THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SEVENTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SEVENTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Gavin Jordan

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Claire Ancell

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-485-9

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2020 Law Business Research Ltd

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

CTSU – SOCIEDADE DE ADVOGADOS

GREENBERG TRAURIG LLP

K&K ADVOCATES

nNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VUKINA & PARTNERS LTD

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 1 GLOBAL OVERVIEW 1
Alan Charles Raul

Chapter 2 EU OVERVIEW 5
William RM Long, Francesca Blythe and Alan Charles Raul

Chapter 3 APEC OVERVIEW 41
Ellyce R Cooper, Alan Charles Raul and Sheri Porath Rockwell

Chapter 4 ARGENTINA 56
Adrián Furman and Francisco Zappa

Chapter 5 AUSTRALIA 67
Michael Morris and Emily Cravigan

Chapter 6 BELGIUM 82
Steven De Schrijver and Olivier Van Fraeyenhoven

Chapter 7 BRAZIL 97
Ricardo Barretto Ferreira, Lorena Pretti Serraglio, Juliana Gebara Sene Ikeda, Isabella de Castro Satiro Aragão, Camilla Lopes Chicaroni and Beatriz Canhoto Lima

Chapter 8 CANADA 110
Shaun Brown

Chapter 9 CHINA 125
Hongquan (Samuel) Yang

Chapter 10 CROATIA 148
Sanja Vukina

Chapter 11 DENMARK 166
Tommy Angermair, Camilla Sand Fink and Søren Bonde

Chapter 12 ESTONIA 184
Risto Hübner

Chapter 13 GERMANY 195
Olga Stepanova and Julius Feldmann

Chapter 14 HONG KONG 206
Yuet Ming Tham

Chapter 15 HUNGARY 224
Tamás Gödölle and Márk Pécsvárady

Chapter 16 INDIA 236
Aditi Subramaniam and Sanuj Das

Chapter 17 INDONESIA 250
Danny Kobrata, Bhredipta Socarana and Rahma Atika

Chapter 18 JAPAN 263
Tomoki Ishiara

Chapter 19 MALAYSIA 283
Shanthi Kandiah

Chapter 20 MEXICO 300
César G Cruz Ayala, Diego Acosta Chin and Marcela Flores González

Chapter 21 NETHERLANDS 316
Herald Jongen, Nienke Bernard and Emre Yildirim

Chapter 22 PORTUGAL 330
Joana Mota Agostinho and Nuno Lima da Luz

Chapter 23 RUSSIA 344
Vyacheslav Khayryuzov

Chapter 24 SINGAPORE 354
Yuet Ming Tham

Chapter 25 SPAIN 372
Leticia López-Lapuente and Reyes Bermejo Bosch

Chapter 26 SWITZERLAND 387
Jürg Schneider, Monique Sturny and Hugh Reeves

Chapter 27 TURKEY 409
Batu Kınıkoğlu, Selen Zengin and Kaan Can Akdere

Chapter 28 UNITED KINGDOM 426
William RM Long and Francesca Blythe

Chapter 29 UNITED STATES 454
Alan Charles Raul and Snezhana Stadnik Tapia

Appendix 1 ABOUT THE AUTHORS 483
Appendix 2 CONTRIBUTORS' CONTACT DETAILS 503

Chapter 28

UNITED KINGDOM

William RM Long and Francesca Blythe[1]

I OVERVIEW

Like other countries in Europe, the United Kingdom (UK) passed legislation designed to supplement the data protection requirements of the EU General Data Protection Regulation (GDPR),[2] which came into force on 25 May 2018, repealing the EU Data Protection Directive 95/46/EC (the Data Protection Directive)[3] and which regulates the collection and processing of personal data across all sectors of the economy. The UK Data Protection Act 2018 (DPA 2018), which came into force on 23 May 2018, repealed the UK Data Protection Act 1998 (DPA 1998), introduced certain specific derogations that further specify the application of the GDPR in UK law, in addition to transposing the data protection and national security provisions of the EU Law Enforcement Directive 2016/680[4] as well as granting powers and imposing duties on the national data supervisory authority, the UK's Information Commissioner's Office (ICO). Importantly, in June 2016, the UK voted to leave the EU, leaving on 31 January 2020. Under the withdrawal agreement agreed between the UK and the EU, EU law, and in turn the GDPR, will continue to apply until the end of the implementation period (more commonly known as the 'transition period') on 31 December 2020. At the end of the transition period, the GDPR will be incorporated into UK law as the 'UK GDPR'. It will therefore be retained into domestic law but the UK will have the independence to keep the framework under review and introduce additional provisions and derogations.

1 William RM Long is a partner and Francesca Blythe is a senior associate at Sidley Austin LLP.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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).

3 European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 Directive (EU) 2016.680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

II THE YEAR IN REVIEW

The ICO has published a variety of guidance addressing compliance with the GDPR[5] and the DPA 2018 including in relation to the impact of Brexit to help organisations prepare for the end of the transition period.[6] Further details on the impact of Brexit are provided in Section VII.

Following the entry into force of the GDPR, the ICO has reported receiving large volumes of personal data breach notifications and complaints from individuals. In the 2019/2020 period, the ICO received 11,854 personal data breach notifications, down from 13,840 in the previous year.[7] Due to the impact of covid-19, the ICO has had to adapt its regulatory approach, recognising that 'organisations are facing staff and operating capacity shortages' and as a result in relation to personal data breach notifications, it will 'assess these reports, taking an appropriately empathetic and proportionate approach'.[8]

Naturally, a significant amount of the ICO's regulatory activity this year involved issuing guidance on how to comply with data protection requirements during the ongoing coronavirus covid-19 pandemic, 'Data protection and coronavirus: what you need to know', with advice on contact tracing, testing, surveillance and updates to privacy notices to incorporate new purposes of personal data processing.

III REGULATORY FRAMEWORK

i Privacy and data protection laws and regulations

Data protection in the UK is governed by the DPA 2018, which replaced the DPA 1998 on 23 May 2018. The DPA 2018 is split into six main parts: general processing, law enforcement processing, intelligence services processing, the UK data supervisory authority, the Information Commissioners Office (ICO), enforcement, and supplementary and final provisions. This chapter will focus on the general processing sections of the DPA 2018.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) Regulations 2011) (PECR) regulate direct marketing, but also the processing of location and traffic data and the use of cookies and similar technologies. The PECR implement Directive 2002/58/EC[9] (as amended by Directive 2009/136/EC) (the ePrivacy Directive). The ICO has updated its guide to PECR to take into account the GDPR.

On 10 January 2017, the European Commission issued a draft of the proposed Regulation on Privacy and Electronic Communications (the ePrivacy Regulation) to replace

5 ICO, Guide to the General Data Protection Regulation (GDPR) accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

6 ICO, Data Protection at the end of the transition period accessible at https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/.

7 ICO, Information Commissioner's Annual Report and Financial Statements 2019–2020 accessible at https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

8 ICO, Regulatory approach during coronavirus, accessible at https://ico.org.uk/media/about-the-ico/policies-and- procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf.

9 Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

the existing ePrivacy Directive.[10] The European Commission's original timetable for the ePrivacy Regulation was for it to apply in EU law and have direct effect in Member State law from 25 May 2018, coinciding with the GDPR's entry into force. However, the text is still to be adopted. On 3 June 2020, the Presidency of the Council of European Union published a progress report indicating that substantial progress on the draft ePrivacy Regulation has been limited due to the covid-19 pandemic.[11] The ePrivacy Regulation is now not expected to come into force until 2021 at the earliest. As a result, it remains to be seen whether the UK will in any case choose to introduce similar rules and obligations into domestic law since it will not come into force before the end of the transition period.

The key changes in the proposed ePrivacy Regulation will:

a require a clear affirmative action to consent to cookies;

b attempt to encourage the shifting of the burden of obtaining consent for the use of cookies to website browsers; and

c make consent for direct marketing harder to obtain and require it to meet the standard set out in the GDPR; however, existing exceptions (such as the exemption that applies where there is an existing relationship and similar products and services are being marketed) are likely to be retained.

Key terms under the DPA 2018

The terms used in the DPA 2018 have the same meaning as they have in the GDPR.[12] The key terms are:

a controller: a natural or legal person who (either alone, or jointly with others) determines the purposes and means of the processing of personal data;

b processor: a natural or legal person who processes personal data on behalf of the controller;

c data subject: an identified or identifiable individual who is the subject of personal data;

d personal data: any information relating to a identified or identifiable individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that individual;

e processing: any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; and

f special categories of data: personal data revealing the racial or ethnic origin of the data subject, his or her political opinions, his or her religious or philosophical beliefs,

10 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

11 Council of the European Union, ePrivacy Regulation Progress Report, accessible at https://data.consilium.europa.eu/doc/document/ST-8204-2020-INIT/en/pdf.

12 Section 5 of the DPA 2018.

whether the data subject is a member of a trade union, genetic data, biometric data for the purpose of uniquely identifying the data subject, data concerning the data subject's health or data concerning the data subject's sexual life or sexual orientation.

Data protection authority

The DPA 2018 and the PECR are enforced by the ICO and, the ICO has powers of enforcement in relation to organisations complying with the data protection requirements in the GDPR and PECR. The ICO also enforces and oversees the Freedom of Information Act 2000, which provides public access to information held by public authorities.

The ICO has independent status and is responsible for:

a maintaining the public register of controllers;

b promoting good practice by giving advice and guidance on data protection and working with organisations to improve the way they process data through audits, arranging advisory visits and data protection workshops;

c ruling on complaints; and

d taking regulatory actions.

IV GENERAL OBLIGATIONS FOR DATA HANDLERS

The DPA 2018 does not create additional principles and obligations in relation to general processing of personal data under the GDPR. Therefore, controllers must comply with the GDPR's data protection principles and ensuing obligations when established in the UK or processing personal data of UK data subjects.

i First data protection principle: fair, lawful and transparent processing

Personal data must be processed fairly, lawfully and in a transparent manner in relation to the data subject. This essentially means that the controller must:

a have a legitimate ground for processing the personal data;

b not use personal data in ways that have an unjustified adverse effect on the data subject concerned;

c be transparent about how the controller intends to use the personal data, and give the data subject appropriate privacy notices when collecting their personal data;

d handle a data subject's personal data only in ways they would reasonably expect and consistent with the purposes identified to the data subject; and

e make sure that nothing unlawful is done with the personal data.

The UK DPA 2018 does not introduce any further requirements in relation to the first data protection principle.

ii Legal basis to process personal data

As part of fair and lawful processing, processing of personal data must be justified by at least one of six specified grounds in Article 6 of the GDPR:

a the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c processing is necessary for compliance with a legal obligation to which the controller is subject;
d processing is necessary in order to protect the vital interests of the data subject or of another individual;
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; and
f processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The ICO guide on the GDPR contains guidance on the reliance of each Article 6 legal basis.[13] In particular, the ICO has also published detailed guidance on legitimate interests as a legal basis together with a legitimate interest assessment template[14] that covers three tests controllers should conduct as part of any legitimate interest assessment:

a the purpose test – to assess whether there is a legitimate interest behind the processing;
b the necessity test – to assess whether the processing is necessary for the purpose it has identified; and
c the balancing test – to consider the impact on data subjects' interests and rights and freedoms and to assess whether they override the controller's own legitimate interests.

The ICO's guidance on the GDPR also contains a section on consent, which makes reference to the GDPR's high standard for valid consent i.e., that consent be unambiguous, involve a clear affirmative action and provide distinct or granular options to give consent for distinct processing operations. As consent must be freely given, certain organisations in a position of power over their data subjects may find it difficult to demonstrate valid freely given consent, for example, consent obtained from employees by their employers is unlikely to be freely given as such consent is not considered freely given or a genuine choice, with employees possibly facing employment consequences as a result of failing to provide consent.

The GDPR and DPA 2018 apply a stricter regime for special categories of personal data and criminal convictions data, where such data may only be processed on the basis of additional conditions being fulfilled.[15]

iii Special categories of personal data

The GDPR distinguishes between personal data and special categories of personal data (or sensitive data). In order to lawfully process special categories of personal data, controllers must identify a legal basis under Article 6 of the GDPR and a condition under Article 9 of the GDPR. The DPA 2018 introduces additional conditions for processing special categories of personal data. Part 1 of Schedule 1 of the DPA 2018 includes the following conditions in relation to employment, health and research:

a employment, social security and social protection;
b health or social care purposes;

13 ICO, Guide to the General Data Protection Regulation (GDPR)/ Lawful basis for processing- accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

14 ICO, Sample LIA template.

15 Articles 9 and 10 of the GDPR, Sections 10 and 11 and Schedule 1 of the DPA 2018.

c public health; and
d research, etc.

Part 2 of Schedule 1 of the DPA 2018 includes 23 conditions in relation to processing necessary for reasons of substantial public interest including, for example:
a equality of opportunity or treatment;
b racial and ethnic diversity at senior levels of organisation;
c regulatory requirements relating to unlawful acts and dishonesty, etc.;
d preventing fraud;
e insurance; and
f occupational pensions.

Where processing special categories of personal data in reliance on a condition under the DPA 2018 the controller will need to have in place an 'appropriate policy document' which explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR, and explains the controller's policies as regards the retention and erasure of special categories of personal data processed in reliance on the DPA 2018 condition.

iv Criminal records personal data

Criminal records and offences data are not included within the scope of special categories of personal data. Section 11 of the DPA 2018 states that references in the GDPR to criminal records and offences data include personal data relating to the alleged commission of offences by the individual, or proceedings for an offence committed or alleged to have been committed by the individual.

In order to lawfully process criminal records and offences data, controllers must: (1) identify a legal ground under Article 6 of the GDPR; and (2) carry out the processing under the control of official authority or when the processing is authorised by EU or Member State law. Where the processing of criminal records and offences data is not carried out under the control of official authority, such processing is authorised by UK law for purposes of Article 10 only if the processing meets a condition in Parts 1, 2 or 3 of Schedule 1 of the DPA 2018.

Part 3 of Schedule 1 of the DPA 2018 sets out a number of conditions for the processing of criminal records and offences data including those that relate to:
a consent;
b protecting data subjects vital interests;
c processing by not-for-profit bodies;
d personal data in the public domain;
e legal claims;
f judicial acts;
g administration of accounts used in commission of indecency offences involving children; and
h extension of the insurance conditions in Part 2 of Schedule 1.

Part 3 also permits a controller to rely on a Part 2 condition and the requirement that the processing be in the substantial public interest can be disapplied. Where processing criminal records and offences data in reliance on a condition under the DPA 2018 the controller will need to have in place an 'appropriate policy document' as explained in Section IV(iii).

v Health Data

Data concerning health falls within scope of the special categories of personal data under Article 9 of the GDPR. The GDPR defines 'data concerning health' as 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'.

One of the lawful processing grounds for health data is Article 9(2)(j) of the GDPR where processing is necessary for scientific research purposes. To rely on this legal ground the processing must comply with Article 89(1) of the GDPR which requires that the processing be subject to appropriate safeguards which ensure technical and organisational measures are in place in particular, to comply with the principle of data minimisation.

Article 19 of the DPA 2018 states that the processing will not meet these requirements where:

a it is likely to cause substantial damage or distress to an individual; or

b the processing is carried out to support measures or decisions relating to a particular individual, unless this includes purposes of approved medical research.

The DPA 2018 includes exemptions from the data subject rights for data concerning health where:

a it is processed by a court, supplied in a report or other evidence given to a court, and under specified rules (i.e., those relating to family and children's hearings in the courts) may be withheld from an individual;[16]

b the request is made by someone with parental responsibility for a person under the age of 18 (or 16 in Scotland) and the data subject has an expectation that the information would not be disclosed to the requestor or has expressly indicated should not be disclosed.[17]

The DPA 2018 also includes an exemption from the subject access right to health data where disclosure would likely cause serious harm to the physical or mental health of the individual or another person.[18]

vi Data protection officer

The appointment of a data protection officer (DPO) in the private sector is required where an organisation's core activities (i.e., the primary business activities of an organisation), involve:[19]

a the regular and systematic monitoring of individuals on a large scale – for example, where a large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, it offers recommendations to them; or

b the large-scale processing of special categories of personal data (e.g., health data) or personal data relating to criminal convictions and offences – for example, a health insurance company processing a wide range of personal data about a large number of individuals, including medical conditions and other health information.

16 Section 3, Part 2 of Schedule 3 to the DPA.

17 Section 4, Part 2 of Schedule 3 to the DPA.

18 Section 2(2), Part 2 of Schedule 3 to the DPA.

19 Section 37(1)(b) and (c) of the GDPR.

The ICO states in its guidance on the appointment of DPOs, that regardless of whether the GDPR requires an organisation to appoint a DPO, the organisation must ensure that it has sufficient staff and resources to discharge its obligations under the GDPR and that a DPO can be seen to play a key role in an organisation's data protection governance structure and to help improve accountability. The guidance further advises that should an organisation decide that it does not need to appoint a DPO it is recommended that this decision be recorded to help demonstrate compliance with the accountability principle.

The DPO must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.[20] The data controllers and data processors who do not meet the criteria for a required appointment of a DPO may voluntarily appoint one and are required to notify the ICO of any voluntary appointment.

Required and voluntary appointments of DPOs must be notified to the ICO in the form of an email, which includes:

a the contact details of the DPO;
b the registration number of the controller or processor; and
c whether the appointment of the DPO was required or voluntary.

The ICO will publish the name of the DPO on the Data Protection Public Register, where the data controller or data processor has consented to publication.

Section 71 of the DPA 2018 requires controllers to entrust their DPO with the following non-exhaustive tasks:

a informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out the processing of personal data, of that person's obligations under the DPA 2018;
b providing advice on the carrying out of a data protection impact assessment (see below) and monitoring compliance;
c cooperating with the ICO;
d acting as the contact point for the ICO on issues relating to processing of personal data;
e monitoring compliance with the policies of the controller in relation to the protection of personal data; and
f monitoring compliance by the controller of Section 71 of the DPA 2018.

vii Registration with the ICO

Under the UK Data Protection (Charges and Information) Regulations 2018[21] (the Charges and Information Regulations), controllers are required to register with the ICO and pay a charge fee to the ICO. The cost of the fee depends on the number of employees and the turnover of the organisation. The Charges and Information Regulations have established three tiers of fees ranging from £40 to £2,900. Registering with the ICO consists of filling in an online form on the ICO website and making the payment of a fee online, which must be paid when the controller registers for the first time and then every year when the registration is renewed.

Article 30 of the GDPR requires controllers to also keep a record of their processing activities. Processors are also under an obligation to keep a record of processing activities

20 Article 37(5) of the GDPR.
21 Data Protection (Charges and Information) Regulations 2018/480.

carried out on behalf of controllers. The ICO has published template controller and processor records of processing activities. Such records will have to be provided to the ICO upon request.[22]

viii Information notices

Controllers must provide data subjects with information on how their personal data is being processed pursuant to Articles 13 and 14 of the GDPR. The list of information to be provided varies if the personal data has been obtained directly from the data subject or from a third party. The DPA 2018 introduces no further requirements in relation to the notices given to data subjects.

The ICO, in its guidance on the GDPR,[23] in particular on the data subject's right to be informed, suggests the information notice can take many forms, including:

a a layered approach: this will usually be a short notice containing key privacy information, with additional layers of more detailed information;

b dashboards: preference management tools that inform people how the controller will use their personal data and provides the option for data subjects to manage what happens with the processing of their personal data;

c just-in-time notices: relevant and focused privacy notices delivered at the time the personal data is collected;

d icons: small, meaningful symbols that highlight the existence of data processing; and

e mobile and smart device functionalities: these include pop-ups, voice alerts and mobile device gestures.

ix Data protection impact assessments (DPIA)

Controllers are under an obligation to carry out a DPIA where the processing is likely to result in a high risk to individuals. While the GDPR provides three specific examples of where a DPIA should be carried out, the ICO in its guidance on DPIAs states that it is also good practice to do a DPIA for any other major project that requires the processing of personal data. The ICO has also published a DPIA Screening Checklist that sets out:

a instances where a DPIA should always be carried out (e.g., where processing special categories of personal data or criminal offence data on a large scale, or where processing personal data without providing a privacy notice directly to the individual); and

b situations where a DPIA should be considered (e.g., where processing on a large scale, or where using innovative technological or organisational solutions).

Section 64 of the DPA 2018 requires controllers to include in their DPIA:

a a general description of the envisaged processing operations;

b an assessment of the risks to the rights and freedoms of data subjects;

c the measures envisaged to address those risks; and

d safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Section 64 of the DPA 2018, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

22 Article 30 of the GDPR.

23 ICO, Guide to the General Data Protection Regulation (GDPR)/Individual Rights/ Right to be Informed – accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

The ICO guidance also recommends that where a controller decides not to carry out a DPIA, the reasons for this decision are documented.[24]

x Second data protection principle: processing for specified, explicit and lawful purposes (purpose limitation)

Personal data can only be obtained for specified, explicit and lawful purposes, and must not be further processed in a manner that is incompatible with those purposes.

The UK DPA 2018 does not introduce any further requirements in relation to the second data protection principle.

The ICO's published guidance on GDPR includes a section on purpose limitation,[25] where it requires controllers to specify the purposes of the processing to data subjects at the outset of the processing, in the form of records of the processing activities that controllers are required to maintain and information notices that are required to be given to data subjects prior to the processing.

xi Third data protection principle: personal data must be adequate, relevant and limited to what is strictly necessary (data minimisation)

A controller must ensure that the personal data it holds is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The UK DPA 2018 does not introduce any further requirements in relation to the third data protection principle.

The ICO's published guidance on the GDPR, contains guidance on data minimisation,[26] requiring controllers to identify the minimum amount of personal data needed to fulfil its processing purposes, noting if the processing carried out does not help the controller to achieve its purposes the personal data held is most likely inadequate.

The ICO recommends controllers should carry out periodic reviews of their processing in order to check that the personal data held is still relevant and adequate for its purposes, deleting any personal data that is no longer needed.[27]

xii Fourth data protection principle: personal data must be accurate and where necessary kept up to date (accuracy)

Controllers must ensure that personal data is accurate and, where necessary, kept up to date. The ICO recommends[28] controllers take reasonable steps to ensure the accuracy of any personal data obtained, ensure that the source and status of any personal data is clear, and carefully consider any challenges to the accuracy of information and whether it is necessary to periodically update the information.

---

24 ICO, Guide to the General Data Protection Regulation (GDPR)/ Accountability and Governance- accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

25 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Purpose limitation, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

26 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Data minimisation, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

27 ibid.

28 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Accuracy, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/.

xiii Fifth data protection principle: personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary (storage limitation)

Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In practice, this means that the controller must review the length of time it keeps personal data and consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain this information. Controllers must also securely delete personal data that is no longer needed for this purpose or these purposes, and update, archive or securely delete information if it goes out of date.

It is good practice to establish standard retention periods for different categories of information (e.g., employee data and customer data). To determine the retention period for each category of information, controllers should take into account and consider any legal or regulatory requirements or professional rules that would apply.[29]

The ICO, in its published guidance on the GDPR, contains guidance on storage limitation, recommending that controllers erase or anonymise personal data[30] where they no longer need it, in order to reduce the risk of the personal data becoming excessive, irrelevant, inaccurate or out of date. This will also help controllers comply with the data minimisation and accuracy principles, while ensuring the risk that the controller uses the personal data in error is reduced.

The ICO also recommends in its GDPR storage limitation guidance[31] that it is good practice for controllers to adopt clear policies on retention periods and erasure, which can help reduce the burden of dealing with questions from data subjects about retention and access requests for the erasure of personal data.

In its GDPR guidance on individuals' rights the ICO states that if a valid erasure request is received and no exemption applies then a controller will have to take steps to ensure erasure from backup systems as well as live systems. However, the ICO acknowledges that the data will remain within the backup environment for a certain period of time until it is overwritten. According to the ICO, the key issue is to 'put the backup data "beyond use", even if it cannot be immediately overwritten'. Provided that the controller does not use the data within the backup for any other purpose, 'it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will be context specific'.

xiv Sixth data protection principle: personal data must be processed in a manner that ensures appropriate security of personal data

Personal data must be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Where a controller uses a processor to process personal data on its behalf, the controller must ensure

29 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Storage limitation, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

30 ICO, Guide to the General Data Protection Regulation (GDPR)/Principles/Storage limitation, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

31 ibid.

that it has entered into a written contract that obliges the processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing personal data.

The ICO recommends, in its published guidance on security under the GDPR,[32] that before deciding what measures are appropriate, controllers should assess the personal data risk by carrying out an information risk assessment. A controller should review the personal data it holds, and the way it is used to assess how valuable, sensitive or confidential the personal data is, including assessing any potential damage or distress that may be caused if the data is compromised.

When carrying out the assessment, the ICO recommends taking into account:

a the nature and extent of the controller's premises and computer systems;

b the number of staff the controller has;

c the extent of the staff's access to the personal data; and

d any personal data held or used by the processor acting on the controller's behalf.[33]

In addition, the ICO recommends that controllers should aim to build a culture of security awareness within the organisation, identifying a person with day-to-day responsibility for information security within the organisation and ensuring the person has the appropriate resources and authority to do their job effectively.[34]

The ICO considers encryption to be an appropriate technical measure owing to its widespread availability and relatively low cost of implementation.[35] However, there are other measures, such as pseudonymisation of data and anonymisation that can also be used to ensure the security of personal data.

The technical and organisational measures controllers have in place are also considered by the ICO when deciding whether to impose an administrative fine on the controller for the infringement of the GDPR and DPA 2018.

xv Seventh data protection principle: accountability

The data protection principle of accountability under Article 5.2 of the GDPR is prevalent throughout the GDPR and requires controllers to not only comply with the GDPR but to demonstrate their compliance with the data protection principles under GDPR.

In addition to putting in place appropriate technical and organisational measures, the ICO suggest in their GDPR accountability guidance[36] a number of measures controllers can adopt to comply with the accountability principle, including:

a adapting and implementing data protection policies;

b taking a 'data protection by design and default' approach;

c having written contracts in place with vendors processing personal data, that comply with Article 28 of the GDPR;

d maintaining records of processing activities;

32 ICO, Guide to the General Data Protection Regulation (GDPR)/Security, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

33 ibid.

34 ibid.

35 ibid.

36 ICO, Guide to the General Data Protection Regulation (GDPR)/Accountability and governance, accessible at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

e recording and, where necessary, reporting personal data breaches;
f carrying out DPIAs for uses of personal data likely to result in a high risk to the data subject's interests; and
g adhering to relevant codes of conduct and sign up to certification schemes.

The ICO notes that if controllers adopt a privacy management framework this can help embed accountability measures and create a culture of privacy across the controller's organisation.[37] The framework could include:

a robust programme controls informed by the GDPR requirements;
b appropriate reporting structures; and
c assessment and evaluation procedures.

In October 2019, the ICO published an updated draft statutory code of practice on data sharing between controllers. The draft code outlines how organisations should engage in data-sharing activities (including the requirement to have in place a data sharing agreement to help demonstrate accountability under the GDPR). The draft code also provides guidance on risk management processes, best practices and misconceptions about data sharing. At the time of writing, it is unclear when the finalised draft will be published.

V TECHNOLOGICAL INNOVATION AND PRIVACY LAW

i Anonymisation

Neither the DPA 2018 nor the GDPR apply to anonymous data. However, there has been a lot of discussion in the past over when data is anonymous and the methods that could be applied to anonymise data.

When the DPA 1998 was in force, the ICO published guidance on anonymisation[38] that recommended organisations using anonymisation have in place an effective and comprehensive governance structure that should include:

a a senior information risk owner with the technical and legal understanding to manage the process;
b staff trained to have a clear understanding of anonymisation techniques, the risks involved and the means to mitigate them;
c procedures for identifying cases where anonymisation may be problematic or difficult to achieve in practice;
d knowledge management regarding any new guidance or case law that clarifies the legal framework surrounding anonymisation;
e a joint approach with other organisations in the same sector or those doing similar work;
f use of a privacy impact assessment;

37 ibid.

38 In November 2012, the ICO published a code of practice on managing data protection risks related to anonymisation. This code provides a framework for organisations considering using anonymisation and explains what it expects from organisations using such processes.

g clear information on the organisation's approach to anonymisation, including how personal data is anonymised and the purpose of the anonymisation, the techniques used and whether the individual has a choice over the anonymisation of his or her personal data;

h a review of the consequences of the anonymisation programme; and

i a disaster-recovery procedure should re-identification take place and the individual's privacy be compromised.

The guidance has not yet been updated to take into account the entry into force of the GDPR and DPA 2018.

ii Big data and artificial intelligence

The DPA 2018 does not prohibit the use of big data analytics. The ICO issued guidance in July 2014 and revised it in August 2017[39] considering the data protection issues raised by big data. The ICO suggested how controllers can comply with the DPA 2018 and the GDPR while using big data, covering a broad range of topics including anonymisation, DPIAs, repurposing data, data minimisation, transparency and subject access. The guidance included three questions on which the ICO invited feedback. A summary of feedback was published in April 2015.[40]

In addition, the Financial Conduct Authority (FCA) published in March 2017 a feedback statement following its call for input on big data on retail general insurance.[41] The FCA's key findings were that although big data is producing a range of benefits for consumers in motor and home insurance, there are also concerns about its impact on data protection. To address some of these concerns the FCA proposed to co-host a roundtable with the ICO and various stakeholders to discuss data protection and the use of personal data in retail general insurance.

On 30 July 2020, the ICO published guidance on best practices for data protection-compliant AI, including how it interprets data protection law as it applies to AI systems that process personal data and best practice organisational and technical measures to mitigate the risks to individuals by the deployment of AI systems.[42]

iii Bring your own device

The ICO has published guidance for companies on implementing bring your own device (BYOD)[43] programmes allowing employees to connect their own devices to company IT systems. Organisations using BYOD should have a clear BYOD policy so that employees connecting their devices to the company IT systems clearly understand their responsibilities.

To address the data protection and security breach risks linked to BYOD, the ICO recommends that organisations take various measures, including:

a considering which type of corporate data can be processed on personal devices;

b how to encrypt and secure access to the corporate data;

39 ICO, Guidelines on Big Data and Data Protection, 28 July 2014 and revised 18 August 2017.

40 ICO, Summary of Feedback on Big Data and Data Protection and ICO Response, 10 April 2015.

41 FCA, FS16/5, Call for Inputs on Big Data in retail general insurance.

42 ICO, Guidance on AI and data protection, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/.

43 ICO, Guidelines on Bring Your Own Device (BYOD), 2013.

c how the corporate data should be stored on the personal devices;
d how and when the corporate data should be deleted from the personal devices; and
e how the data should be transferred from the personal device to the company servers.

Organisations should also install antivirus software on personal devices, provide technical support to the employees on their personal devices when they are used for business purposes, and have in place a 'BYOD acceptable-use policy' providing guidance to users on how they can use their own devices to process corporate data and personal data.

The guidance has not yet been updated to take into account the entry into force of the GDPR and DPA 2018.

iv Cloud computing

The ICO, like many other data protection authorities in the EU, published guidance on cloud computing, in 2012.[44]

The ICO proposes a checklist that organisations can follow prior to entering into an agreement with a cloud provider, with questions on confidentiality, integrity, availability, and other legal and data protection issues.[45]

According to the guidance, cloud customers should choose their cloud provider based on economic, legal and technical considerations. The ICO considers it is important that, at the very least, such contracts should allow cloud customers to retain sufficient control over the data to fulfil their data protection obligations.

The ICO is currently updating the cloud computing guidance to reflect the entry into force of the GDPR and DPA 2018.

v Cookies and similar technologies

Article 5(3) of the ePrivacy Directive 2002/58/EC – implemented in the UK through the PECR – requires consent for the use of non-essential cookies (e.g., audience measurement cookies) and similar technologies. As a result, organisations have an obligation to obtain the consent of website users to place non-essential cookies or similar technologies on their computers and mobile devices.[46] The consent obligation does not apply where the cookie is used 'for the sole purpose of carrying out the transmission of a communication over an electronic communication network' or is 'strictly necessary' to provide the service explicitly requested by the user. This exemption is applied restrictively and so cannot be used when using analytical cookies. Organisations must also provide users with clear and comprehensive information about the purposes for which the information, such as that collected through cookies, is used.

In July 2019, the ICO published new guidance on the use of cookies and similar technologies. In the new guidance the ICO formally recognises the stricter standards of consent and transparency now in force under the GDPR. In particular, the new guidance states that:

a consent for non-essential cookies must comply with GDPR standards, which means it must involve: (1) a clear positive action (continuing to browse the website is not

44 ICO, Guidance on the Use of Cloud Computing, 2012.
45 See the European Union Overview chapter for more details on cloud computing.
46 PECR Regulation 6.

sufficient) and not implied consent; (2) granularity (the ability to consent to cookies used for some purposes, but not others); and (3) no pre-ticked boxes or sliders set to 'on' (i.e., the default option for non-essential cookies must be off);

b the legitimate interest legal ground cannot be used as an alternative for consent to place non-essential cookies on a website;

c blanket cookie walls to restrict access to websites until a user consents to the use of cookies are unlikely to represent valid consent. The guidance confirms that statements such as 'by continuing to use this website you are agreeing to cookies' is not considered valid consent under the higher GDPR standard;

d information provided on cookies must align with the GDPR standards for transparency; and

e if an organisation's use of cookies changes significantly, users will need to be made aware of these changes to allow them to make an informed choice about the new activity.

To help address the above, the ICO recommends that organisations conduct a 'cookie audit' which will: (1) confirm the purpose(s) of each cookie; (2) confirm the type of cookie (session or persistent); (3) distinguish between those that are strictly necessary and non-essential; (4) document the findings; and (5) consider follow-up actions while building in an appropriate review period. The ICO views this as an opportunity for organisations to 'clean up' existing web pages and stop using unnecessary cookies, particularly if the website has evolved since an initial assessment was undertaken. The numbers published by the ICO on its website show a significant increase in complaints relating to cookies, rising from 327 for Q4 2018/2019 to 1,473 in Q4 2019/2020.

The new guidance confirms that enforcement action will vary, as expected, depending on the level of privacy intrusion and risk of harm posed by cookies and related technologies. The current enforcement regime for PECR remains as was in effect under the DPA 1998 (except where personal data is processed, in which case the GDPR enforcement penalties will apply). However, it is expected that this will be brought into line with the GDPR with the introduction of the ePrivacy Regulation, which will replace the ePrivacy Directive when finalised.[47]

VI SPECIFIC REGULATORY AREAS

i Minors

On 12 August 2020, the ICO issued the Age Appropriate Design Code for online services likely to be accessed and used by children under 18. The Code came into force on 2 September 2020 with a 12-month transition period. It sets out 15 standards that online services should meet to protect children's privacy including high-privacy settings by default, data minimisation and the switching off of geolocation settings by default. The Code also provides that nudge techniques should not be used to encourage children to provide unnecessary personal data, weaken or turn off their privacy settings. It also addresses issues of parental control and profiling.[48]

47 See the European Union Overview chapter for more details on the proposed ePrivacy Regulation.

48 ICO, Guide to Data Protection, Key DP Themes, Age Appropriate design: a code of practice for online services, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/#:~:text=The%20code%20is%20a%20set,designing%20and%20developing%20online%20services.

ii Employee data

There is no specific law regulating the processing of employee data. However, the ICO has published an employment practices code and supplementary guidance to help organisations comply with UK data protection laws and to adopt good practices.[49]

The code contains four parts covering:

a recruitment and selection, providing recommendations with regard to the recruitment process and pre-employment vetting;

b employment records, which is about collecting, storing, disclosing and deleting employees' records;

c monitoring at work, which covers employers' monitoring of employees' use of telephones, internet, email systems and vehicles; and

d workers' health, covering occupational health, medical testing and drug screening.

The code and supplementary guidance has not yet been updated to reflect the entry into force of the GDPR and DPA 2018.

iii Employee monitoring[50]

The DPA 2018 does not prevent employers from monitoring their employees. However, monitoring employees will usually be intrusive, and workers have legitimate expectations that they can keep their personal lives private. Workers are also entitled to a degree of privacy in their work environment.

DPIAs must be carried out when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. The EDPB's Guidance on Data Protection Impact Assessments[51] provides examples of when a DPIA should be carried out and an employee monitoring programme is identified as an example of when a DPIA should be carried out. Likewise, the ICO in its Guidance on DPIAs states that a controller should think carefully about doing a DPIA for any processing that inter alia involves monitoring, sensitive data or vulnerable individuals (e.g., employees).

Organisations should carry out a DPIA before starting to monitor their employees to clearly identify the purposes of monitoring, the benefit it is likely to deliver, the potential adverse impact of the monitoring arrangement, and to judge if monitoring is justified, as well as take into account the obligation that arises from monitoring. Organisations should also inform workers who are subject to the monitoring of the nature, extent and reasons for monitoring unless covert monitoring is justified.

Employers should also establish a policy on use by employees of electronic communications, explaining acceptable use of internet, phones and mobile devices, and the purpose and extent of electronic monitoring. It should also be outlined how the policy is enforced and the penalties for a breach of the policy.

Opening personal emails should be avoided where possible and should only occur where the reason is sufficient to justify the degree of intrusion involved.

49 ICO, The Employment Practices Code: Supplementary Guidance, November 2011.

50 ibid.

51 Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679 – Adopted on 4 April 2017 – As last Revised and Adopted on 4 October 2017.

On 8 June 2017, the former Article 29 Working Party adopted an opinion on data processing at work that also addressed employee monitoring.[52] This opinion is unlikely to fundamentally change the ICO's approach to employee monitoring in the UK. However, it does include a number of new recommendations, including that where it is possible to block websites rather than continually monitoring internet usage, employers should prefer prevention to detection.

iv Whistle-blowing hotlines

The use of whistle-blowing hotlines (where employees and other individuals can report misconduct or wrongdoing) is not prohibited by the DPA 2018 and their use is not restricted by the ICO. The ICO published guidance on the use of whistle-blowing hotlines in June 2017,[53] where it noted that employees can notify the ICO where they believe the employer has not processed their personal data in accordance with data protection legislation. The ICO has not published updated guidance on the use of whistle-blowing hotlines after the entry into force of the GDPR and DPA 2018. However, organisations using whistle-blowing hotlines in the UK will have to comply with the data-protection principles under the DPA 2018 and the GDPR.[54]

v Electronic marketing[55]

Under PECR, unsolicited electronic communications to individuals should only be sent with the recipient's consent.[56] The only exemption to this rule is known as 'soft opt-in', which will apply if the sender has obtained the individual's details in the course of a sale or negotiations for a sale of a product or service; the messages are only marketing for similar products; and the person is given a simple opportunity to refuse marketing when his or her details are collected, and if he or she does not opt out, he or she is given a simple way to do so in future messages. These UK rules on consent do not apply to marketing emails sent to companies and other corporate bodies, such as a limited liability partnership, Scottish partnership or UK government body.[57]

Senders of electronic marketing messages must provide the recipients with the sender's name and a valid contact address.[58]

The ICO has created a direct-marketing checklist, which enables organisations to check if their marketing messages comply with the law and which also proposes a guide to the different rules on marketing calls, texts, emails, faxes and mail.

52 WP 249: Opinion 2/2017 on data processing at work, adopted 8 June 2017.

53 ICO, 'Disclosures from whistleblowers', 2 June 2017.

54 For guidance on how to comply with data protection principles under the DPA see WP 117: Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime adopted on 1 February 2006.

55 ICO, Guide to the Privacy and Electronic Communications Regulations, 2013, and Direct Marketing Guidance, V.2.2.

56 PECR Regulation 22(2).

57 Guide to PECR/ Electronic and telephone marketing/ electronic mail marketing- accessible at https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/.

58 PECR Regulation 23.

In addition, the ICO has published on its website a guide on rules for businesses when marketing to other businesses under GDPR and PECR.[59] It advises that the GDPR applies to individuals who can be identified either directly or indirectly, even when they are acting in a professional capacity. It also notes the GDPR only applies to loose business cards where controllers intend to file them or input the details of the card into a computer system.

The proposed ePrivacy Regulation, which is still under review and will not come into force before 2021 at the earliest, will not have direct effect in the UK. It remains to be seen whether similar rules and obligations will be introduced in the UK under domestic law and any updates to PECR.

In January 2020, the ICO published a draft Direct Marketing Code of Practice (Draft Code) for public consultation. The Draft Code is intended to update existing guidance published pre-GDPR and provide clarity on certain important issues. The key takeaways from the Draft Code are as follows: consent is not required under the PECR where an organisation sends service or operational messages to individuals (e.g., a message informing a user they are approaching their monthly data limit); where an organisation partners with a third party to deliver electronic communications, both parties will need to comply with PECR irrespective of who has access to the data used; the two lawful bases for direct marketing under the GDPR are consent and legitimate interests. However, the Draft Code confirms that if consent is required under PECR, it will also be the relevant legal basis under the GDPR. The Draft Code also provides that 'tell a friend schemes' are in breach of PECR because it is impossible for the organisation to obtain valid consent from the 'friend', in other words, the organisation does not have a direct relationship with the 'friend'.

vi Financial services

Financial services organisations, in addition to data protection requirements under the DPA 2018, also have legal and regulatory responsibilities to safeguard consumer data under rules of the UK Financial Conduct Authority (FCA), which includes having adequate systems and controls in place to discharge their responsibilities.

This includes financial services firms taking reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime, such as by misuse of customer data.[60]

Failure to comply with these security requirements may lead to the imposition of significant financial penalties by the FCA.

VII INTERNATIONAL TRANSFERS

The GDPR prohibits the transfer of personal data outside of the EEA to third countries (non-EEA Member State) unless:

a the recipient country is considered to offer an adequate level of data protection; or

b a data protection safeguard has been applied (such as the EU's standard contractual clauses (SCCs) for transfers of personal data from the EU also known as 'model contracts' or the organisation has implemented binding corporate rules); or

59 ICO, For organisations/Marketing/The rules around business to business marketing, the GDPR and PECR, accessible at https://ico.org.uk/for-organisations/marketing/the-rules-around-business-to-business-marketing-the-gdpr-and-pecr/.

60 SYSC 3.

c a derogation from the prohibition applies (such as the data subject has explicitly consented to the transfer).

This chapter does not consider the data protection safeguards and derogations in detail, which are set out in the EU chapter. However, it should be noted that under the DPA 1998, controllers were allowed to determine for themselves that their transfers of personal data outside of the EEA were adequately protected. The DPA 2018 does not contain such a self-adequacy assessment. However, under the recent ruling by the Court of Justice of European Union (CJEU), which invalidated the EU–US Privacy Shield as a mechanism to legitimise the transfer of personal data from the EEA/UK to the United States, the CJEU held that it is the responsibility of the data exporter and data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by SCCs (and Binding Corporate Rules) can be complied with in practice. If this is not the case then an assessment should be carried out on whether supplementary measures can be provided to ensure an essentially equivalent level of protection. In addition, the GDPR contains a more limited version of the DPA 1998 self-adequacy assessment, and allows transfers:

a that are not repetitive, concern only a limited number of data subjects and are necessary for the purposes of compelling legitimate interests that are not overridden by the interests or rights and freedoms of the data subject;
b where the controller has assessed all the circumstances surrounding the data transfer and has, as a result, implemented suitable data protection safeguards; and
c has notified the relevant data protection authority of the transfer.

The DPA 2018 also introduces a derogation where the transfer is a necessary and proportionate measure for the purposes of the controller's statutory function.

In addition, the DPA 2018 also introduces further derogations for the transfer of personal data from the UK to a country outside of the EEA where the transfer is necessary for law enforcement purposes and is based on an adequacy decision.

If it is not based on an adequacy decision, it must be based on appropriate safeguards where a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the personal data, or the data controller having assessed all the circumstances surrounding the transfers of that type of personal data to that specific country or territory outside of the EEA concludes that appropriate safeguards exist to protect the personal data. When relying on this particular derogation, the transfer must also be documented and such documents must be provided to the ICO upon request, including the date and time of the transfer, the name or any other pertinent information about the recipient, the justification for the transfer of the personal data; and a description of the personal data transferred.

If it is not based on an adequacy decision or on there being appropriate safeguards, it must be based on special circumstances that allow for the transfer of personal data from the UK to a country or territory outside of the EEA, where the transfer is necessary:

a to protect the vital interests of the data subject or another person;
b to safeguard the legitimate interests of the data subject;
c for the protection of an immediate and serious threat to the public security of a Member State or a third country;

d in individual cases for any law enforcement purposes, (provided the controller has not determined that fundamental rights and freedoms of the data subject override the public interest in the transfer of personal data from the UK to a third country); or

e in individual cases for a legal purpose (provided the controller has not determined that fundamental rights and freedoms of the data subject override the public interest in the transfer of personal data from the UK to a third country). When relying on this particular derogation, the transfer must also be documented and such documents must be provided to the ICO upon request, including the date and time of the transfer, the name or any other pertinent information about the recipient, the justification for the transfer of the personal data, and a description of the personal data transferred.

Brexit will have fundamental implications for data protection and the ongoing flow of personal data from the EU to the UK, and vice versa. On 31 December 2020, at the end of the transition period, transfers from the EU to the UK will be restricted. Until the end of the Transition Period, data transfers between the EU and the UK can continue unrestricted. At the end of the transition period, companies will have to put in place a valid data transfer solution to legitimise their transfers of personal data from the EU to the UK (e.g., EU standard contractual clauses).

VIII DISCOVERY AND DISCLOSURE

The ICO has not published any specific guidance on this topic.[61] E-discovery procedures and the disclosure of information to foreign enforcement agencies will, most of the time, involve the processing of personal data. As a result, organisations will have to comply with the data protection principles under the DPA 2018 in relation to e-discovery and must comply with the requirements of the GDPR.

In practice, this will mean informing data subjects about the processing of their personal data for this purpose. Organisations will also have to have a legal basis for processing the data.

A data transfer solution will also have to be implemented if the data is sent to a country outside the EEA that is not deemed to provide an adequate level of protection pursuant to Article 45 of the GDPR.

IX PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The ICO has a range of enforcement powers under the DPA 2018, including monitoring and enforcement of the GDPR and the DPA 2018 in the UK. Such monitoring and enforcement powers include the power to issue:

a information notices: requiring controllers and processors to provide the ICO with information that the Commissioner reasonably requires in order to assess compliance with the GDPR or DPA 2018;

b assessment notices: requiring the controller or processor to permit the ICO to carry out an assessment of whether the controller or processor is in compliance with the

61 The Article 29 Working Party has, however, published a working document on this topic. See the European Union Overview chapter for more details.

GDPR or DPA 2018 (this may include the power of the ICO to conduct an audit, where the assessment notice permits the ICO to enter specified premises, inspect or examine documents, information, material and observe processing of personal data on the premises);

c notice of intent: where, after conducting its investigation, the ICO issues a notice of intent to fine the controller or processor in relation to a breach of the GDPR or the DPA 2018. Such a notice sets out the ICO's areas of concern with respect to potential non-compliance of the GDPR or the DPA 2018 and grants the controller or processor the right to make representations. After such representations have been carefully considered, the ICO reaches its final decision on any enforcement action in the form of an enforcement notice;

d enforcement notices: such notices are issued where the ICO has concluded the controller or processor has failed to comply with the GDPR or the UK DPA 2018, setting out the consequences of non-compliance, which could include a potential ban on processing all or certain categories of personal data; and

e penalty notices: if the ICO is satisfied that the controller or processor has failed to comply with the GDPR or the DPA 2018 or has failed to comply with an information notice, an assessment notice or an enforcement notice, the ICO may, by written notice, require a monetary penalty to be paid for failing to comply with the GDPR or the DPA 2018. Under the GDPR, such monetary penalties can amount to €20 million or 4 per cent of annual worldwide turnover.

As the DPA 2018 came into effect on 23 May 2018, any information notices issued by the ICO to commence possible investigations, assessment notices or enforcement notices served pre-23 May 2018 and thus served under the DPA 1998, continue to have effect under the DPA 2018.

In a speech at the Data Protection Practitioners' Conference on 9 April 2018, the Information Commissioner, Elizabeth Dunham, stated that 'enforcement is a last resort' and that 'hefty fines will be reserved for those organisations that persistently, deliberately or negligently flout the law' and 'those organisations that self-report, engage with us to resolve issues and can demonstrate effective accountability arrangements can expect this to be a factor when we consider any regulatory action'.

In addition, the ICO is responsible for promoting public awareness and in particular raising awareness among controllers and processors, of their obligations under the GDPR and DPA 2018.

The FCA also has enforcement powers and can impose financial penalties on financial services organisations for failure to comply with their obligations to protect customer data.

ii Recent ICO-led enforcement cases

Following the entry into force of the GDPR, the ICO has taken the following high-profile enforcement actions:

a in October 2018, issuing an enforcement action against a Canadian data analytics firm in relation to its political campaign behavioural advertising techniques;

b on 8 July 2019, the ICO issued a notice of its intention to fine British Airways (BA) £183.39 million for infringements of the GDPR. The proposed fine relates to a

cyber-incident that BA notified to the ICO (as BA's lead data protection authority) in September 2018. The incident involved the theft from the BA website and mobile app of personal data pertaining to customers over a two-week period; and

c on 9 July 2019, the ICO issued another statement of its intention to fine Marriott International, Inc over £99 million in relation to a security incident affecting the Starwood reservation database that Marriott had acquired in 2016 and discovered in November 2018. The statement came in response to Marriott's filing with the US Securities and Exchange Commission that the ICO intended to fine it for breaches of the GDPR. The UK Information Commissioner confirmed in a statement that 'organisations must be accountable for the personal data they hold and this includes carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but how it is protected.'

Both BA and Marriott had the opportunity to make detailed representations to the ICO as to the proposed findings and sanctions. In early 2020, the ICO issued a statement delaying the issuance of both GDPR fines, which had originally been expected by the end of 2019. It is understood that the delay was agreed between both parties and the ICO respectively in accordance with Schedule 16 of the UK Data Protection Act 2018, which provides that the ICO must give a penalty notice to a person in reliance on a notice of intent within six months of that notice of intent, unless that period is extended by agreement between the ICO and that person. In light of covid-19, the notice of intent to fine in both instances has been extended, and is expected to be announced in late 2020.

iii Private enforcement

Under the GDPR, data subjects are able to claim for 'material or non-material damage' as a result of a breach of the GDPR. In addition, not-for-profit organisations have the right to lodge a complaint on behalf of the data subject. For example, BA is currently involved in group litigation before the UK High Court against over 50,000 BA customers who are seeking damages as a result of the personal data breach. BA had already pledged to cover any losses suffered by its customers, but public estimates of expected compensation to affected individuals vary, ranging from £2,200 to £6,000 each.

In addition, in a recent case in the UK relates to a former employee who copied payroll data of 100,000 employees onto an external drive and subsequently posted the data on a file sharing website. The individual was jailed for eight years under the UK's Computer Misuse Act. The employer was found by the court of first instance and the Court of Appeal to be vicariously liable to approximately 5,000 employees who joined the group litigation for breach of confidence and UK data protection laws because it was held that there was a sufficient connection between the employer having authorised the tasks of the former employee (i.e., he was entrusted with the payroll data) and the wrongful acts committed by him. On 1 April 2020, the UK Supreme Court reversed the ruling, holding that the employer was not vicariously liable for a data breach committed maliciously by a former employee who, acting to satisfy a personal vendetta against the employer, had disclosed employee payroll

data online, as the wrongful conduct was not so closely connected with acts that he was authorised to do by his employer that it could be fairly regarded as carried out by him during his ordinary course of employment.[62]

Further, on 19 August 2020, Martin Bryant, a technology journalist, announced he had filed a data breach representative action in the High Court of England and Wales against Marriott following its data breach, seeking compensation of the loss of control over his personal data as well as on behalf of other claimants.

X CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPA 2018 applies to a controller established in the UK and processing personal data in the context of that establishment, regardless of whether the processing takes place in the UK. It also applies to foreign organisations not established in the UK, or in any other EEA state, that process personal data in relation to the offering of goods or services to data subjects in the UK or to the monitoring of data subjects in the UK, as far as their behaviour takes place in the UK. Controllers not established in the UK or any other EEA country and processing personal data of data subjects in the UK must nominate a representative established in the UK and comply with the data principles and requirements under the GDPR and DPA 2018.

XI CYBERSECURITY AND DATA BREACHES

i Cybersecurity

Investigatory Powers Act 2016 (the Investigatory Powers Act)

The Investigatory Powers Act (IPA) received Royal Assent on 29 November 2016. The Act prohibits the interception of communications without lawful authority and sets out the situations in which there is lawful authority. Various law enforcement and intelligence authorities can, under the IPA, make targeted demands on telecommunications operators.

Under the IPA, the Secretary of State may by giving notice require a public telecommunications operator to retain communications data for a period that must not exceed 12 months if he or she considers that this is necessary and proportionate for one or more of the purposes for which communications may be obtained under the IPA. The IPA also expands the data retention requirements in the DRIP Act that it replaces (see below) to a broader range of communications data, such as site browsing histories.

The IPA is controversial and like its predecessor, the DRIP Act, which was an emergency piece of legislation and automatically expired on 31 December 2016, it has been criticised for lacking basic safeguards and for granting overly expansive powers for the bulk collection of data. The legality of the IPA has already been called into question following a ruling of the CJEU on the data retention provisions in the DRIP Act. One year after receiving Royal Assent, the English High Court issued a landmark judgment declaring the DRIP Act unlawful. The High Court ruled that a number of the provisions in the DRIP Act were incompatible with EU human rights law. However, the ruling was suspended until 31 March 2016 to give UK legislators time to implement appropriate safeguards. Preliminary questions were referred to the CJEU by the English Court of Appeal. On 21 December 2016, the CJEU issued a landmark ruling that effectively upheld an original decision of the High

62 *WM Morrison Supermarkets PLC v. Various Claimants* [2020] UKSC 12.

Court in relation to the validity of the provisions of the DRIP Act.[63] Although the ruling concerned the DRIP Act, the IPA does little to address the criticisms of the DRIP Act in the CJEU's judgment and in some cases provides for even more extensive powers than under the DRIP Act. The case was returned to the Court of Appeal, who in January 2018, issued its judgment, ruling the DRIP Act was incompatible with EU law as the DRIP Act did not restrict the accessing of communications data to 'investigations of serious crime' nor did requests by police or other public bodies to access communications data meet independent oversight by way of a 'prior review by a court or independent administrative authority'. The UK government responded that it was making amendments to the IPA to take into account judicial criticisms of the DRIP Act. The UK High Court ruled in April 2018 that the UK government had six months to introduce changes to the IPA to make it compatible with UK law. On 31 October 2018 the Data Retention and Acquisition Regulations 2018 came into force to address the UK High Court's ruling.

The Regulation of Investigatory Powers Act 2000 (RIPA)

The interception powers in Part 1, Chapter 1 of RIPA have been repealed and replaced by a new targeted interception power under the IPA.

UK cybersecurity strategy

In November 2011, the Cabinet Office published the UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, with four objectives for the government to achieve by 2015:

a tackling cybercrime and making the UK one of the most secure places in the world to do business;

b to be more resilient to cyberattacks and better able to protect our interests in cyberspace;

c to create an open, stable and vibrant cyberspace that the UK public can use safely and that supports open societies; and

d to have the cross-cutting knowledge, skills and capability it needs to underpin all our cybersecurity objectives.

In March 2013, the government launched the Cyber-security Information Sharing Partnership to facilitate the sharing of intelligence and information on cybersecurity threats between the government and industry.

The government has also developed the Cyber Essentials scheme, which aims to provide clarity on good cybersecurity practice.

Along with the Cyber Essentials scheme, the government has published the Assurance Framework, which enables organisations to obtain certifications to reassure customers, investors, insurers and others that they have taken the appropriate cybersecurity precautions. The voluntary scheme is currently open and available to all types of organisation.

In June 2015, the government launched a new online cybersecurity training course to help the procurement profession stay safe online.

63 Case C-698/15 *Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis.*

In July 2015, the government announced the launch of a new voucher scheme to protect small businesses from cyberattacks, which will offer micro, small and medium-sized businesses up to £5,000 for specialist advice to boost their cybersecurity and protect new business ideas and intellectual property.

In January 2016, the government announced plans to assist start-ups offering cybersecurity solutions. Such start-ups will be given help, advice and support through the Early State Accelerator Programme, a £250,000 programme designed to assist start-ups in developing their products and bringing them to market. The programme is run by Cyber London and the Centre for Secure Information Technologies, and is funded by the government's National Cyber Security Strategy programme.

In March 2016, the government announced that the UK's new national cyber centre (announced in November 2015) would be called the National Cyber Security Centre (NCSC). The NCSC, which is based in London, opened in October 2016 and is intended to help tackle cybercrime.

In response to the European Parliament's proposal for a NIS Directive in March 2014, which was part of the European Union's Cybersecurity Strategy, and proposed certain measures including new requirements for 'operators of essential services' and 'digital service providers', the UK government has implemented the NIS Directive into national law in the form of the UK Network and Information Systems Regulations 2018 (the NIS Regulations), which came into force on 10 May 2018.

The NIS Regulations have established a legal framework that imposes security and notification of security incident obligations on:

a operators of essential services, being energy, transport, digital infrastructure, the health sector and drinking water supply and distribution services; and

b on relevant digital service providers, being online marketplace providers, online search engines and cloud computing service providers.

The NIS Regulations also require the UK government to outline and publish a strategy to provide strategic objectives and priorities on the security of the network and information systems in the UK.

The NIS Regulations also impose a tiered system of fines in proportion to the impact of the security incident, with a maximum fine of £17 million imposed where a competent authority decides the incident has caused or could cause an immediate threat to life or a significantly adverse impact on the UK economy.

Controllers in the UK may in the event of a data security breach have to notify the relevant authorities both under the GDPR and the NIS Regulations.

Data breaches

Under the GDPR controllers are required to report personal data breaches to the ICO without undue delay, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject. and, where feasible, no later than 72 hours after the controller becomes aware of the breach.[64] If a controller does not report the data breach within 72 hours, it must provide a reasoned justification for the delay in notifying the ICO. The controller is also subject to a concurrent obligation to notify affected data subjects without undue delay when the

64 Article 33(1) of the GDPR.

notification is likely to result in a high risk to the rights and freedoms of natural persons.[65] Under the GDPR, processors also have an obligation to notify the controller of personal data breaches without undue delay after becoming aware of a personal data breach.[66]

According to the ICO, there should be a presumption to report a breach to the ICO if a significant volume of personal data is concerned and also where smaller amounts of personal data are involved but there is still a significant risk of individuals suffering substantial harm.[67] The ICO have stated the 72-hour deadline to report a personal data breach includes evenings, weekends and bank holidays[68] and where a controller is not able to report a breach within the 72-hour deadline, it must give reasons to the ICO for its delay.

As part of the notification, the ICO requires controllers to inform the ICO of:

a the number of data subjects affected by the personal data breach;

b the type of personal data that has been affected;

c the likely impact on the data subjects as a result of the personal data breach;

d steps the controller has taken to rectify the personal data breach and to ensure it does not happen again; and

e the name of the DPO or another point of contact for the ICO to request further information.

The GDPR also imposes a requirement on controllers to inform the data subject where the personal data breach represents a high risk to their rights and freedoms. The ICO, in a webinar in July 2018,[69] stated it was of the view that the threshold is higher for informing data subjects of the personal data breach than it is for informing the ICO of the personal data breach. According to the ICO, this is because the aim of informing data subjects is so that they can take action to protect themselves in the event of a personal data breach. Therefore, informing them of every personal data breach, regardless of whether it has an effect on the data subject, can lead to notification fatigue, where the consequences of the breach are relatively minor.

In addition, when notification is given to the ICO of the personal data breach, the ICO can also require the controller to inform the data subjects of the personal data breach.

In addition, under the PECR[70] and the Notification Regulation,[71] internet and telecommunication service providers must report breaches to the ICO no later than 24 hours after the detection of a personal data breach where feasible.[72] The ICO has published guidance on this specific obligation to report breaches.[73]

65 Article 34 of the Regulation.

66 Article 33(2) of the Regulation.

67 ICO, Guidance on Notification of Data Security Breaches to the Information Commissioner's Office, 27 July 2012.

68 ICO, Personal Data Breach Reporting Webinar, 19 July 2018.

69 ibid.

70 PECR Regulation 5A(2).

71 Commission Regulation No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (the Notification Regulation), which entered into force on 25 August 2013.

72 Article 2 of the Notification Regulation. The content of the notification is detailed in Annex 1 to the Notification Regulation.

73 ICO, Guidance on Notification of PECR Security Breaches, 26 September 2013.

XII OUTLOOK

In light of the upcoming end to the transition period, negotiations on a UK adequacy decision are expected to continue between the UK government and the European Commission, with the UK government expected to set out further guidance on the UK's data protection framework post-Brexit.

More generally, it is expected the ICO will continue to publish guidance on the DPA 2018 and the impact of Brexit on data protection during 2020 and beyond. We also expect a resurgence in enforcement action from the ICO in the coming months, as well as a steep increase in consumers exercising their privacy rights and a continued growth in privacy litigation.

Appendix 1

ABOUT THE AUTHORS

WILLIAM RM LONG

Sidley Austin LLP

William Long is a global co-leader of Sidley's highly ranked privacy and cybersecurity practice and also leads the EU data protection practice at Sidley. William advises international clients on a wide variety of GDPR, data protection, privacy, information security, social media, e-commerce and other regulatory matters. William has been a member of the European Advisory Board of the International Association of Privacy Professionals (IAPP) and on the DataGuidance panel of data protection lawyers. He is also on the editorial board of *e-Health Law & Policy* and also assists with dplegal ('data privacy legal'), a networking group of in-house lawyers in life sciences companies examining international data protection issues. William was previously in-house counsel to one of the world's largest international financial services groups. He has been a member of a number of working groups in London and Europe looking at the EU regulation of e-commerce and data protection and spent a year at the UK's Financial Law Panel (established by the Bank of England), as assistant to the chief executive working on regulatory issues with online financial services.

FRANCESCA BLYTHE

Sidley Austin LLP

Francesca Blythe is a senior associate in the London office at Sidley Austin LLP, whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

SIDLEY AUSTIN LLP

70 St Mary Axe
London EC3A 8BE
United Kingdom
Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
wlong@sidley.com
fblythe@sidley.com
www.sidley.com

an LBR business

ISBN 978-1-83862-485-9