See https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765268 (accessed 1 June 2017).

opposed to transparency – although one can be seen as a function of the other (as far as personal data is involved, transparency remains a legal requirement for organisations carrying out big data analytics). Rather than focusing on providing people with the 'hows' and 'whys' of the processing of their personal data, accountability concentrates on monitoring its use through mechanisms such as scrutinising the technical design of algorithms, auditability and software-defined regulation.

The emerging importance of accountability is reflected in the GDPR, which includes it as a new data protection principle and is, in part, being introduced to address the implications of the processing of personal data in a big data world. New provisions regarding data protection by design and default, data protection impact assessments and certification all emphasise the growing role accountability has to play both within organisations and externally. However, although early drafts of the GDPR enshrined what is called a "right to explanation" in law, researchers[46] argue that the final version contains no legal guarantee. Since approval of the GDPR in 2016, it has been widely claimed that a 'right to explanation' of decisions made by automated or artificially intelligent algorithmic systems will be legally mandated by the regulation. This right to explanation is viewed as an ideal mechanism to enhance the accountability and transparency of automated decision-making. Yet, there are several reasons to doubt both the legal existence and the feasibility of such a right. "There is an idea that the GDPR will deliver accountability and transparency for AI, but that's not at all guaranteed. It all depends on how it is interpreted in the future by national and European courts"[47].

The ambiguity and limited scope of the 'right not to be subject to automated decision-making' contained in Article 22 (from which the 'right to explanation' stems) raises questions over the protection actually afforded to data subjects. The best the new regulation offers is a "right to be informed" compelling companies to reveal the purpose of an algorithm, the kinds of data it draws on to make its decisions, and other basic information (Articles 13-15). The researchers argue for the regulation to be amended to make the "right to explanation" legally binding. "We are already too dependent on algorithms to give up the right to question their decisions. The GDPR should be improved to ensure that such a right is fully and unambiguously supported"[48]. "The GDPR lacks precise language as well as explicit and well-defined rights and safeguards against automated decision-making, and therefore runs the risk of being toothless"[49]. However, regulators may see things differently. In the ICO's view, the requirement under GDPR to provide meaningful information about the logic involved in automated decision making amounts to providing an explanation of it, including of its consequences. The ICO argues that the GDPR in fact does provide a comprehensive transparency mechanism for all organisations processing personal data in big data and other contexts. The ICO recognises the challenges of explaining how – for example – artificial intelligence works. However, the ICO has explained that it will use its powers to ensure that organisations provide individuals with explanations that are as clear and comprehensive as the circumstances allow and encourages organisations to innovate and recognises the limitations of a long, detailed 'notice' type approach[50]. The ICO also recognises that as data protection law is only concerned with personal data, it has its limits in terms of regulating the broader societal consequences of big data once the data being analysed has ceased to be 'personal'.

46 Wachter S, Mittelstadt B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. 28 Dec 2016; See https://ssrn.com/abstract=2903469 (accessed 1 June 2017).

47 Wachter S, Mittelstadt B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. 28 Dec 2016; See https://ssrn.com/abstract=2903469 (accessed 1 June 2017).

48 Wachter S, Mittelstadt B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. 28 Dec 2016; See https://ssrn.com/abstract=2903469 (accessed 1 June 2017).

49 Wachter S, Mittelstadt B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. 28 Dec 2016; See https://ssrn.com/abstract=2903469 (accessed 1 June 2017).

50 Processing personal data fairly and lawfully (Principle 1). 1 Feb 2017; See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/ (accessed 1 June 2017).

According to the ICO's approach, achieving transparency is not impossible in a big data world. But the methods by which it is achieved are altering, with a shift towards a more 'layered' approach to transparency. This approach is exemplified in the layering of privacy notices to individuals (as and when the purposes for collecting and using their personal data emerge), and also in the layering of information about the inner workings of big data analytics, with a greater level of detail and access given to regulators, auditors and accredited certification bodies. The ICO's approach envisages individuals being given appropriate information (and choices where appropriate) at appropriate times, as an alternative to 'classical' terms and conditions type privacy notices. Big data analytics and data protection should not be viewed in simple binary terms; the same also applies to the principles of transparency and accountability. There has been somewhat of a paradigm shift regarding the emerging importance of accountability, but this is not a wholesale replacement for transparency. In fact, the Centre for Information Policy Leadership lists transparency as part of one of the essential elements of accountability. In the ICO's view, a combination of both approaches will help to ensure the protection of privacy rights while delivering the benefits of big data[51]. As noted above, transparency and accountability can be seen as functions of each other – and present a powerful combination in terms of individual empowerment and engagement and the fostering of corporate responsibility.

There are other suggestions to deal with these issues. Wachter, Mittelstadt and Floridi (2016)[52] propose a number of legislative steps that, if taken, may improve the transparency and accountability of automated decision-making when the GDPR comes into force in 2018. The researchers also suggest that an artificial intelligence watchdog should be set up to make sure people are not discriminated against by the automated computer systems making important decisions about their lives. The rise of artificial intelligence has led to an explosion in the number of algorithms that are used by employers, banks, police forces and others, but the systems can make bad decisions that seriously impact people's lives. But because technology companies are so secretive about how their algorithms work – to prevent other firms from copying them – they rarely disclose any detailed information about how AI algorithms have made particular decisions. According to them, there should be a trusted third party body that can investigate AI decisions for people who believe they have been discriminated against. "What we'd like to see is a trusted third party, perhaps a regulatory or supervisory body, that would have the power to scrutinise and audit algorithms, so they could go in and see whether the system is actually transparent and fair"[53]. In the ICO's view, however, it would be important for any such body to work alongside existing regulators, to provide comprehensive individual and societal protection and to avoid confusing regulatory overlaps and the creation of competing standards.

51 Big data, artificial intelligence, machine learning and data protection. 3 Mar 2017; See https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (accessed 1 June 2017).

52 Wachter S, Mittelstadt B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. 28 Dec 2016; See https://ssrn.com/abstract=2903469 (accessed 1 June 2017).

53 AI watchdog needed to regulate automated decision-making, say experts. The Guardian . 2017 Jan 27 ; See http://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions (accessed 1 June 2017).

3. **Processing special categories of data:** Under the Data Protection Directive, the processing of special categories of personal data is prohibited unless there is a specific legal ground to process such data. These grounds consist mainly of the consent of the individual, the performance of specific contracts, or processing for specific purposes. Increasingly, it is becoming unclear whether specific categories of data are sensitive. Rather, the use of data may be sensitive. Furthermore, several types of data do not belong to special categories of data according to the law, but are sensitive because of the potential impact on individuals if the data are lost or stolen. Generally, the ICO has recognised this contextual approach and has focussed on the risk to individuals in the round, rather than just the nature of the data involved. However, data protection law is framed in a simple binary/non-binary system.

Practice shows that the same data may be sensitive in one context but not in another (particularly where data are combined) – and that data that is not technically 'sensitive', for example financial data, can be very sensitive in real-world contexts. Therefore, the existing regime — which is based on the processing of a pre-defined set of special categories of data — does not achieve the intended effect. The regime does not include a check on whether there is a legitimate interest for the use of special categories of data. Under the Directive, the legitimate interest ground is not available as a legal ground for processing of special categories of data. Reviewing the specific legal grounds further shows that none of them require a contextual balancing of interests, which would include an assessment of the measures taken by the data controller to mitigate any adverse effects on the privacy of the individuals concerned[54]. This has also been acknowledged by the WP29[55].

The WP29 has attempted to overcome this problem by requiring that the protection of such data under Article 8 of the Directive (the regime for special categories of data) should not be less than if the processing had been based on Article 7 (providing the legal grounds for the processing of regular personal data)[56]. The WP29 accommodates the ground of consent by specifying that the principles of Article 6 of the Directive are applicable (personal data must be processed fairly and lawfully, and the requirements of necessity and proportionality apply)[57].

According to some experts[58], in light of these shortcomings and the additional requirements introduced by the WP29, the effectiveness and legitimacy of the GDPR would have been served by abolishing the separate regime for special categories of personal data. Instead, it would have been preferable if it could have moved to a framework whereby the legitimate interest ground would have been the principal test for the various phases of the life cycle of all types of personal data: collection, use, further use and destruction. However, the specific regime for special categories of data remains in place in Articles 9 and 10 of the GDPR. The shortcomings described above are, to a large extent, offset by the new requirement to perform a Data Protection Impact Assessment (DPIA), when a type of processing is likely to result in a high risk to the rights and freedoms of individuals, and this is an explicit requirement in the case of large-scale processing of special categories of data (Article 35(3)(b) of the GDPR). Based on this approach, the conclusion is that the GDPR will not bring the required improvements in terms of legal complexity. Data controllers must consult their supervisory authorities prior to starting data processing when the DPIA indicates that such processing would result in a high risk in the absence of mitigating measures taken by the controller. However, the prevailing view within the data protection supervisory authorities seems to be that if the mitigating factors are put in place then supervisory authority consultation will

54 GDPR conundrums: Processing special categories of data. See https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/ (accessed 1 June 2017).

55 Opinions and recommendations - European Commission. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (accessed 1 June 2017).

56 Opinions and recommendations - European Commission. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (accessed 1 June 2017).

57 Opinions and recommendations - European Commission. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (accessed 1 June 2017).

58 GDPR conundrums: Processing special categories of data. See https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/ (accessed 1 June 2017).

not be necessary. In their view, the text of the GDPR is open to interpretation and ultimately this issue could be tested before the courts.

4. **Pseudonymisation:** The GDPR introduces the concept of pseudonymisation. The concept refers to the technique of processing personal data in such a way that it can no longer be attributed to a specific "data subject" without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution. Organisations must be able to demonstrate their compliance with the GDPR's principles, including by adopting certain "data protection by design" measures (for example the use of pseudonymisation techniques), staff training programmes and adopting policies and procedures[59]. Rather than having a separate data class of 'pseudonymous data' – as envisaged in early drafts of the GDPR – the concept was somewhat 'demoted' to be a security measure.

There are three major roles of anonymisation and pseudonymisation and there are significant differences between the two techniques. First, anonymisation and pseudonymisation can serve as a safe harbour from the entire application of data privacy rules provided they are used to irreversibly prevent identification, although achieving this goal seems increasingly challenging in the current state of technological advancement. It is possible, though, for the 'additional information' referred to above to be destroyed meaning that the pseudonym can no longer be attributed to a living individual so will in effect become anonymous. Second, anonymisation and pseudonymisation can provide a safe harbour from certain data privacy obligations, such as the notification of personal data breaches, provided they are engineered appropriately and complemented by adequate organisational measures. Third, anonymisation and pseudonymisation can constitute mandated measures for compliance with data privacy obligations, such as the data security and purpose specification and limitation principles[60].

Substantial uncertainty however exists on the role of anonymised or pseudonymised data in the data privacy discourse; this is even more so as de-anonymisation science advances and the ubiquity of information increases. Such uncertainty affects not only the wider usage of such measures but also creates the temptation, both on the part of the entities that process personal data and the individuals whose personal data is processed, to downplay privacy risks associated with anonymised or pseudonymised data[61]. The ICO's argument is that it is better to focus on attributing compliance duties and data protection measures according to the potential risks to the original subjects of personally identifiable information – and information derived from that. Although regulators can build it – to an extent – into their regulatory approaches, the law however does not support that approach.

59 Bird & Bird GDPR guide PDF.
See https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic (accessed 1 June 2017).

60 Esayas SY. The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the "All or Nothing" Approach. 2015;
See https://ssrn.com/abstract=2746831 (accessed 1 June 2017).

61 Esayas SY. (2015).

Under the Directive, the Article 29 Working Party found that "pseudonymisation is not a method of anonymisation. It merely reduces the linkability of a dataset with the original identity of a data subject, and is accordingly a useful security measure"[62]. Because some risks of reidentification remained, even if those risks were very small, the Working Party found that the data was still covered by the Directive if any third party could conceivably reidentify the data sometime in the future. A controller could escape regulation only by not collecting identifying information in the first place[63]. According to the International Association of Privacy Professionals (IAPP), pseudonymised data, unlike anonymous data, faces the risk of reidentification in two ways. First, a data breach may permit an attacker to obtain the key or otherwise link the pseudonymised data set to individual identities. Alternatively, even if the key is not revealed, a malicious actor may be able to identify individuals by combining indirect identifiers in the pseudonymous database with other available information[64]. However, if the key is irreversibly and permanently destroyed then this raises questions over the veracity of this approach, and of the status of the residual information.

The GDPR addresses the first concern in Recital 75, which instructs controllers to implement appropriate safeguards to prevent the "unauthorised reversal of pseudonymisation." To mitigate the risk, controllers should have in place appropriate technical (e.g. encryption, hashing or tokenization) and organisational (e.g. agreements, policies, privacy by design) measures separating pseudonymous data from an identification key. In Recital 26, the GDPR recognises the second type of reidentification risk by considering whether a method of reidentification is "reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." Such an analysis is necessarily contextual and "account should be taken of all the objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

Despite the legal complexity here, the ICO and other Data Protection regulators argue that pseudonymisation remains an important means of reducing information risk and minimising the chances of data used in research and other contexts having a negative effect on particular individuals.

5. **Data transfer:** Under the GDPR, certain provisions become directly applicable to EU processors, including the data transfer requirements. Article 46 of the GDPR provides that controllers and processors may only transfer personal data to third countries that do not provide for an adequate protection (non-adequate countries), if the controller or processor has provided "adequate safeguards," and on condition that individuals are provided with enforceable rights and effective legal remedies. However, some experts believe that it is not correct to impose the same regime that applies to controllers also to processors[65]. The transfer requirement should only apply to processors when they transfer data to a sub-processor in a non-adequate country (and not when they transfer data to a controller) and then in respect of their own data processor obligations only (and not the full scope of the GDPR). The regime should therefore neither apply when the processor transfers the data back to the original controller on whose behalf the processor is processing the data nor when transferring to subsequent controllers if the processor is instructed to do so by the original controller.

62 Opinions and recommendations - European Commission.
See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (accessed 1 June 2017).

63 Top 10 operational impacts of the GDPR: Part 8 - Pseudonymization.
See https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/ (accessed 1 June 2017).

64 Top 10 operational impacts of the GDPR: Part 8 - Pseudonymization.
See https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/ (accessed 1 June 2017).

65 GDPR conundrums: Data transfer.
See https://iapp.org/news/a/gdpr-conundrums-data-transfer/ (accessed 1 June 2017).

Many EU DPAs have indicated that if the relevant data is coming from outside the EU and transferred back again, EU data protection law applies and therefore also the EU data transfer rules, but that enforcement of these rules "will not be their priority." According to the WP29, the result that EU law applies to these data processing activities has "unsatisfactory consequences" and is also not satisfactory in that "European data protection law is applicable in cases where there is a limited connection with the EU," which "may have undesirable consequences in terms of economic impact and enforceability"[66].

Rather than applying the full scope of the directive also to EU data processors, the WP29 suggested as an option[67] that the data processor becomes subject to specific EU data protection provisions only, such as in any event the EU data security provisions. The GDPR indeed deals with this issue by limiting its scope (and dropping the equipment criterion) and imposing certain direct obligations on processors.

Some experts believe that the transfer rules should only apply to processors insofar as they transfer data to a sub-processor in a non-adequate country and then only in respect of their own legal obligations under the GDPR. The WP29 already made draft Processor SCCs for this situation. It would help if the WP29 could clarify that this is indeed how the data-transfer requirements for processors should be applied. "The current provision whereby processors are required to impose "adequate safeguards" in case of transfers to all third parties in a non-adequate country – therefore both controllers and processors – seems incorrect"[68]. On the other hand, there is an argument that the distinction between processors and controllers is becoming increasingly difficult to draw. An alternative approach might be to see both as organisations that process personal data and that each has its own responsibility in respect of the data.

### 3.5 Digital Single Market Strategy[69]

The European Commission's Digital Agenda forms one of the seven pillars of the Europe 2020 Strategy[70] for the growth of the European Union by 2020. The Digital Agenda's main objective is to develop a digital single market in order to generate smart, sustainable and inclusive growth in Europe. GDPR is a centrepiece of the EU Digital Single Market.

A Digital Single Market (DSM)[71] is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence.

The set of regulations and directives coming out of the Digital agenda include:

- Copyright in the Digital Single Market[72]: Delivering on its Digital Single Market Strategy, the Commission is rolling out an ambitious modernisation of the EU copyright framework[73]. EU actions have led to more harmonised protection of right holders, lower transaction costs and greater choice for users of content, notably through: a European regulatory framework for copyright and related rights; the promotion of inclusive and dynamic stakeholder's dialogues on copyright and related issues, to seek views, concrete experience and contributions from all interested parties; a leading role in international negotiations and discussions on copyright and related issues. The objective is to make EU copyright rules fit for the digital age.

66 Opinions and recommendations - European Commission. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (accessed 1 June 2017).

67 Opinions and recommendations - European Commission. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (accessed 1 June 2017).

68 GDPR conundrums: Data transfer. See https://iapp.org/news/a/gdpr-conundrums-data-transfer/ (accessed 1 June 2017).

69 Digital Single Market. See https://ec.europa.eu/digital-single-market/en/digital-single-market (accessed 1 June 2017).

70 EUR-Lex - em0028 - EN - EUR-Lex. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Aem0028 (accessed 1 June 2017).

71 EUR-Lex - 52015DC0192 - EN - EUR-Lex. See http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192 (accessed 1 June 2017).

72 Copyright. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/copyright (accessed 1 June 2017).

73 The EU copyright legislation. Digital Single Market. See https://ec.europa.eu/digital-single-market/eu-copyright-legislation (accessed 1 June 2017).

The Communication[74] on a modern and more European copyright framework sets out the main political objectives and areas of action as well as the timeline.

A first legislative proposal[75] on cross-border portability of online content services aims at ensuring that consumers who buy or subscribe to films, sport broadcasts, music, e-books and games can access them when they travel in other EU countries.

A second set of legislative proposals[76] aims at modernising the copyright framework, focusing on allowing for wider online availability of content across the EU, adapting exceptions and limitations to the digital world, and achieving a well-functioning copyright market place.

- Telecoms: The Commission proposed a new European Electronic Communications Code[77] including forward-looking and simplified rules that make it more attractive for all companies to invest in new top-quality infrastructures, everywhere in the EU, both locally and across national borders.
- Audio-visual media: A new legislative proposal amending the Revision of the Audio-visual Media Services Directive (AVMSD) has been adopted by the European Commission on 25 May 2016. The reform brings the Directive in line with the new realities[78].
- Review of the ePrivacy directive[79]: A consultation on the evaluation and review of the ePrivacy Directive was launched to gather input for the evaluation process in order to assess the current rules and to seek views on possible adaptations to the ePrivacy Directive considering market and technological developments.
- EU cyber security strategy[80]: The cybersecurity strategy for the European Union and the European Agenda on security provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime.
- Free Flow of Data Initiative[81]: Its aim is to ensure that data flows across borders and sectors in the EU. This data should be accessible and reusable by most stakeholders in an optimal way. A coordinated European approach is seen as essential for the development of the data economy, as part of the Digital Single Market strategy.

The Commission considers some necessary steps to ensure the free flow of data by tackling data location restrictions. It will also explore possible solutions to several legal uncertainties emerging in the data economy, such as access to and transfer of non-personal machine-generated data, data liability and portability of non-personal data, interoperability and standards.

The Commission has also launched a European Cloud initiative, covering certification, switching of cloud service providers and a research cloud.[82]

74 EUR-Lex - 52015DC0626 - EN - EUR-Lex. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A626%3AFIN (accessed 1 June 2017).

75 EUR-Lex - 52015PC0627 - EN - EUR-Lex. See http://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:52015PC0627 (accessed 1 June 2017).

76 Modernisation of the EU copyright rules. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules (accessed 1 June 2017).

77 Telecoms. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/telecoms (accessed 1 June 2017).

78 Revision of the Audiovisual Media Services Directive (AVMSD). Digital Single Market. See https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd (accessed 1 June 2017).

79 Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive (accessed 1 June 2017).

80 Cybersecurity. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/cybersecurity (accessed 1 June 2017).

81 Digital Single Market - Free Flow of Data Initiative. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/news/digital-single-market-free-flow-data-initiative (accessed 1 June 2017).

82 Economy & Society. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/economy-society-digital-single-market (accessed 1 June 2017).

### 3.5.1 Challenges[83]

According to the European Commission, the benefits of the Single Market sometimes do not materialise because the rules are not known or implemented, or they are undermined by other barriers. That is why the Commission has decided to give the Single Market a boost by taking measures that will[84]:

- Enable the balanced development of the collaborative economy.
- Help SMEs and start-ups to grow.
- Improve the opportunities for businesses and professionals to move across borders.
- Address restrictions in the retail sector.
- Prevent discrimination against consumers based on nationality or place of residence.
- Modernise the standards system.
- Create more transparent, efficient and accountable public procurement.
- Consolidate Europe's intellectual property framework.
- Ensure a culture of compliance and smart enforcement to help deliver a true Single Market.

The European Commission is currently defining, scoping and articulating the following issues in order to trigger and frame a dialogue with stakeholders:

- Non-personal machine-generated data need to be tradable to allow innovative business models to flourish, new market entrants to propose new ideas and start-ups to have a fair chance to compete.
- Data-driven technologies are transforming the economy and society, resulting in the production of ever-increasing amounts of data. This phenomenon leads to innovative ways of collecting, acquiring, processing and using data which can pose a challenge to the current legal framework.
- Access to and transfer of non-personal data, data liability, as well as portability of non-personal data, interoperability and standards are complex legal issues.

83 Building a European Data Economy. Digital Single Market. See https://ec.europa.eu/digital-single-market/en/building-european-data-economy (accessed 1 June 2017).

84 The Single Market Strategy - Growth - European Commission. Growth. See http://ec.europa.eu/growth/single-market/strategy_en (accessed 1 June 2017).

CHAPTER 4

# UK data regulation

This section sets out the main UK data governance framework. The aim is to summarise the main elements of the UK framework outlining its focus and purpose.

## 4.1 Current regulation and regulatory bodies

### 4.1.1 The Information Commissioner's Office – ICO

- **Definition**
  The ICO is the UK's independent body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They are in charge of improving the information rights practices of organisations by gathering and dealing with concerns raised by members of the public. ICO has a duty to co-operate with the other EU data protection authorities, but also works jointly with other bodies within and beyond the EU.
- **Enforcement**
  There are a number of tools[85] available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. The main options are:

  1. Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period.
  2. Issue undertakings committing an organisation to a particular course of action in order to improve its compliance.
  3. Serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law.
  4. Conduct consensual assessments (audits) to check organisations are complying.
  5. Serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice.
  6. Issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.
  7. Prosecute those who commit criminal offences under the Act.
  8. Report to Parliament on issues of concern.

- **Tools of Governance:** The ICO oversees the following legislation:

#### a) Data Protection Act (1998)[86]

The 1998 Data Protection Act (DPA) defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Although the Act itself does not mention privacy, it was enacted to bring British law into line with the 1995 EU Data Protection Directive. In practice, it provides a way for individuals to control information about themselves.

85 Taking action - data protection; See https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/ (accessed 1 June 2017).
86 Guide to data protection; See https://ico.org.uk/for-organisations/guide-to-data-protection/ (accessed 1 June 2017).

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available; or
- alignment, combination, blocking, erasure or destruction of the information or data[87].

### Data Protection Principles

**Principle 1**

Personal data shall be processed fairly and lawfully[88] and, in particular, shall not be processed unless:

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The conditions set out in Schedules 2 and 3 of the Data Protection Act are known as the "conditions for processing". The conditions for processing are more exacting when sensitive personal data is involved, such as information about an individual's health or criminal record. In practice, it means that organisations must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure they do not do anything unlawful with the data.

Processing personal data must above all else be fair, as well as satisfying the relevant conditions for processing. If any aspect of processing is unfair, there will be a breach of the first data protection principle. Why and how personal data is collected and used will be relevant in assessing fairness. Fairness requires an organisation to:

- be open and honest about their identity;
- tell people how they intend to use any personal data they collect about them (unless this is obvious);
- usually handle their personal data only in ways they would reasonably expect; and
- above all, not use their information in ways that unjustifiably have a negative effect on them.

If processing personal data involves committing a criminal offence, the processing will obviously be unlawful. However, processing may also be unlawful if it results in:

- a breach of a duty of confidence. Such a duty may be stated, or it may be implied by the content of the information or because it was collected in circumstances where confidentiality is expected – medical or banking information, for example;
- an organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations;
- a breach of the Human Rights Act 1998. The Act implements the European Convention on Human Rights which, among other things, gives individuals the right to respect for private and family life, home and correspondence.

87 Key definitions of the Data Protection Act.
See https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ (accessed 1 June 2017).

88 Processing personal data fairly and lawfully (Principle 1);
See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/ (accessed 1 June 2017).

**Principle 2**
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes[89].

The second data protection principle means that organisations must:

- be clear from the outset about why they are collecting personal data and what they intend to do with it;
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- comply with what the Act says about notifying the Information Commissioner; and
- ensure that if they wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

Organisations need to be clear about the purpose or purposes for which they hold personal data so that they can then ensure that they process the data in a way that is compatible with their original purpose. The Act says that when deciding whether disclosing personal data is compatible with the purpose for which an organisation obtained it, they should bear in mind the purposes for which the information is intended to be used by any person to whom it is disclosed.

If an organisation wishes to use or disclose personal data for a purpose that was not contemplated at the time of collection (and therefore not specified in a privacy notice), they have to consider whether this will be fair. If using or disclosing the information would be unfair because it would be outside what the individual concerned would reasonably expect, or would have an unjustified adverse effect on them, then an organisation should regard the use or disclosure as incompatible with the purpose they obtained the information for. In practice, they often need to get prior consent to use or disclose personal data for a purpose that is additional to, or different from, the purpose they originally obtained it for.

**Principle 3[90]**
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

The Data Protection Act requires an organisation to ensure they only collect the personal data they need for the purposes they have specified. They are also required to ensure that the personal data they collect is sufficient for the purpose for which it was collected. An organisation should identify the minimum amount of personal data they need to properly fulfil their purpose. They should hold that much information, but no more. This is part of the practice known as "data minimisation". Where sensitive personal data is concerned, it is particularly important to make sure only the minimum amount of information is collected or retained.

Personal data should not be processed if it is insufficient for its intended purpose. In some circumstances, an organisation may need to collect more personal data than they had originally anticipated using, so that they have enough information for the purpose in question.

89 Processing personal data for specified purposes (Principle 2); See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-2-purposes/ (accessed 1 June 2017).

90 The amount of personal data you may hold (Principle 3); See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/ (accessed 1 June 2017).

**Principle 4**[91]

Personal data shall be accurate and, where necessary, kept up to date.

The Data Protection Act imposes obligations on organisations to ensure the accuracy of the personal data they process. It must also be kept up to date where necessary. The Act makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties. To comply with these provisions organisations should:

- take reasonable steps to ensure the accuracy of any personal data they obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

The Data Protection Act does not define the word "accurate", but it does say that personal data is inaccurate if it is incorrect or misleading as to any matter of fact. The Act says that even if an organisation is holding inaccurate personal data, they will not be considered to have breached the fourth data protection principle as long as:

- they have accurately recorded information provided by the individual concerned, or by another individual or organisation;
- they have taken reasonable steps in the circumstances to ensure the accuracy of the information; and
- if the individual has challenged the accuracy of the information, this is clear to those accessing it.

If an individual challenges the accuracy of information held about them an organisation should consider whether the information is accurate and, if it is not, they should delete, correct it, or insert a note of correction.

**Principle 5**[92]

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant. The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. In practice, it means that organisations will need to:

- review the length of time they keep personal data;
- consider the purpose or purposes they hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Personal data will need to be retained for longer in some cases than in others. How long an organisation retains different categories of personal data should be based on individual business needs. A judgement must be made about:

- the current and future value of the information;
- the costs, risks and liabilities associated with retaining the information; and
- the ease or difficulty of making sure it remains accurate and up to date.

At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly useful where many records of the same type are held.

91 Keeping personal data accurate and up to date (Principle 4); See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/ (accessed 1 June 2017).

92 Retaining personal data (Principle 5); See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/ (accessed 1 June 2017).

**Principle 6**[93]

Personal data shall be processed in accordance with the rights of data subjects under this Act. The rights of individuals that it refers to are:

1. A right of access to a copy of the information comprised in their personal data.

This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

2. A right to object to processing that is likely to cause or is causing damage or distress.

The Act refers to the "right to prevent processing". An individual has a right to object to processing only if it causes unwarranted and substantial damage or distress. If it does, they have the right to require an organisation to stop (or not to begin) the processing in question.

3. A right to prevent processing for direct marketing.

Individuals have the right to prevent their personal data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not begin) using their personal data for direct marketing.

4. A right to object to decisions being taken by automated means.

The right of subject access allows an individual access to information about the reasoning behind any decisions taken by automated means. The Act complements this provision by including rights that relate to automated decision taking. Consequently:

- an individual can give written notice requiring an organisation not to take any automated decisions using their personal data;
- even if they have not given notice, an individual should be informed when such a decision has been taken; and
- an individual can ask an organisation to reconsider a decision taken by automated means.

These rights can be seen as safeguards against the risk that a potentially damaging decision is taken without human intervention.

5. A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed.

The fourth data protection principle requires personal data to be accurate. Where it is inaccurate, the individual concerned has a right to apply to the court for an order to rectify, block, erase or destroy the inaccurate information. In addition, where an individual has suffered damage in circumstances that would result in compensation being awarded and there is a substantial risk of another breach, then the court may make a similar order in respect of the personal data in question.

6. A right to claim compensation for damages caused by a breach of the Act.

If an individual suffers damage because an organisation has breached the Act, they are entitled to claim compensation from the data controller. This right can only be enforced through the courts.

93 The rights of individuals (Principle 6); See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/ (accessed 1 June 2017).

**Principle 7**[94]

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In practice, it means organisations must have appropriate security to prevent the personal data they hold being accidentally or deliberately compromised. In particular, they will need to:

- design and organise their security to fit the nature of the personal data they hold and the harm that may result from a security breach;
- be clear about who in the organisation is responsible for ensuring information security;
- make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

**Principle 8**[95]

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. If an organisation transfers personal data outside the EEA, they are required to comply with all the principles and the Act as a whole, not just the eighth principle relating to international data transfers.

### b) The Freedom of Information Act[96]

The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways: public authorities are obliged to publish certain information about their activities and members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Public authorities include government departments, local authorities, the NHS, state schools and police forces. However, the Act does not necessarily cover every organisation that receives public money. For example, it does not cover some charities that receive grants and certain private sector organisations that perform public functions.

The Data Protection Act exists to protect people's right to privacy, whereas the Freedom of Information Act is about getting rid of unnecessary secrecy. These two aims are not necessarily incompatible but there can be a tension between them, and applying them sometimes requires careful judgement. When someone makes a request for information that includes someone else's personal data, organisations will need to carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the Data Protection Act in deciding whether they can release the information without breaching the data protection principles. This does not prevent organisations voluntarily giving information to certain people outside the provisions of the Act.

94 Information security (Principle 7); See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/ (accessed 1 June 2017).

95 Sending personal data outside the European Economic Area (Principle 8); See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/ (accessed 1 June 2017).

96 What is the Freedom of Information Act? See https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/ (accessed 1 June 2017).

The main principle behind freedom of information legislation is that people have a right to know about the activities of public authorities, unless there is a good reason for them not to. This is sometimes described as a presumption or assumption in favour of disclosure. The Act is also sometimes described as purpose and applicant blind. This means that:

- everybody has a right to access official information. Disclosure of information should be the default – in other words, information should be kept private only when there is a good reason and it is permitted by the Act;
- an applicant (requester) does not need to give an organisation a reason for wanting the information. On the contrary, organisations must justify refusing them information;
- an organisation must treat all requests for information equally, except under some circumstances relating to vexatious requests and personal data. The information someone can get under the Act should not be affected by who they are. Organisations should treat all requesters equally, whether they are journalists, local residents, public authority employees, or foreign researchers; and
- because organisations should treat all requesters equally, they should only disclose information under the Act if they would disclose it to anyone else who asked.

There are a number of tools available to the ICO for taking action to help organisations follow the Freedom of Information Act. They include non-criminal enforcement and assessments of good practice. Specifically, where authorities or public sector bodies repeatedly or seriously fail to meet the requirements of the legislation, or conform to the associated codes of practice, the ICO can take the following action:

- conduct assessments to check organisations are complying with the Act;
- serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- issue undertakings committing an authority to a particular course of action to improve its compliance;
- serve enforcement notices where there has been a breach of the Freedom of Information Act requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- issue recommendations specifying steps the organisation should take to comply;
- issue decision notices detailing the outcome of the ICO's investigation to publicly highlight particular issues with an organisation's handling of a specific request;
- prosecute those who commit criminal offences under the Act; and
- report to Parliament on freedom of information issues of concern.

The Act does not affect copyright and intellectual property rights that give owners the right to protect their original work against commercial exploitation by others. If someone wishes to re-use public sector information for commercial purposes, they should make an application under the Re-use of Public Sector Information Regulations.

### c) The Privacy and Electronic Communications Regulations (PECR)[97]

The Privacy and Electronic Communications (EC Directive) Regulations 2003 sit alongside the Data Protection Act. They implement European Directive 2002/58/EC, also known as 'the ePrivacy Directive'[98]. They give people specific privacy rights in relation to electronic communications. There are specific rules on: marketing calls, emails, texts and faxes; cookies (and similar technologies); keeping communications services secure; and customer privacy about traffic and location data, itemised billing, line identification, and directory listings.

The ICO aims to help organisations comply with PECR and promote good practice by offering advice and guidance. The ICO has several ways of taking action to change the behaviour of anyone who breaches PECR. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner can also serve a monetary penalty notice imposing a fine of up to £500,000.

### d) The Environmental Information Regulations[99]

The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities. The Regulations do this in two ways: public authorities must make environmental information available proactively; and members of the public are entitled to request environmental information from public authorities. The Regulations cover any recorded information held by public authorities in England, Wales and Northern Ireland.

The Regulations are derived from European law. They implement the European Council Directive 2003/4/CE[100] on public access to environmental information (the EC Directive) in the UK. The source of the EC Directive is an international agreement called the 'Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters'. The Regulations interact with the Infrastructure for Spatial Information in the European Community Regulations 2009 (INSPIRE).

### e) INSPIRE Regulations[101]

The INSPIRE Regulations derive from a European Directive (INSPIRE Directive 2007/2/EC)[102] create a right to discover and view spatial datasets (e.g. map data). The objective behind the Directive from the European Parliament was to establish an Infrastructure for Spatial Information in the European Community (INSPIRE). This will enable the sharing of environmental spatial information among public sector organisations and will better facilitate public access to spatial information across Europe.

The regulations apply to all public authorities in England, Wales and Northern Ireland. The Information Commissioner is responsible for regulating certain, limited, aspects of the regulations. The ICO's responsibilities under INPSIRE are intended to mirror certain aspects of this role under the Freedom of Information Act 2000 and Environmental Information Regulations 2004.

### f) Re-use of Public Sector Information Regulations (RPSI)[103]

Re-use means using public sector information, for a purpose other than the initial public task it was produced for. RPSI is intended to encourage re-use of public sector information and is about permitting re-use of information and how it is made available.

The ICO's decision making and investigatory powers in RPSI are taken from the equivalent provisions in FOIA. Where they can issue a legally binding decision notice, they also have certain other enforcement powers. They can issue an information notice to obtain information in order to deal with a complaint. If necessary, they can also issue an enforcement notice to compel the organisation to take steps to comply with RPSI.

97 What are PECR? See https://ico.org.uk/for-organisations/guide-to-pecr/introduction/what-are-pecr/ (accessed 1 June 2017).

98 EUR-Lex - 32002L0058 - EN; See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (accessed 1 June 2017).

99 What are the Environmental Information Regulations? 2017 Mar 31 ; See https://ico.org.uk/for-organisations/guide-to-the-environmental-information-regulations/what-are-the-eir/ (accessed 1 June 2017).

100 EUR-Lex - 32003L0004 - EN - EUR-Lex. See http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32003L0004 (accessed 1 June 2017).

101 Guide to the INSPIRE Regulations; See https://ico.org.uk/for-organisations/inspire-regulations/ (accessed 1 June 2017).

102 INSPIRE | Welcome to INSPIRE. See http://inspire.ec.europa.eu/ (accessed 1 June 2017).

103 Guide to RPSI; See https://ico.org.uk/for-organisations/guide-to-rpsi/ (accessed 1 June 2017).

### 4.1.2 Challenges[104]

As many areas of law are complex, "the ICO is not and cannot be expected to be expert in all of them"[105]. For example, the ICO is in charge of overseeing the Data Protection Act, which requires organisations to process personal data fairly and lawfully. However, although processing personal data in breach of copyright (for example) will involve unlawful processing, this does not mean that the ICO will pursue allegations of breach of copyright (or any other law) as this would go beyond the remit of the Data Protection Act.

Additionally, according to the ICO, some specific data governance issues that should be prioritised are[106]:

**Transparency**

It is necessary to find effective ways of explaining to 'ordinary' members of the public how their information will be used and shared. The ICO believes that transparency in the use of personal information is a desirable end in itself, but that it also acts as a catalyst for change when organisations use personal information in a way that individuals find objectionable.

**Choice**

The ICO observes that confusion can arise as to whether individuals have to be given a choice and have to agree to their data being used in a particular way. In a strict data protection sense, the law generally provides alternatives to individual consent for data usage. In the ICO's view policy makers need to be much clearer as to whether they are giving people a choice, or whether they are going to go ahead without consent – or even in the face of objection – because it is in the public interest to do so. The ICO believes that this is a confusing area for both individuals and data-holding organisations. The role of consent in data governance systems needs to be clarified.

**Communication**

The ICO believes that data-holders and data-providers should do more to explain the form in which individuals' information is made available for research or other purposes. The language around privacy and informatics can be very confusing for information professionals, let alone the general public.

**Ethics**

The ICO sees data protection – and data privacy more generally – as having a clear ethical dimension; it is about the relationship between individuals and the organisations that keep records about them. This ethical dimension is transposed into data protection law primarily through the concept of fairness. The ICO believes that individuals expect their personal data to be used in a fair and ethical way. Individuals would be more open to secondary use of their personal information if they knew more about this and had a guarantee that the information organisations hold about them will only be used in a way that is ethical and in the public interest. The ICO believes that there needs to be a clearer articulation of 'the deal' between individuals and the organisations that hold data about them.

104 Please note that sections setting out challenges to UK Data Regulation in Chapter 4 (4.1.2, 4.2.1 and 4.2.2) are by necessity drawn from a smaller number of specific sources in comparison to those set out in Chapter 3. As new legislations become embedded, challenges and issues are likely to become more widely debated and documented.

105 Processing personal data fairly and lawfully (Principle 1);
See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/ (accessed 1 June 2017).

106 ICO. Royal Society and British Academy consultation: Data governance;
See https://ico.org.uk/about-the-ico/consultations/royal-society-and-british-academy-consultation-data-governance/ (accessed 1 June 2017).

## 4.2 New Legislation:

### 4.2.1 Investigatory Powers Act 2016[107]

On Tuesday 29 November 2016, the Investigatory Powers Bill received Royal Assent and is now known as the Investigatory Powers Act 2016. It provides a new framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies. According to the Home Office, the act does 3 things:

1. Brings together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It makes these powers and the safeguards that apply to them clear and understandable.
2. Radically overhauls the way these powers are authorised and overseen. It introduces a 'double-lock' for interception warrants, so that, following Secretary of State authorisation, these (and other warrants) cannot come into force until they have been approved by a judge. And it creates a powerful new Investigatory Powers Commissioner to oversee how these powers are used.
3. Ensures powers are fit for the digital age. It makes provision for the retention of internet connection records for law enforcement to identify the communications service to which a device has connected.

**Challenges**

The Bill generated significant public debate about balancing intrusive powers and mass surveillance with the needs of the police and intelligence agencies to gain targeted access to information as part of their investigations. Although the Home Office said the bill would be compatible with the European Convention on Human Rights, the content of the draft bill has raised concerns about the impact on privacy, with privacy campaigners claiming that it would provide an international standard to authoritarian regimes around the world to justify their own intrusive surveillance powers[108].

According to the Open Rights Group[109], the law is one of the most extreme surveillance laws ever passed in a democracy. "People appear to be worried about new powers that mean our web browsing activity can be collected by internet service providers and viewed by the police and a whole range of government departments. Parliament may choose to ignore calls for a debate but this could undermine public confidence in these intrusive powers."

techUK has issued the following comment[110]: "The Bill has been strengthened in some key areas of importance to the tech sector during this parliamentary process. Judicial Commissioners will now have equal responsibility for authorising warrants, third party data retention is explicitly excluded on the face of the Bill and an overarching duty to safeguard privacy has been placed on Government and agencies. Furthermore, Government has publicly committed to using international agreements as the primary route by which UK agencies request data from overseas operators. However, there are a number of important questions that must be addressed regarding implementation of the Bill. Government needs to be more consistent on how it views the priorities of national security and cyber security alongside user privacy when implementing the Bill, set out clearly the functions and duties of the Investigatory Powers Commission and outline next steps on creating an international legal framework."

107 Investigatory Powers Act - GOV.UK. See https://www.gov.uk/government/collections/investigatory-powers-bill (accessed 1 June 2017).

108 "Snooper"s charter' bill becomes law, extending UK state surveillance. The Guardian; See http://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance (accessed 1 June 2017).

109 Jim Killock, executive director of the Open Rights Group. Report: "Digital Surveillance" | Tangled Webs. See http://www.pseudonymity.net/blog/index.php/2013/05/16/communications-data-bill-org-report/ (accessed 1 June 2017).

110 (techUK) TR. Investigatory Powers Bill Passed by Both Houses of Parliament. See http://www.techuk.org/insights/news/item/9715-investigatory-powers-bill-passed-by-both-houses-of-parliament (accessed 1 June 2017).

### 4.2.2 Digital Economy Bill[111]

The Digital Economy Bill will implement a number of government commitments on the digital economy made in the Conservative Party Manifesto. The main elements of the bill are:

- Fast broadband and support for consumers.
- New powers for Ofcom to help consumers access better information.
- New and simpler planning rules for building broadband infrastructure.
- New measures to manage radio spectrum to increase the capacity of mobile broadband.
- Further supporting digital industries equalising penalties for online copyright infringement with laws on physical copyright infringement.
- Enabling government to deliver better public services and produce world leading research and statistics.
- Enabling technology to manage information by allowing public authorities to connect where the objective has a public benefit.
- Tough safeguards of personal data, reinforcing the Data Protection Act with new offences for unlawful disclosure.
- A new statutory code of practice for direct marketing, ensuring the Information Commissioner can better enforce sanctions against nuisance callers and spammers, ensuring that consent is obtained from consumers.
- Protecting children from online pornography by requiring age verification for access to all sites and applications containing pornographic material.

**Challenges**

The Open Rights Group[112] have raised concerns over aspects of the bill. The provisions for the age verification of pornographic website users caused concern regarding the privacy of collected user data. The proposals for bulk data sharing raised concerns over the risk of misuse. The provisions regarding copyright infringements were criticised for the vagueness of the definition and the severity of the maximum sentence (10 years in prison).

BILETA, the British and Irish Law, Education and Technology Association[113], also criticised the proposal to increase maximum jail term in its submission to the Government's consultation. The proposal was described as 'unacceptable', 'unaffordable', and 'infeasible'.

The Open Data Institute, commented[114] on the lack of transparency regarding existing public sector data sharing agreements and how the bill's measures fit with them. They believe that the bill lacks the transparency needed to avoid the kind of problems that arose with NHS Digital's abandoned Care.data programme.

111 Digital Economy Bill 2016. See https://www.gov.uk/government/collections/digital-economy-bill-2016 (accessed 1 June 2017).

112 Open Rights Group: Your Rights in The Digital Age. See https://www.openrightsgroup.org/ (accessed 1 June 2017).

113 Bileta - British and Irish Law Education and Technology Association. See http://www.bileta.ac.uk/ (accessed 1 June 2017).

114 Jeni Tennison, CEO of the Open Data Institute. Digital Economy Bill lacks clarity on data sharing, experts say. ComputerWeekly. See http://www.computerweekly.com/news/450401071/Economy-Bill-lacks-clarity-on-data-sharing (accessed 1 June 2017).

The Royal Society is a self-governing Fellowship of many of the world's most distinguished scientists drawn from all areas of science, engineering, and medicine. The Society's fundamental purpose, as it has been since its foundation in 1660, is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity.

The Society's strategic priorities emphasise its commitment to the highest quality science, to curiosity-driven research, and to the development and use of science for the benefit of society. These priorities are:

- Promoting excellence in science
- Supporting international collaboration
- Demonstrating the importance of science to everyone

**For further information**
The Royal Society
6 – 9 Carlton House Terrace
London SW1Y 5AG

**T** +44 20 7451 2500
**E** science.policy@royalsociety.org
**W** royalsociety.org

Registered Charity No 207043

The British Academy is the UK's national body for the humanities and social sciences – the study of peoples, cultures and societies, past, present and future. We have three principle roles: as an independent Fellowship of world-leading scholars and researchers; a Funding Body that supports the best ideas, nationally and internationally; and a Forum for debate and engagement – a voice that champions the humanities and social sciences.

**For further information**
The British Academy
10 – 11 Carlton House Terrace
London SW1Y 5AH

**T** +44 20 7969 5200
**W** britishacademy.ac.uk

@britac_news
@TheBritishAcademy
Britacfilm
BritishAcademy

Registered Charity No 233176

Issued: June 2017 DES4735