THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SIXTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Sixth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2019
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
Tommy Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Charlotte Stretch

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC2A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-062-2

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

© 2019 Law Business Research Ltd

ACKNOWLEDGEMENTS

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

ALLENS

ANJIE LAW FIRM

ASTREA

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

KOBYLAŃSKA LEWOSZEWSKI MEDNIS SP. J.

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

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, Géraldine Scali, Francesca Blythe and Alan Charles Raul

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

Chapter 4 ARGENTINA 54
Adrián Furman and Francisco Zappa

Chapter 5 AUSTRALIA 66
Michael Morris

Chapter 6 BELGIUM 79
Steven De Schrijver and Olivier Van Fraeyenhoven

Chapter 7 CANADA 99
Shaun Brown

Chapter 8 CHINA 115
Hongquan (Samuel) Yang

Chapter 9 COLOMBIA 135
Natalia Barrera Silva

Chapter 10 CROATIA 145
Sanja Vukina

Chapter 11 DENMARK 162
Tommy Angermair, Camilla Sand Fink and Søren Bonde

Chapter 12 GERMANY....180
Olga Stepanova and Florian Groothuis

Chapter 13 HONG KONG....189
Yuet Ming Tham

Chapter 14 HUNGARY....206
Tamás Gödölle

Chapter 15 INDIA....218
Aditi Subramaniam and Sanuj Das

Chapter 16 JAPAN....233
Tomoki Ishiara

Chapter 17 MALAYSIA....251
Shanthi Kandiah

Chapter 18 MEXICO....266
César G Cruz Ayala, Diego Acosta Chin and Marcela Flores González

Chapter 19 POLAND....282
Anna Kobylańska, Marcin Lewoszewski, Aleksandra Czarnecka and Karolina Gałęzowska

Chapter 20 RUSSIA....296
Vyacheslav Khayryuzov

Chapter 21 SINGAPORE....306
Yuet Ming Tham

Chapter 22 SPAIN....323
Leticia López-Lapuente and Reyes Bermejo Bosch

Chapter 23 SWITZERLAND....338
Jürg Schneider, Monique Sturny and Hugh Reeves

Chapter 24 TURKEY....360
Batu Kınıkoğlu, Selen Zengin and Kaan Can Akdere

Chapter 25 UNITED KINGDOM 373
William RM Long, Géraldine Scali and Francesca Blythe

Chapter 26 UNITED STATES 399
Alan Charles Raul, Christopher C Fonzone, and Snezhana Stadnik Tapia

Appendix 1 ABOUT THE AUTHORS 423
Appendix 2 CONTRIBUTORS' CONTACT DETAILS 439

Chapter 2

EU OVERVIEW

William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul[1]

I OVERVIEW

In the EU, data protection is principally governed by the EU General Data Protection Regulation (GDPR),[2] which came into force on 25 May 2018 and is applicable in all EU Member States. The GDPR repealed the Data Protection Directive 95/46/EC (Directive),[3] regulates the collection and processing of personal data across all sectors of the EU economy and introduced new data protection obligations for controllers and processors alongside new rights for EU individuals.

The GDPR created a single EU-wide law on data protection and has empowered Member State data supervisory authorities (DSAs) with significant enforcement powers, including the power to impose fines of up to 4 per cent of annual worldwide turnover or €20 million, whichever is greater, on organisations for failure to comply with the data protection obligations contained in the GDPR.

In March 2019, the European Data Protection Board's (EDPB) published its first overview on the implementation of the GDPR. The overview provided statistics on the consistency mechanism, the cooperation mechanism and enforcement under the GDPR. In particular, as at the time of publication the total number of cases reported by DSAs from 31 EEA countries totalled 206,326 with 94,622 of these constituting complaints and 64,684 initiated as a data breach notification. In addition, DSAs from 11 EEA countries reported imposing administrative fines under the GDPR totalling €55,955,871. In May 2019, the European Data Protection Board's (EDPB) published further statistics noting that DSAs had logged over 144,000 queries and complaints, and over 89,000 data breaches.

Set out in this chapter is a summary of the main provisions of the GDPR. We then cover guidance provided by the EU's former Article 29 Working Party (which has, since 25 May 2018, been replaced by the EDPB) on the topical issues of cloud computing and whistle-blowing hotlines. We conclude by considering the EU's Network and Information Security Directive (the NIS Directive).

---

1 William RM Long and Alan Charles Raul are partners, Géraldine Scali is a counsel 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.

II THE GDPR

The GDPR imposes a number of obligations on organisations processing the personal data of individuals (data subjects). The GDPR also provides several rights to data subjects in relation to the processing of their personal data.

Failure to comply with the GDPR and Member State data protection laws enacted to supplement the data protection requirements of the GDPR can amount to a criminal offence and can result in significant fines and civil claims from data subjects who have suffered as a result.

Although the GDPR sets out harmonised data protection standards and principles, the GDPR grants EU Member States the power to maintain or introduce national provisions to further specify the application of the GDPR in Member State law.

i The scope of the GDPR

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing of personal data that forms part of a filing system or is intended to form part of a filing system other than by automated means. The GDPR does not apply to the processing of personal data by an individual in the course of a purely personal or household activity.

The GDPR only applies when the processing is carried out in the context of an establishment of the controller or processor in the EU, or, where the controller or processor does not have an establishment in the EU, but processes personal data in relation to the offering of goods or services to individuals in the EU; or the monitoring of the behaviour of individuals in the EU as far as their behaviour takes place within the EU.

This means that many non-EU companies that have EU customers will need to comply with the data protection requirements in the GDPR.[4]

The EDPB published its draft guidance on the territorial application of the GDPR in November 2018 that was subject to public consultation until January 2019. The draft guidance largely reaffirms prior interpretations but it does leave some legal uncertainty for non-EU organisations including on how to deal with the GDPR's international data transfer restrictions. It is hoped that these concerns will be addressed once the finalised guidance is published.

There are a number of important terms used in the GDPR,[5] including:

a controller: any natural or legal person who alone or jointly with others, determines the purpose and means of processing personal data. Interestingly, a recent decision from the CJEU (decided under the former Directive) considered the question of joint controllership. In particular, the CJEU held that for there to be a relationship of joint control, the parties do not need to share responsibility equally, nor do they have to have access to the personal data processed. Unfortunately the ruling does not address the question of liability between the parties;

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 the personal data;

4 Article 3(2) of the GDPR.

5 Article 4 of the GDPR.

d establishment: the effective and real exercise of activity through stable arrangements in a Member State;[6]

e filing system: any structured set of personal data that is accessible according to specific criteria, whether centralised or decentralised or dispersed on a functional or geographical basis, such as a filing cabinet containing employee files organised according to their date of joining or their names or location;

f personal data: any information that relates to an identified or identifiable individual who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. In practice, this is a broad definition including anything from someone's name, address or national insurance number to information about their taste in clothes. Additionally, personal data that has undergone pseudonymisation, where the personal data has been through a process of de-identification so that a coded reference or pseudonym is attached to a record to allow the data to be associated to a particular data subject without the data subject being identified, is considered personal data under the GDPR; and

g processing: any operation or set of operations performed upon 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. This definition is so broad that it covers practically any activity in relation to personal data.

ii Obligations of controllers and processors under the GDPR

Notification

The notification obligation under the Directive requiring controllers to notify their national DSA prior to carrying out any processing of personal data no longer exists under the GDPR. Instead, DSAs may introduce their own notification requirements. For example, the UK's DSA, the Information Commissioners Office (ICO), requires controllers to register on a public register maintained by the ICO, in addition to paying a fee to the ICO ranging from £40 to £2,400 depending on the type of organisation the controller is.

Importantly, instead of the notification obligation, Article 30 of the GDPR requires controllers (and processors) to maintain a record of their processing activities. For controllers, this record should include the purpose of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries (non-EEA Member States); identifying the third country if there are transfers of personal data to a third country; envisaged time limits for the retention of the different categories of personal data; and a general description of the technical and organisational security measures in place to protect the personal data.

6 Recital 22 of the GDPR.

Data protection principles and accountability

Generally, the GDPR requires controllers to comply with the following data protection principles when processing personal data:

a the lawfulness, fairness and transparency principle:[7] personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;

b the purpose limitation principle:[8] personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c data minimisation principle:[9] personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d accuracy principle:[10] personal data must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are erased or rectified without delay;

e storage limitation principle:[11] personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f integrity and confidentiality: personal data must be processed in a manner that ensures appropriate security of personal data as described below; and

g accountability: the GDPR's principle of accountability under Article 5(2) of the GDPR is a central focus of the data protection requirements in the GDPR and requires controllers to process personal data in accordance with data protection principles found in the GDPR. Article 24 of the GDPR further provides that controllers implement appropriate technical and organisational measures to ensure and to be able to demonstrate that data processing is performed in accordance with the GDPR.

Data protection impact assessments (DPIA)

Article 35(1) of the GDPR imposes an obligation on controllers to conduct a DPIA prior to the processing of personal data, when using new technologies and where the processing is likely to result in a high risk to the rights and freedoms of data subjects. This may be relevant to certain activities of the controller such as, where it decides to carry out extensive monitoring of its employees. The controller is required to carry out a DPIA, which assesses the impact of the envisaged processing on the personal data of the data subject, taking into account the nature, scope, context and purposes of the processing.

Article 35(3) of the GDPR provides that a DPIA must be conducted where the controller engages in:

a a systematic and extensive evaluation of personal aspects relating to data subjects which is based on automated processing, including profiling, and produces legal effects concerning the data subject or similarly significantly affecting the data subject; or

7 Article 5(1)(a) of the GDPR.

8 Article 5(1)(b) of the GDPR.

9 Article 5(1)(c) of the GDPR.

10 Article 5(1)(d) of the GDPR.

11 Article 5(1)(e) of the GDPR.

b processing on a large scale special categories of personal data under Article 9(1) of the GDPR, or of personal data revealing criminal convictions and offences under Article 10 of the GDPR; or

c a systematic monitoring of a publicly accessible area on a large scale.

Article 35(4) of the GDPR requires the DSA to publish a list of activities in relation to which a DPIA should be carried out. If the controller has appointed a Data Protection Officer (DPO), the controller should seek the advice of the DPO when carrying out the DPIA.

Importantly, Article 36(1) of the GDPR states that where the outcome of the DPIA indicates that the processing involves a high risk, which cannot be mitigated by the controller, the DSA should be consulted prior to the commencement of the processing.

A DPIA involves balancing the interests of the controller against those of the data subject. Article 35(7) of the GDPR states that a DPIA should contain at a minimum:

a a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;

b an assessment of the necessity and proportionality of the processing operations in relation to the purpose of the processing;

c an assessment of the risks to data subjects; and

d the measures in place to address risk, including security and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of the data subject.

The EDPB noted in its guidelines on DPIAs that the reference to the 'rights and freedoms' of data subjects under Article 35 of the GDPR while primarily concerned with rights to data protection and privacy also includes other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition on discrimination, right to liberty and conscience and religion.[12]

The EDPB introduced the following nine criteria that should be considered by controllers when assessing whether their processing operations require a DPIA, owing to their inherent high risk[13] to data subjects rights and freedoms:

a evaluation or scoring, including profiling and predicting, especially from 'aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements';

b automated-decision making with legal or similar significant effects – processing that aims at taking decisions on data subjects producing 'legal effects concerning the natural person' or which 'similarly significantly affects the natural person'. For example, the processing may lead to the exclusion or discrimination against data subjects. Processing with little or no effect on data subjects does not match this specific criterion;

c systematic monitoring – processing used to observe, monitor or control data subjects, including data collected through networks or 'a systematic monitoring of a publicly

12 Article 29 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, WP 248, as last revised and adopted on 4 October 2017, page 6.

13 Article 29 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, WP 248, as last revised and adopted on 4 October 2017, pages 9–11.

accessible area'. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how their data will be used;

d sensitive data or data of a highly personal nature – this includes special categories of personal data as defined in Article 9 of the GDPR (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10 of the GDPR. An example would be a hospital keeping patients' medical records or a private investigator keeping offenders' details. Additionally, beyond the GDPR, there are some categories of data that can be considered as increasing the possible risk to the rights and freedoms of data subjects. These personal data are considered as sensitive (as the term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud);

e data processed on a large scale: the GDPR does not define what constitutes large-scale. In any event, the EDPB recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
- the volume of data and/or the range of different data items being processed;
- the duration, or permanence, of the data processing activity; and
- the geographical extent of the processing activity.

f matching or combining datasets, for example originating from two or more data processing operations performed for different purposes or by different controllers in a way that would exceed the reasonable expectations of the data subject;

g data concerning vulnerable data subjects – the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the data subjects may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children as they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data and employees; and

h innovative use or applying new technological or organisational solutions, for example, combining use of finger print and face recognition for improved physical access control. The GDPR makes it clear that the use of a new technology, defined in 'accordance with the achieved state of technological knowledge' can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to data subjects' rights and freedoms. Furthermore, the personal and social consequences of the deployment of a new technology may be unknown.

i When the processing in itself 'prevents data subjects from exercising a right or using a service or a contract'. This includes processing operations that aim to allow, modify or refuse data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

Additionally, the EDPB noted that the mere fact the controller's obligation to conduct a DPIA has not been met does not negate its general obligation to implement measures to appropriately manage risks to the rights and freedoms of the data subject when processing their personal data.[14] In practice, this means controllers are required to continuously assess the risks created by their processing activities in order to identify when a type of processing is likely to result in a high risk to the rights and freedoms of the data subject.

The EDPB recommends that as a matter of good practice, controllers should continuously review and regularly reassess their DPIAs.[15]

Data protection by design and by default

Article 25 of the GDPR requires controllers to, at the time of determining the means of processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation and anonymisation, which are designed to implement the data protection principles in the GDPR, in an effective manner, and to integrate the necessary and appropriate safeguards into the processing of personal data in order to meet the data protection requirements of the GDPR and protect the rights of the data subject.

Controllers are also under an obligation to implement appropriate technical and organisational measures that ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. This obligation under Article 25(2) of the GDPR covers the amount of personal data collected, the extent of the processing of the personal data, the period of storage of the personal data and its accessibility.

DPOs

Article 37 of the GDPR requires both controllers and processors to appoint a DPO where:

a the processing is carried out by a public authority or body, except where courts are acting in their judicial capacity;

b the core activities of the controller or processor consist of processing operations that, by virtue of their nature, scope or purpose, require regular and systematic monitoring of data subjects on a large scale; or

c the core activities of the controller or processor consist of processing on a large scale special categories of personal data pursuant to Article 9 of the GDPR or personal data about criminal convictions and offences pursuant to Article 10 of the GDPR.

The EDPB, in its guidance on DPOs, noted that 'core activities' can be considered key operations[16] required to achieve the controller or processor's objectives. However, it should not be interpreted as excluding the activities where the processing of personal data forms an

14 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, WP 248, as last revised and adopted on 4 October 2017, page 6.

15 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, WP 248, as last revised and adopted on 4 October 2017, page 14.

16 Article 29 Working Party, Guidelines on Data Protection Officers (DPOs), WP 243, as last revised and adopted on 5 April 2017, page 20.

'inextricable' part of the controller or processor's activities. The EDPB provides the example of the core activity of a hospital being to provide healthcare. However, it cannot provide healthcare effectively or safely without processing health data, such as patients' records.[17]

Any DPO appointed must be appointed on the basis of their professional qualities and expert knowledge of data protection law and practices.[18] The EDPB note personal qualities of the DPO should include integrity and high professional ethics, with the DPO's primary concern being enabling compliance with the GDPR.[19]

Staff members of the controller or processor may be appointed as a DPO, as can a third-party consultant. Once the DPO has been appointed, the controller or processor must provide their contact details to their DSA.[20]

A DPO must be independent, whether or not he or she is an employee of the respective controller or processor and must be able to perform his or her duties in an independent manner.[21] The DPO can hold another position but must be free from a conflict of interests. For example, the DPO could not hold a position within the controller organisation that determined the purposes and means of data processing, such as the head of marketing, IT or human resources.

Once appointed, the DPO is expected to perform the following, non-exhaustive list of tasks.

a inform and advise the controller or processor and the employees who carry out the processing of the GDPR obligations and relevant Member State data protection obligations;

b monitor compliance with the GDPR, and other relevant Member State data protection obligations, and oversee the data protection policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations and the related audits;

c provide advice where requested in relation to the DPIA;

d cooperate with the DSA; and

e act as the contact point for the DSA on issues relating to processing.[22]

The GDPR also provides the option, where controllers or processors do not meet the processing requirements necessary to appoint a DPO, to voluntarily appoint one.[23]

The EDPB recommends in its guidance on DPOs that even where controllers or processors come to the conclusion that a DPO is not required to be appointed, the internal analysis carried out to determine whether or not a DPO should be appointed should be documented to demonstrate that the relevant factors have been taken into account properly.[24]

17 Article 29 Working Party Guidelines on Data Protection Officers ('DPOs'), WP 243, as last revised and adopted on 5 April 2017, page 7.

18 Article 37(5) of the GDPR.

19 Article 29 Working Party Guidelines on Data Protection Officers ('DPOs'), WP 243. as last revised and adopted on 5 April 2017, page 12.

20 Article 37(7) of the GDPR.

21 Recital 97 of the GDPR.

22 Article 39 of the GDPR.

23 Article 37(4) of the GDPR.

24 Article 29 Working Party Guidelines on Data Protection Officers (DPOs), WP 243, as last revised and adopted on 5 April 2017, page 5.

Lawful grounds for processing

Controllers may only process personal data if they have satisfied one of six conditions:

a the data subject in question has consented to the processing;

b the processing is necessary to enter into or perform a contract with the data subject. The EDPB published draft guidelines on this lawful ground in April 2019 in which a very narrow interpretation of contractual necessity was adopted;

c the processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of the personal data;

d the processing is necessary to comply with a legal obligation to which the controller is subject;

e the processing is necessary to protect the vital interests of the data subject; or

f the 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. Of these conditions, the first three will be most relevant to business.[25]

Personal data that relates to a data subject's racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (special categories of personal data) can only be processed where both a lawful ground under Article 6 and a condition under Article 9 are satisfied. The Article 9 conditions that are most often relevant to a business are where the data subject has explicitly consented to the processing or the processing is necessary for the purposes of carrying out its obligations in the field of employment and social security and social protection law.

The EDPB states in its guidance on consent, that where controllers intend to rely on consent as a lawful ground for processing, they have a duty to assess whether they will meet all of the GDPR requirements to obtain valid consent.[26] Valid consent under the GDPR is a clear affirmative act that should be freely given, specific, informed and an unambiguous indication of the data subject's agreement to the processing of their personal data. Consent is not regarded as freely given where the data subject has no genuine or free choice or is not able to refuse or withdraw consent without facing negative consequences. For example, where the controller is in a position of power over the data subject, such as an employer, the employee's consent is unlikely to be considered freely given or a genuine or free choice, as to choose to withdraw consent or refuse to give initial consent in the first place could result in the employee facing consequences detrimental to their employment.

As the EDPB notes, consent can only be an appropriate lawful ground for processing personal data if the data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without negative effects.[27] Without such genuine and free choice, the EDPB notes the data subject's consent becomes illusory and consent will be invalid, rendering the processing unlawful.[28]

25 Article 6 of the GDPR.

26 Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259, as last revised and adopted on 10 April 2018, page 3.

27 ibid.

28 ibid.

Provision of information

Certain information needs to be provided by controllers to data subjects when controllers collect personal data about them, unless the data subjects already have that information. Article 13 of the GDPR provides a detailed list of the information required to be provided to data subjects either at the time the personal data is obtained or immediately thereafter, including:

a the identity and contact details of the controller (and where applicable, the controller's representative);
b the contact details of the DPO, where applicable;
c the purposes of the processing;
d the lawful ground for the processing;
e the recipients or categories of recipients of the personal data;
f where the personal data is intended to be transferred to a third country, reference to the appropriate legal safeguard to lawfully transfer the personal data;
g the period for which the personal data will be stored or where that is not possible, the criteria used to determine that period;
h the existence of rights of data subjects to access, correct, restrict and object to the processing of their personal data;
i the right to lodge a complaint with a DSA; and
j whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract.

In instances where the personal data are not collected by the controller directly from the data subject concerned, the controller is expected to provide the above information to the data subject, in addition to specifying the source and types of personal data, within a reasonable time period after obtaining the personal data, but no later than a month after having received the personal data or if the personal data is to be used for communication with the data subject, at the latest, at the time of the first communication to that data subject.[29] In cases of indirect collection, it may also be possible to avoid providing the required information if to do so would be impossible or involve a disproportionate effort, or if the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Member State law or obtaining or disclosing of personal data is expressly laid down by EU or Member State law to which the controller is subject.[30] These exceptions, according to the EDPB should be interpreted narrowly.[31]

The EDPB notes that in order to ensure the information notices are concise, transparent, intelligible and easily accessible under Article 12 of the GDPR, controllers should present the information efficiently and succinctly to prevent the data subjects from experiencing information fatigue.[32]

29 Article 14(3) of the GDPR.

30 Article 14(5) of the GDPR.

31 Article 29 Working Party Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018, page 25.

32 Article 29 Working Party Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018, page 7.

iii Security and breach reporting

The GDPR requires controllers and, where applicable, processors to ensure that appropriate technical and organisational measures are in place to protect personal data and ensure a level of security appropriate to the risk.[33] Such technical and organisational measures include the pseudonymisation of personal data, encryption of personal data, anonymisation of personal data, and de-identification of personal data, which occurs where the information collected has undergone a process that involves the removal or alteration of personal identifiers and any additional techniques or controls required to remove, obscure, aggregate or alter the information in such a way that no longer identifies the data subject. Additionally, controllers must also ensure that when choosing a processor they choose one that provides sufficient guarantees as to the security measures applied when processing personal data on behalf of the controller, pursuant to Article 28 of the GDPR. A controller must also ensure that it has in place a written contract with the processor under which the processor undertakes to comply with data protection requirements under Article 28 of the GDPR, including only processing the personal data on the instructions of the controller and being subject to the same data protection obligations as set out in the contract between the controller and processor. Under such an agreement, the processor will remain liable for the failure of the sub-processor to perform its data protection obligations under the agreement between the processor and the sub-processor.[34]

Personal data breaches

Article 4(1) of the GDPR defines a personal data breach broadly as a 'breach of security leading to the accidental or unlawful destruction, loss, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed'. According to the guidelines published by the EDPB on personal data breach notification under the GDPR[35] personal data breaches typically fall in one of the following categories:

a confidentiality breaches: where there is an unauthorised or accidental disclosure of, or access to, personal data;

b availability breaches: where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and

c integrity breaches: where there is an unauthorised or accidental alteration of personal data.

Additionally, controllers are required, with the assistance of the processors, where applicable, to report personal security breaches that are likely to result in a risk to the rights and freedoms of the data subject, to the relevant DSA without undue delay and, where feasible, not later than 72 hours after having first become aware of the personal data breach. Where the processor becomes aware of a personal data breach it is under an obligation to report the breach to the controller. Upon receiving notice of the breach from the processor, the controller is then considered aware of the personal data breach and has 72 hours to report the breach to the relevant DSA.

33 Article 32 of the GDPR

34 Article 28(4) of the GDPR.

35 Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP 250, as last revised and adopted on 6 February 2018, page 7.

The EDPB notes in its guidance on personal data breaches that the controller should have internal processes in place that are able to detect and address a personal data breach.[36] The EDPB provides the example of using certain technical measures such as data flow and log analysers to detect any irregularities in processing of personal data by the controller.[37] Importantly, the EDPB notes that once a breach is detected it should be reported upwards to the appropriate level of management so it can be addressed and contained effectively. These measures and reporting mechanisms could, in the view of the EDPB, be set out in the controller's incident response plans.[38]

Exceptions

Controllers are exempted from notifying a personal data breach to the relevant DSA if it is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. In assessing the level of risk, the following factors should be taken into consideration:

a Type of personal data breach: is it a confidentiality, availability, or integrity type of breach?

b Nature, sensitivity and volume of personal data: usually, the more sensitive the data, the higher the risk of harm from a data subject's point of view. Also, combinations of personal data are typically more sensitive than single data elements.

c Ease of identification of data subjects: the risk of identification may be low if the data were protected by an appropriate level of encryption. In addition, pseudonymisation can reduce the likelihood of data subjects being identified in the event of a breach.

d Severity of consequences of data subjects: especially if sensitive personal data are involved in a breach, the potential damage to data subjects can be severe and thus the risk may be higher.

e Special characteristics of the data subjects: data subjects who are in a particularly vulnerable position (e.g., children) are potentially at greater risk if their personal data are breached.

f Number of affected data subjects: generally speaking, the more data subjects that are affected by a breach, the greater the potential impact.

g Special characteristics of the controller: for example, if a breach involves controllers who are entrusted with the processing of sensitive personal data (e.g., health data), the threat is presumed to be greater.

h Other general considerations: assessing the risk associated with a breach can be far from straightforward. Therefore the EDPB, in its guidance on personal data breach notifications, refers to the recommendations published by the European Union Agency for Network and Information Security (ENISA), which provides a methodology for assessing the severity of the breach and which may help with designing breach management response plans.[39]

36 Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP 250, as last revised and adopted on 6 February 2018, page 12.

37 ibid.

38 ibid.

39 Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP 250, as last revised and adopted on 6 February 2018, page 26.

Notifying affected data subjects

In addition to notifying the relevant DSA, in certain cases controllers may also be required to communicate the personal data breach to affected data subjects (i.e. when the personal data breach is likely to result in a 'high risk' to the rights and freedoms of data subjects). The specific reference in the law to high risk indicates that the threshold for communicating a breach to data subjects is higher than for notifying the DSAs – taking account of the risk factors listed above.

It should be noted that the accountability requirements in the GDPR summarised above, such as purpose limitation, data minimisation and storage limitation, mean, for example, that implementing technical controls in isolation, or the piecemeal adoption of data security standards, are unlikely to be sufficient to ensure compliance. As a default position, controllers should seek to minimise the collection and retention of personal data, and especially where sensitive personal data are collected and retained, ensure that those data are encrypted or otherwise made unintelligible to unauthorised parties, to the greatest extent possible.

iv Prohibition on transfers of personal data outside the EEA

Controllers and/or processors may not transfer personal data to countries outside of the European Economic Area (EEA)[40] unless the recipient country provides an adequate level of protection for the personal data.[41] The European Commission can make a finding on the adequacy of any particular non-EEA state and Member States are expected to give effect to these findings as necessary in their national laws. So far, the European Commission has made findings of adequacy with respect to Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay. In addition, on 12 July 2016, the Privacy Shield was adopted by the European Commission, with US companies being able to self-certify under the Privacy Shield from 1 August 2016 in order to receive personal data from organisations in the EU.[42] On 11 June 2018, members of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (MEPs), voted in favour of the suspension of the Privacy Shield until the US is in full compliance with the data protection requirements contained in the Privacy Shield. In July 2018, the European Parliament adopted the resolution and called on the US to comply with the requirements of the Privacy Shield by 1 September 2018, such as the appointment of an ombudsman to deal with complaints by data subjects in relation to the Privacy Shield and to remove organisations who fail to comply with data protection requirements contained in the Privacy Shield. The second annual review of the functioning of the Privacy Shield was published by the European Commission on 19 December 2018, also asking the US to appoint a permanent Privacy Shield ombudsman by 28 February 2019. On 18 January 2019, the US announced its intention to appoint Keith Krach as the Privacy Shield's first permanent ombudsman. Mr Krach's nomination was confirmed by the US Senate on 20 June 2019. The validity of the Privacy Shield has also been challenged before the CJEU by the French digital privacy rights advocacy group, La Quadrature du Net, claiming the Privacy Shield is incompatible with

40 The EEA consists of the 28 EU Member States together with Iceland, Liechtenstein and Norway.

41 Article 45 of the GDPR.

42 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016.

EU data protection laws, given the potential access to the transferred personal data by US surveillance agencies. The CJEU has, however, postponed the hearing of this case pending judgment in the case before the CJEU concerning the validity of model contracts (see below).

Where transfers are to be made to countries that are not deemed adequate, other exceptions may apply to permit the transfer.[43] The European Commission has approved EU standard contractual clauses that may be used by controllers and processors when transferring personal data from the EU to non-EEA countries (a model contract).[44] There are two forms of model contract: one where both the data exporter and data importer are controllers; and another where the data exporter is a controller and the data importer is a data processor. Personal data transferred on the basis of a model contract will be presumed to be adequately protected. However, model contracts have been widely criticised as being onerous on the parties. This is because they grant third-party rights to data subjects to enforce the terms of the model contract against the data exporter and data importer, and require the parties to the model contract to give broad warranties and indemnities. The clauses of the model contracts also cannot be varied and model contracts can become impractical where a large number of data transfers need to be covered by numerous model contracts. However, the status of model contracts is currently uncertain, as following questions as to the validity of model contracts from the Irish DSA, the Irish High Court referred the questions to the CJEU for a preliminary ruling to determine the legal status of model contracts. The CJEU is expected to give its judgment in early 2020. Separately, the European Commission recently announced that it is working to modernise model contracts, but this is unlikely to be completed before the CJEU publishes its judgment.

An alternative means of authorising transfers of personal data outside the EEA is the use of binding corporate rules. This approach may be suitable for multinational companies transferring personal data within the same company, or within a group of companies. Under the binding corporate rules approach, the company would adopt a group-wide data protection policy that satisfies certain criteria and, if the rules bind the whole group, then those rules could be approved by the relevant DSA as providing adequate data protection for transfers of personal data throughout the group. The EDPB has published various documents[45] on binding corporate rules, including a model checklist for the approval of binding corporate rules,[46] a table setting out the elements and principles to be found in binding corporate

43 Article 46 of the GDPR.

44 Article 46(2)(c) of the GDPR.

45 WP 133 – Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data adopted on 10 January 2007.
WP 154 – Working Document setting up a framework for the structure of Binding Corporate Rules adopted on 24 June 2008.
WP 155 – Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules adopted on 24 June 2008 and last revised on 8 April 2009.
WP 195 – Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules adopted on 6 June 2012.
WP 195a – Recommendation 1/2012 on the standard application form for approval of Binding Corporate Rules for the transfer of personal data for processing activities adopted on 17 September 2012.
WP 204 – Explanatory Document on the Processor Binding Corporate Rules last revised and adopted on 22 May 2015.

46 WP 108 – Working Document establishing a model checklist application for approval of binding corporate rules adopted on 14 April 2005.

rules,[47] an explanatory document on processor binding corporate rules, recommendations on the standard application for approval of controller and processor binding corporate rules,[48] a co-operation procedure for issuing common opinions on adequate safeguards resulting from binding corporate rules, a framework for the structure of binding corporate rules, and frequently asked questions on binding corporate rules.

In addition to binding corporate rules and other data transfer solutions, the transfer of personal data outside of the EEA can occur via the use of approved codes of conduct or certification mechanisms.

v Rights of the data subject

The GDPR provides for a series of rights data subjects can use in relation to the processing of their personal data, with such rights subject to certain restrictions or limitations.

Timing and costs

The GDPR requires that a data subject's request to exercise their rights be complied with without undue delay and in any event within one month of receipt of the request. If the request is particularly complex, then this period can be extended to three months if the data subject is informed of the reasons for the delay within one month. Where it is determined that compliance with the request is not required, then data subjects should be informed of this within one month together with the reasons as to why the request is not being complied with and the fact that they can lodge a complaint with a DSA and seek a judicial remedy.

A fee must not be charged for compliance with a data subject's rights request unless it can be demonstrated that the request is manifestly unfounded or excessive.

Right to access personal data

Article 15 of the GDPR provides data subjects with the right to access their personal data processed by the controller. The right requires controllers to confirm whether or not they are processing the data subject's personal data and confirm:

a the purpose of the processing;
b the categories of personal data concerned;
c the recipients or categories of recipients to whom the personal data has been or will be disclosed to, in particular recipients in third countries;
d where possible, the retention period for storing the personal data, or, where that is not possible, the criteria used to determine that period;
e the existence of the right to request from the controller rectification, erasure, restriction or objection to the processing of their personal data;
f the right to lodge a complaint with the DSA;
g where personal data is not collected from the data subject, the source of the personal data; and
h the existence of automated decision making, including profiling, where applicable.

47 WP 153 – Working Document setting up a table with the elements and principles to be found in binding corporate rules adopted on 24 June 2008.

48 WP 264 – Recommendation on the Standard Application form for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data – Adopted on 11 April 2018.
WP 265 – Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data – Adopted on 11 April 2018.

Under the right of access to personal data, the controller is required to provide a copy of the personal data undergoing processing.

This right is not absolute, but subject to a number of limitations, including the right to obtain a copy of the personal data shall not adversely affect the rights and freedoms of others.[49] According to Recital 63 of the GDPR, these rights may include trade secrets or other intellectual property rights. As such, before disclosing information in response to a subject access request, controllers should first consider whether the disclosure would adversely affect the rights of any third party's personal data; and the rights of the controller and in particular, its intellectual property rights. However, even where such an adverse effect is anticipated, the controller cannot simply refuse to comply with the access request. Instead, the controller would need to take steps to remove or redact information that could impact the rights or freedoms of others.

Where the controller processes a large quantity of the data subject's personal data, as would likely be the case in respect of an organisation and its employees, the controller has a right to request that, before the personal data is delivered, the data subject should specify the information or processing activities to which the request relates.[50] However, caution should be exercised when requesting further information from the data subject as it is likely that under the GDPR a controller will not be permitted to narrow the scope of a request itself.

Where the controller is able to demonstrate that the data subject's request for access to the personal data the controller holds is manifestly unfounded or excessive because of its repetitive nature, the controller can refuse to comply with the data subject's request.[51] However, in the absence of guidance or case law to provide parameters around the scope of these exemptions, a strict interpretation should be considered for the concept of 'manifestly unfounded' with repetitive requests being documented in order to fulfil the burden of proof as to their excessive character.

If the controller has reasonable doubts concerning the identity of the data subject making the access request, the controller can request the provision of additional information necessary to confirm the identity of the data subject.[52]

If the controller is able to demonstrate that it is not in a position to identify the data subject, it can refuse to comply with a data subject's request to access their personal data.[53]

Right of rectification of personal data

Article 16 of the GDPR provides data subjects with the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

The right is not absolute but subject to certain limitations or restrictions, including:

a where the controller is able to demonstrate that the data subject's request for rectification of their personal data the controller holds is manifestly unfounded or excessive because of its repetitive nature, the controller can refuse to comply with the data subject's request;[54]

49 Article 15(4) of the GDPR.

50 Recital 63 of the GDPR.

51 Article 12(5) of the GDPR.

52 Article 12(6) of the GDPR.

53 Article 12(2) of the GDPR.

54 Article 12(5) of the GDPR.

b where the controller has reasonable doubts concerning the identity of the data subject making the request, the controller can request the provision of additional information necessary to confirm the identity of the data subject;[55] and

c where the controller is able to demonstrate that it is not in a position to identify the data subject, it can refuse to comply with a data subject's request to access their personal data.[56]

Right of erasure of personal data ('right to be forgotten')

Article 17 of the GDPR provides data subjects with the right of erasure of their personal data the controller holds without undue delay, where:

a the personal data are no longer necessary for the purposes for which they were collected;[57]

b the data subject withdraws consent to the processing and there is no other legal ground for the processing;[58]

c the data subject objects to the processing and there are no overriding legitimate grounds for the processing;[59]

d the personal data has been unlawfully processed;[60]

e the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;[61] and

f the personal data has been collected in connection with an online service offered to a child.[62]

However, the right of erasure is not absolute and is subject to certain restrictions or limitations:

a the data subject's right of erasure will not apply where the processing is necessary for exercising the right of freedom and expression and information;

b where complying with a legal obligation which requires processing by Union or Member State law;

c reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (i);

d for archiving purposes in the public interest, scientific, historical research or statistical research purposes;

e for the establishment, exercise or defence of legal claims;

f where the controller is able to demonstrate that the data subject's request for rectification of their personal data the controller holds is manifestly unfounded or excessive because of its repetitive nature, the controller can refuse to comply with the data subject's request;[63]

55 Article 12(6) of the GDPR.
56 Article 12(2) of the GDPR.
57 Article 17(1)(a) of the GDPR.
58 Article 17(1)(b) of the GDPR.
59 Article 17(1)(c) of the GDPR.
60 Article 17(1)(d) of the GDPR.
61 Article 17(1)(e) of the GDPR.
62 Article 17(1)(f)) of the GDPR.
63 Article 12(5) of the GDPR.

g where the controller has reasonable doubts concerning the identity of the data subject making the request, the controller can request the provision of additional information necessary to confirm the identity of the data subject;[64] and

h where the controller is able to demonstrate that it is not in a position to identify the data subject, it can refuse to comply with a data subject's request to access their personal data.[65, 66]

Right to restriction of processing

Article 18 of the GDPR also provides data subjects with the right to restrict the processing of their personal data in certain circumstances. The restriction of processing means that, with the exception of storage, the personal data can only be processed where:

a the accuracy of the personal data is contested by the data subject, enabling the controller to verify the accuracy of the personal data;

b the processing is unlawful and the data subject opposes the erasure of the personal data and requests restriction of the processing;

c the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

d the data subject has objected to the processing pursuant to Article 21(1) of the GDPR, pending the verification of whether the legitimate grounds of the controller override those of the data subject.

The right of the data subject to request the restriction of the processing of their personal data is not absolute and is qualified:

a where the controller is able to demonstrate that the data subject's request for rectification of their personal data the controller holds is manifestly unfounded or excessive because of its repetitive nature, the controller can refuse to comply with the data subject's request;[67]

b where the controller has reasonable doubts concerning the identity of the data subject making the request, the controller can request the provision of additional information necessary to confirm the identity of the data subject;[68] and

c where the controller is able to demonstrate that it is not in a position to identify the data subject, it can refuse to comply with a data subject's request to access their personal data.[69]

64 Article 12(6) of the GDPR.
65 Article 12(2) of the GDPR.
66 Article 17(3) of the GDPR.
67 Article 12(5) of the GDPR.
68 Article 12(6) of the GDPR.
69 Article 12(2) of the GDPR.

Right to data portability

Article 20 of the GDPR provides data subjects with the right to receive their personal data which they have provided to the controller, in a structured, commonly used and machine-readable format and have the right to transmit their personal data to another controller without hindrance, where the processing is based on consent pursuant to Article 6(1)(a) or 9(2)(a) of the GDPR; and where the processing is carried out by automatic means.

This right would, for example, permit a user to have a social media provider transfer his or her personal data to another social media provider.

Article 20(2) of the GDPR limits the requirement for a controller to transmit personal data to a third-party data controller where this is 'technically feasible'. The EDPB has published guidance on the right to data portability, stating that a transmission to a third-party data controller is 'technically feasible' when 'communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data'.[70]

In addition, the EDPB guidance recommends that controllers begin developing technical tools to deal with data portability requests and that industry stakeholders and trade associations should collaborate to deliver a set of interoperable standards and formats to deliver the requirements of the right to data portability.[71]

The guidance also clarifies which types of personal data the right to data portability should apply to, specifically:

a that the right applies to data provided by the data subject, whether knowingly and actively as well as the personal data generated by his or her activity;[72]

b the right does not apply to data inferred or derived by the controller from the analysis of data provided by the data subject (e.g., a credit score);[73] and

c the right is not restricted to data communicated by the data subject directly.[74]

Right to object to the processing of personal data

Article 21 of the GDPR provides data subjects with the right to object to the processing of their personal data. This right includes the right to object to:

a processing where the controller's legal basis for the processing of the personal data is either necessary for public interest purposes or where the processing is in the legitimate interests of the controller ('general right to object');

b processing for direct marketing purposes (the 'right to object to marketing'); and

c processing necessary for scientific or historical research purposes or statistical purposes and the data subject has grounds to object that relate to 'his or her particular situation'.

---

70 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 16.

71 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 3.

72 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 10.

73 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 10.

74 Article 29 Working Party, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), page 3.

The right of the data subject to object to the processing of their personal data is not absolute:

a where the data subject can demonstrate compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject or where the processing is necessary for the establishment, exercise or defence of legal claims;[75] or

b where the processing is necessary for research purposes, there is an exemption to the right of data subjects to object where the processing is necessary for the performance of a task carried out for reasons of public interest.[76]

vi Company policies and practices

While the GDPR is not prescriptive as to the policies and procedures that a company should have in place, it emphasises the concept of accountability (i.e., the ability to demonstrate compliance with the GDPR). In turn, to comply with the accountability obligations under the GDPR, a company will need to have in place a number of policies and procedures. These may include, for example:

a a data protection policy – addressing how the company complies with the principles of the GDPR;

b a data processing record – to comply with Article 30 of the GDPR;

c legitimate interest assessments – where processing personal data relies on the legitimate interest ground for processing;

d data protection or fair processing notices – to comply with Articles 13/14 of the GDPR (e.g., for customers and employees);

e data processing provisions for inclusion in contracts entered into between controllers and processors – to comply with Article 28 of the GDPR;

f a vendor data protection questionnaire – to assess data protection compliance of processors processing personal data on company's behalf;

g a GDPR-compliant form of consent or checklist to assess requirements for valid consent;

h data treatment guidelines – to address how in practice the company complies with the data treatment principles under Article 5 of the GDPR;

i a data protection impact assessment template and guidelines for when it should be completed;

j a records retention policy and schedule – which will in fact be broader than data protection;

k information security policies and procedures, and a personal data breach response plan;

l data subject rights' guidelines – addressing how in practice the company will respond to a request made by a data subject to exercise their rights under the GDPR;

m EU standard contractual clauses or other data transfer solutions;

n a data protection officer (DPO) assessment – to document whether or not the company is under a statutory obligation to appoint a DPO;

o a GDPR audit checklist;

p a data protection representative agreement – as required under Article 27 of the GDPR;

75 Article 21(1) of the GDPR.

76 Article 21(6) of the GDPR.

q a lead DPA assessment – documenting whether or not the company can take the benefit of the one-stop-shop principle under the GDPR and in turn, identify a lead DPA and if so, which DPA will likely be the lead DPA; and
r GDPR training materials for staff.

vii Enforcement under the GDPR

DSAs, lead DSAs and 'one-stop shop'

Enforcement of the GDPR is done at a national level through national or state DSAs. In addition, one of the aims of the GDPR was to enable a controller that processes personal data in different EU Member States to deal with one lead DSA, known as the 'One Stop Shop' mechanism.

The one-stop shop mechanism

Under Article 56 of the GDPR, a controller or processor that carries out cross-border processing will be primarily regulated by a single lead DSA where the controller or processor has its main establishment.

Article 4(23) of the GDPR defines cross-border processing as either:

a processing of personal data that takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the EU where the controller or processor is established in more than one Member State (i.e., processing of personal data by the same controller or processor through local operations across more than one Member State – e.g., local branch offices); or
b the processing of personal data that takes place in the context of the activities of a single establishment of a controller or processor in the EU but that substantially affects or is likely to substantially affect data subjects in more than one Member State.

In determining whether the processing falls within this scope, the EDPB has published guidance stating that DSAs will interpret 'substantially affects' on a case-by-case basis taking into account:

a the context of the processing;
b the type of data;
c the purpose of the processing and a range of other factors, including, for example, whether the processing causes, or is likely to cause, damage, loss or distress to data subjects; or
d whether it involves the processing of a wide range of personal data.

Assuming a controller is engaged in cross-border processing, it will need to carry out the main establishment test. If a controller has establishments in more than one Member State, its main establishment will be the place of its 'central administration' (which is not defined in the GDPR) unless this differs from the establishment in which the decisions on the purposes and means of the processing are made and implemented, in which case the main establishment will be the latter.[77]

For processors, the main establishment will also be the place of its central administration. However, to the extent a processor does not have a place of central administration in the

77 Article 4(16) of the GDPR.

EU, the main establishment will be where its main processing activities are undertaken. The EDPB in its guidance on lead supervisory authorities, make it clear that the GDPR does not permit 'forum shopping'[78] and that where a company does not have an establishment in the EU, the one-stop-shop mechanism does not apply and it must deal with DSAs in every EU Member State in which it is active.[79]

Importantly under Article 60 of the GDPR, other concerned DSAs can also be involved in the decision-making for a cross-border case. According to the GDPR, a concerned DSA will participate where:

a the establishment of the controller or processor subject to the investigation is in the concerned DSA's Member State;

b data subjects in the concerned DSA's Member State are substantially or are likely to be substantially affected by the processing of the subject of the investigation; or

c a complaint has been lodged with that DSA.[80]

In the case of a dispute between DSAs, the EDPB shall adopt a final binding decision.[81] The GDPR also promotes cooperation among Member State DSAs by requiring the lead DSA to submit a draft decision on a case to the concerned DSA, where they will have to reach a consensus prior to finalising any decision.[82]

EDPB

The EDPB is an independent EU-wide body, which contributes towards ensuring the consistent application of the GDPR across all EU Member States, and promotes cooperation between EU DSAs. The EDPB is comprised of representatives from all EU DSAs, the European Data Protection Supervisor, the EU's independent data protection authority, and a European Commission representative, who has a right to attend EDPB meetings without voting rights.

Since the coming into force of the GDPR, the EDPB has been fairly active in publishing GDPR guidance and for the most part this has been well received by companies. In addition to the GDPR guidance published by the former Article 29 Working Party and adopted by the EDPB, the EDPB has finalised guidelines on codes of conduct and certification mechanisms. The EDPB has also published a variety of draft guidelines including addressing the territorial scope of the GDPR and video surveillance. We expect to see further guidance published in the coming year.

Enforcement rights

The GDPR provides data subjects with a multitude of enforcement rights in relation to the processing of their personal data:

a Right to lodge a complaint with the DSA: Article 77 of the GDPR provides data subjects with the right to lodge a complaint with a DSA, in the Member State of the

78 Article 29 Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, WP244, adopted on 13 December 2016 and revised on 5 April 2017, page 8.

79 Article 29 Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, WP244, adopted on 13 December 2016 and revised on 5 April 2017, page 10.

80 Article 4(22) of the GDPR.

81 Article 65(1) of the GDPR.

82 Article 60 of the GDPR.

data subject's habitual residence, place of work or place of the alleged infringement of the GDPR, where the data subject considers that the processing of his or her personal data infringes the data protection requirements of the GDPR.

b Right to an effective judicial remedy against a controller or processor: Article 79 of the GDPR provides data subjects with the right to bring a claim against a controller or a processor before the courts of the Member State where the controller or processor is established in, or where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

c Right to compensation and liability: Article 82 of the GDPR provides data subjects with the right to receive compensation from the controller or processor where the data subject has suffered material or non-material damage as a result of an infringement of the GDPR.

Administrative fines

Notably, Article 83 of the GDPR grants DSAs the power to impose substantial fines on controllers or processors for the infringement of the GDPR. The GDPR provides a two-tier structure for fines, where the following will result in fines of up to €10 million or 2 per cent of annual turnover, whichever is greater:

a failure to ensure appropriate technical and organisational measures are adopted when determining the means of processing the personal data in addition to the actual processing itself;

b failing to comply with the Article 28(3) of the GDPR, where any processing of personal data must be governed by a written data processing agreement;

c maintaining records as a controller of all processing activities under its responsibility;

d conducting data protection impact assessments; and

e notifying personal data breaches to the data subject and data supervisory authorities, respectively.[83]

The GDPR states that certain infringements of the GDPR merit a higher penalty and will be subject to higher fines of up to €20 million or 4 per cent of annual turnover, whichever is the greater.[84] These include:

a infringements of the basic principles of processing personal data, including conditions for obtaining consent;

b failing to comply with data subjects' rights requests; and

c failing to ensure there are appropriate safeguards for the transfer of personal data outside the EEA.

These extensive penalties represent a significant change in the field of data protection that should ensure that businesses and governments take data protection compliance seriously.

83 Article 83(4) of the GDPR.

84 Article 83(5) of the GDPR.

DSAs' investigative powers

DSAs also have investigative powers under Article 58(1), including the power to:

a carry out investigations in the form of data protection audits;

b notify the controller or processor of an alleged infringement of the GDPR; and

c obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

DSAs are not limited to enforcement and investigative powers, but also have corrective[85] and authorisation and advisory[86] powers.

DSAs' corrective powers

Article 58(2) of the GDPR grants DSAs the power to require the controller or processor to make certain corrections in relation to the processing of personal data, including to:

a issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the GDPR;

b issue reprimands to a controller or processor where processing operations have infringed provisions of the GDPR;

c order the controller or processor to comply with the data subject's requests to exercise their data subject's rights in accordance with the GDPR;

d order the controller or processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period;

e order the controller to communicate a personal data breach to the data subject;

f impose a temporary or definitive limitation on processing, including a ban;

g order the rectification or erasure of personal data or restriction of processing of personal data and the notification of such actions to recipients to whom the personal data has been disclosed; and

h order the suspension of data flows to a recipient in a third country.

DSAs' authorisation and advisory powers

DSAs also have a range of advisory and authorisation powers under Article 58(3) of the GDPR, including the power to:

a issue opinions to the relevant Member State national parliament, Member State government or other institutions and bodies, as well as to the general public on the protection of personal data;

b authorise processing pursuant to Article 36(5) of the GDPR, if the law of the Member State requires prior authorisation;

c issue an opinion and approve draft codes of conduct pursuant to Article 40(5) of the GDPR;

d issue certifications and approve criteria of certification in accordance with Article 42(5) of the GDPR; and

e approve binding corporate rules pursuant to Article 47 of the GDPR.

85 Article 58(2) of the GDPR.

86 Article 58(3) of the GDPR.

vii Health data under the GDPR

Data concerning health falls within the 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'.[87]

The GDPR also states health data should include the following:

a all data pertaining to the health status of a data subject that reveals information relating to the past, current, or future physical or mental health status of the data subject;

b information collected in the course of registration for or the provision of healthcare services;

c a number, symbol, or particular assigned to an individual that uniquely identifies that individual for health purposes;

d information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and

e any information on disease, disability, disease risk, medical history, clinical treatment, or the physiological or biomedical state of the individual, independent of its source, for example, from a physician or a medical device.[88]

Relevant in the context of health data is Article 9(2)(j) of the GDPR, which includes the legal ground regarding where the 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 to ensure technical and organisational measures are in place and in particular, to comply with the principle of data minimisation.

III DIRECT MARKETING

The EU Electronic Communications (Data Protection and Privacy) Directive 2002/58/EC (the ePrivacy Directive) places requirements on Member States in relation to the use of personal data for direct marketing. Direct marketing for these purposes includes unsolicited faxes, or making unsolicited telephone calls through the use of automated calling machines, or direct marketing by email. In such instances, the direct marketer needs to have the prior consent of the recipient (i.e., consent on an opt-in basis). However, in the case of emails, there are limited exceptions for email marketing to existing customers where, if certain conditions[89] are satisfied, unsolicited emails can still be sent without prior consent. In other instances of unsolicited communications, it is left up to each Member State to decide whether such

87 Article 4(15) of the GDPR.

88 Recital 35 of the GDPR.

89 Unsolicited emails may be sent without prior consent to existing customers if the contact details of the customer have been obtained in the context of a sale of a product or a service and the unsolicited email is for similar products or services; and if the customer has been given an opportunity to object, free of charge in an easy manner, to such use of his or her electronic contact details when they are collected and on the occasion of each message in the event the customer has not initially refused such use – Article 13(2) of the ePrivacy Directive.

communications will require the recipient's prior consent or can be sent without prior consent unless recipients have indicated that they do not wish to receive such communications (i.e., consent on an opt-out basis).[90]

The ePrivacy Directive imposes requirements on providers of publicly available electronic communication services to put in place appropriate security measures and to notify subscribers of certain security breaches in relation to personal data.[91] The ePrivacy Directive was also amended in 2009[92] to require that website operators obtain the informed consent of users to collect personal data of users through website 'cookies' or similar technologies used for storing information. There are two exemptions to the requirement to obtain consent before using cookies: when the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; and when the cookie is strictly necessary for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[93]

The former Article 29 Working Party published an opinion on the cookie consent exemption[94] that provides an explanation on which cookies require the consent of website users (e.g., social plug-in tracking cookies, third-party advertising cookies used for behavioural advertising, analytics) and those that fall within the scope of the exemption (e.g., authentication cookies, multimedia player session cookies and cookies used to detect repeated failed login attempts). Guidance on how to obtain consent has been published at a national level by various data protection authorities.[95]

In July 2016, the former Article 29 Working Party issued an opinion on a revision of the rules contained in the ePrivacy Directive.[96]

On 10 January 2017, the European Commission issued a draft of the proposed Regulation on Privacy and Electronic Communications (the ePrivacy Regulation) to replace the existing ePrivacy Directive.[97] The ePrivacy Regulation will complement the GDPR and provide additional sector-specific rules, including in relation to marketing and the use of website cookies.

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 cookie use to website browsers; and

c ensuring that consent for direct marketing will be harder to obtain and must meet the standard set out in the Regulation; however, existing exceptions, such as the exemption where there is an existing relationship and similar products and services are being marketed, are likely to be retained.

90 Article 13(3) of the ePrivacy Directive.

91 Recital 20 and Article 4 of the ePrivacy Directive.

92 Directive 2009/56/EC.

93 Article 5(3) of the ePrivacy Directive.

94 WP 194 – Opinion 04/2012 on Cookie Consent Exemption.

95 For example: UK Information Commissioner's Office, 'Guidance on the rules on use of cookies and similar technologies'; and the French Commission Nationale de l'Informatique et des Libertés.

96 Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC).

97 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).

The European Commission's original timetable for the ePrivacy Regulation was for it to apply from 25 May 2018 and coincide with the coming into force of the GDPR. However, owing to ongoing political negotiations between the European Council (which represents EU Member States) and the European Parliament, the ePrivacy Regulation is not expected to come into force until 2021 at the earliest.

IV CLOUD COMPUTING

In its guidance on cloud computing adopted on 1 July 2012,[98] the EU's WP29 states that the majority of data protection risks can be divided into two main categories: lack of control over the data; and insufficient information regarding the processing operation itself. The lawfulness of the processing of personal data in the cloud depends on adherence to the principles of the now repealed Directive that are considered in the WP29 opinion, and some of which are summarised below. It would be reasonable to expect that the EDPB will issue new guidance on cloud computing and data protection to reflect new requirements under the GDPR. For the purposes of this section, references to the Directive should be read as references to the GDPR.

i Instructions of the controller

To comply with the requirements of the Directive, the WP29 provides that the extent of the instructions should be detailed in the relevant cloud computing agreement (the cloud agreement) along with service levels and financial penalties on the provider for non-compliance.

ii Purpose specification and limitation requirement[99]

Under the Directive, personal data must be collected for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes. To address this requirement, the agreement between the cloud provider and the client should include technical and organisational measures to mitigate this risk and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of the cloud provider or subcontractors.

iii Security[100]

Under the Directive, a controller must have in place adequate organisational and technical security measures to protect personal data and should be able to demonstrate accountability. The WP29 opinion comments on this point, reiterating that it is of great importance that concrete technical and organisational measures are specified in the cloud agreement, such as availability, confidentiality, integrity, isolation and portability. As a consequence, the agreement with the cloud provider should contain a provision to ensure that the cloud provider and its subcontractors comply with the security measures imposed by the client. It should also contain a section regarding the assessment of the security measures of the cloud

98 WP 196 – Opinion 5/2012 on Cloud Computing.

99 Article 6(b) of the Data Protection Directive.

100 Article 17(2) of the Data Protection Directive.

provider. The agreement should also contain an obligation for the cloud provider to inform the client of any security event. The client should also be able to assess the security measures put in place by the cloud provider.

iv Subcontractors

The WP29 opinion indicates that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard, with the controller retaining at all times the possibility to object to the changes or to terminate the agreement. There should also be a clear obligation on the cloud provider to name all the subcontractors commissioned, as well as the location of all data centres where the client's data can be hosted. It must also be guaranteed that the cloud provider and all the subcontractors shall act only on instructions from the client. The agreement should also set out the obligation on the part of the processor to deal with international transfers, for example, by signing contracts with sub-processors, based on the EU model contract clauses.

v Erasure of data[101]

The WP29 opinion states that specifications on the conditions for returning the personal data or destroying the data once the service is concluded should be contained in the agreement. It also states that data processors must ensure that personal data are erased securely at the request of the client.

vi Data subjects' rights[102]

According to the WP29 opinion, the agreement should stipulate that the cloud provider is obliged to support the client in facilitating exercise of data subjects' rights to access, correct or delete their data, and to ensure that the same holds true for the relation to any subcontractor.

vii International transfers[103]

As discussed above, under the Directive, personal data can only be transferred to countries located outside the EEA if the country provides an adequate level of protection.

viii Confidentiality

The WP29 opinion recommends that an agreement with the cloud provider should contain confidentiality wording that is binding both upon the cloud provider and any of its employees who may be able to access the data.

ix Request for disclosure of personal data by a law enforcement authority

Under the WP29 opinion, the client should be notified of any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as under a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

101 Article 6(e) of Data Protection Directive.

102 Article 12 and 14 of the Data Protection Directive.

103 Article 25 and 26 of the Data Protection Directive.

x Changes concerning the cloud services

The WP29 recommends that the agreement with the cloud provider should contain a provision stating that the cloud provider must inform the client about relevant changes concerning the cloud service concerned, such as the implementation of additional functions.

Now that the GDPR is in effect, clients and cloud service providers will need to be mindful that references to the Directive in the WP29 opinion will be defunct and that the equivalent principles and requirements in the GDPR should be complied with instead. For example, under Article 28(3) of the GDPR, processing by the processor (i.e., the cloud service provider) must be governed by a contract with the controller that stipulates a number of obligations set out by the GDPR.

V WHISTLE-BLOWING HOTLINES

The WP29 published an Opinion in 2006 on the application of the EU data protection rules to whistle-blowing hotlines[104] providing various recommendations under the now repealed Directive, which are summarised below. It would be reasonable to expect that the EDPB will issue new guidance on whistle-blowing hotlines to reflect new requirements under the GDPR. For the purposes of this section, references to the Directive should be read as references to the GDPR.

i Legitimacy of whistle-blowing schemes

Under the GDPR, personal data must be processed fairly and lawfully. For a whistle-blowing scheme, this means that the processing of personal data must be on the basis of at least one of certain grounds, the most relevant of which include where:

a the processing is necessary for compliance with a legal obligation to which the data controller is subject, which could arguably include a company's obligation to comply with the provisions of the US Sarbanes-Oxley Act (SOX). However, the WP29 concluded that an obligation imposed by a foreign statute, such as SOX, does not qualify as a legal obligation that would legitimise the data processing in the EU; or

b the processing is necessary for the purposes of the legitimate interests pursued by the data controller, or by the third party or parties to whom the data are disclosed, except where those interests are overridden by the interests or the fundamental rights and freedoms of the data subject. The WP29 acknowledged that whistle-blowing schemes adopted to ensure the stability of financial markets, and in particular the prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing matters and reporting as well as the fight against bribery, banking and financial crime, or insider trading, might be seen as serving a legitimate interest of a company that would justify the processing of personal data by means of such schemes.

104 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, fight against bribery, banking and financial crime.

ii Limiting the number of persons eligible to use the hotline

Applying the proportionality principle, the WP29 recommends that the company responsible for the whistle-blowing reporting programme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct and the number of persons who might be incriminated. However, the recommendations acknowledged that in both cases the categories of personnel involved may still sometimes include all employees in the fields of accounting, auditing and financial services.

iii Promotion of identified reports

The WP29 pointed out that, although in many cases anonymous reporting is a desirable option, where possible, whistle-blowing schemes should be designed in such a way that they do not encourage anonymous reporting. Rather, the helpline should obtain the contact details of reports and maintain the confidentiality of that information within the company, for those who have a specific need to know the relevant information. The WP29 opinion also suggested that only reports that included information identifying the whistle-blower would be considered as satisfying the essential requirement that personal data should only be processed 'fairly'.

iv Proportionality and accuracy of data collected

Companies should clearly define the type of information to be disclosed through the system by limiting the information to accounting, internal accounting control or auditing, or banking and financial crime and anti-bribery. The personal data should be limited to data strictly and objectively necessary to verify the allegations made. In addition, complaint reports should be kept separate from other personal data.

v Compliance with data-retention periods

According to the WP29, personal data processed by a whistle-blowing scheme should be deleted promptly and usually within two months of completion of the investigation of the facts alleged in the report. These periods would be different when legal proceedings or disciplinary measures are initiated. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Personal data found to be unsubstantiated should be deleted without delay.

vi Provision of clear and complete information about the whistle-blowing programme

Companies as data controllers must provide information to employees about the existence, purpose and operation of the whistle-blowing programme, the recipients of the reports and the right of access, rectification and erasure for reported persons. Users should also be informed that the identity of the whistle-blower shall be kept confidential, that abuse of the system may result in action against the perpetrator of that abuse and that they will not face any sanctions if they use the system in good faith.

vii Rights of the incriminated person

The WP29 noted that it was essential to balance the rights of the incriminated person and of the whistle-blower and the company's legitimate investigative needs. In accordance with the Directive, an accused person should be informed by the person in charge of the ethics reporting programme as soon as practicably possible after the ethics report implicating them is received. The implicated employee should be informed about:

a the entity responsible for the ethics reporting programme;
b the acts of which he or she is accused;
c the departments or services that might receive the report within the company or in other entities or companies of the corporate group; and
d how to exercise his or her rights of access and rectification.

Where there is a substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather evidence, then notification to the incriminated person may be delayed as long as the risk exists.

The whistle-blowing scheme also needs to ensure compliance with the individual's right, under the Directive, of access to personal data on them and their right to rectify incorrect, incomplete or outdated data. However, the exercise of these rights may be restricted to protect the rights of others involved in the scheme and under no circumstances can the accused person obtain information about the identity of the whistle-blower, except where the whistle-blower maliciously makes a false statement.

viii Security

The company responsible for the whistle-blowing scheme must take all reasonable technical and organisational precautions to preserve the security of the data and to protect against accidental or unlawful destruction or accidental loss and unauthorised disclosure or access. Where the whistle-blowing scheme is run by an external service provider, the EU controller needs to have in place a data processing agreement and must take all appropriate measures to guarantee the security of the information processed throughout the whole process and commit themselves to complying with the data protection principles.

ix Management of whistle-blowing hotlines

A whistle-blowing scheme needs to carefully consider how reports are to be collected and handled with a specific organisation set up to handle the whistle-blower's reports and lead the investigation. This organisation must be composed of specifically trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations. The whistle-blowing system should be strictly separated from other departments of the company, such as human resources.

x Data transfers from the EEA

The WP29 believes that groups should deal with reports locally in one EEA state rather than automatically share all the information with other group companies. However, data may be communicated within the group if the communication is necessary for the investigation, depending on the nature or seriousness of the reported misconduct or results from how the group is set up. The communication will be considered necessary, for example, if the report incriminates another legal entity within the group involving a high-level member of management of the company concerned. In this case, data must only be communicated under confidential and secure conditions to the competent organisation of the recipient entity, which provides equivalent guarantees as regards management of the whistle-blowing reports as the EU organisation.

VI E-DISCOVERY

The former Article 29 Working Party published a working document providing guidance to controllers in dealing with requests to transfer personal data to other jurisdictions outside the EEA for use in civil litigation[105] and to help them to reconcile the demands of a litigation process in a foreign jurisdiction with EU data protection obligations.

The main suggestions and guidelines include the following:

a Possible legal bases for processing personal data as part of a pre-trial e-discovery procedure include consent of the data subject and compliance with a legal obligation. However, the former Article 29 Working Party states that an obligation imposed by a foreign statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. A third possible basis is a legitimate interest pursued by the data controller or by the third party to whom the data are disclosed where the legitimate interests are not overridden by the fundamental rights and freedoms of the data subjects. This involves a balance-of-interest test taking into account issues of proportionality, the relevance of the personal data to litigation and the consequences for the data subject.

b Restricting the disclosure of data if possible to anonymised or redacted data as an initial step and after culling the irrelevant data, disclosing a limited set of personal data as a second step.

c Notifying individuals in advance of the possible use of their data for litigation purposes and, where the personal data is actually processed for litigation, notifying the data subject of the identity of the recipients, the purposes of the processing, the categories of data concerned and the existence of their rights.

d Where the non-EEA country to which the data will be sent does not provide an adequate level of data protection, and where the transfer is likely to be a single transfer of all relevant information, then there would be a possible ground that the transfer is necessary for the establishment, exercise or defence of a legal claim. Where a significant amount of data is to be transferred, the WP29 previously suggested the use of binding corporate rules or the Safe Harbor regime. However, Safe Harbor was found to be invalid by the CJEU in 2015 and was effectively replaced on 12 July 2016 by the Privacy Shield. In the absence of any updates from the EDPB to the former Article 29 Working Party's e-discovery working document, it can be assumed that the use of Privacy Shield is also an appropriate means of transferring significant amounts of data. It also recognises that compliance with a request made under the Hague Convention would provide a formal basis for the transfer of the data.

It would be reasonable to expect that the EDPB will issue new guidance on e-discovery, in light of the entry into force of Article 48 of the GDPR.

Article 48 of the GDPR facilitates the transfer of personal data from the EU to a third country on the basis of a judgment of a court or tribunal or any decision of an administrative authority of a third country where the transfer is based on a mutual legal assistance treaty (MLAT) between the requesting third country and the EU Member State concerned.[106] As

105 WP 158 – Working Document 1/2009 on pretrial discovery for cross-border civil litigation adopted on 11 February 2009.

106 Article 48 of the GDPR.

MLATs between EU Member States and third countries are not widespread, there is a further exception for data controllers to rely on. The GDPR states that the restrictive requirements in which a judicial or administrative request from a third country to transfer personal data from the EU to that third country is only permissible on the basis of an MLAT, is 'without prejudice to other grounds for transfer' in the GDPR.

Accordingly, this enables controllers in the EU facing e-discovery requests to transfer personal data to a jurisdiction outside of the EU to rely on transfer mechanisms such as EU standard contractual clauses and binding corporate rules. In the absence of a transfer mechanism, the GDPR provides certain derogations for several specific situations in which personal data can in fact be transferred outside the EEA:

a where the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b the transfer is necessary for the performance of a contract between the data subject and the controller;

c the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject;

d the transfer is necessary for important reasons of public interest under EU law or the law of the Member State in which the controller is subject;

e the transfer is necessary for the establishment, exercise or defence of legal claims;

f the transfer is necessary to protect the vital interests of the data subject, where the data subject is physically or legally incapable of giving consent; and

g the transfer is made on the basis of compelling legitimate interests of the controller, provided the transfer is not repetitive and only concerns a limited number of data subjects.[107]

VII EU CYBERSECURITY STRATEGY

The NIS Directive is part of the European Union's Cybersecurity Strategy aimed at tackling network and information security incidents and risks across the EU and was adopted on 6 June 2016 by the European Parliament at second reading.[108]

The main elements of the NIS Directive include:

a new requirements for 'operators of essential service' and 'digital service providers';

b a new national strategy;

c designation of a national competent authority; and

d designation of computer security incident response teams (CSIRTs) and a cooperation network.

i New national strategy

The NIS Directive requires Member States to adopt a national strategy setting out concrete policy and regulatory measures to maintain a high level of network and information security.[109] This includes having research and development plans in place or a risk assessment

107 Article 49 of the GDPR.

108 Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

109 Article 7 of the NIS Directive.

plan to identify risks, designating a national competent authority that will be responsible for monitoring compliance with the NIS Directive and receiving any information security incident notifications,[110] and setting up of at least one CSIRT that is responsible for handling risks and incidents.[111]

ii Cooperation network

The competent authorities in EU Member States, the European Commission and ENISA will form a cooperation network to coordinate against risks and incidents affecting network and information systems.[112] The cooperation network will exchange information between authorities and also provide early warnings on information security risks and incidents, and agree on a coordinated response in accordance with an EU–NIS cyber-cooperation plan.

iii Security requirements

A key element of the NIS Directive is that Member States must ensure public bodies and certain market operators[113] take appropriate technical and organisational measures to manage the security risks to networks and information systems, and to guarantee a level of security appropriate to the risks.[114] The measures should prevent and minimise the impact of security incidents affecting the core services they provide. Public bodies and market operators must also notify the competent authority of incidents having a significant impact on the continuity of the core services they provide, and the competent authority may decide to inform the public of the incident. The significance of the disruptive incident should take into account:

a the number of users affected;
b the dependency of other key market operators on the service provided by the entity;
c the duration of the incident;
d the geographic spread of the area affected by the incident;
e the market share of the entity; and
f the importance of the entity for maintaining a sufficient level of service, taking into account the availability of alternative means for the provisions of that service.

Member States had until May 2018 to implement the NIS Directive into their national laws.

Organisations should review the provisions of the NIS Directive and of any relevant Member State implementing legislation and take steps as applicable to amend their cybersecurity practices and procedures to ensure compliance.

110 Article 8 of the NIS Directive.
111 Article 9 of the NIS Directive.
112 Article 11 of the NIS Directive.
113 Operators of essential services are listed in Annex II of the NIS Directive and include operators in energy and transport, financial market infrastructures, banking, operators in the production and supply of water, the health sector and digital infrastructure. Digital service providers (e.g., e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores) are listed in Annex III. The requirements for digital service providers are less onerous than those imposed on operators of essential services; however, they are still required to report security incidents that have a significant impact on the service they offer in the EU.
114 Article 14 of the proposed NIS Directive.

iv New Cybersecurity Act

In June 2019, the EU Cybersecurity Act[115] (Act) came into force. The Act creates an EU-wide cybersecurity certification scheme for the purposes of ensuring an adequate level of cybersecurity of information and communication technology (ICT) products and services across the EU. The Act introduces a set of technical requirements and rules relating to the production of certifications for ICT devices, or products, ranging from smart medical devices and connected cars to video game consoles and fire alarms. The Act is part of the European Union's push towards a digital single market.

The Act includes a permanent mandate for ENISA as the renamed European Union Agency for Cybersecurity and grants ENISA new powers to provide effective and efficient support to EU Member States and EU institutions on cybersecurity issues and to ensure a secure cyberspace across the EU. In addition, ENISA will be responsible for carrying out product certifications, with certifications voluntary for companies unless otherwise stated in EU or Member State law. The EU wide cybersecurity certification framework for ICT products and services will allow certificates to be issued by ENISA ensuring an adequate level of cybersecurity for the ICT products and services, which will be valid and recognised across all EU Member States, and serve to address the current market and Member State fragmentation in relation to cybersecurity certifications for ICT products and services.

On 26 June 2019, the European Commission released questions and answers on EU cybersecurity that address the certification framework among other things.

VIII OUTLOOK

The GDPR came into force over a year ago and while it appears the immediate panic surrounding it seems to have subsided, the legislation remains a hot topic and one many companies continue to grapple with. The GDPR continues to evolve with new guidance being published at an EU and national level. At the same time there have been a number of enforcement actions and cases dealing with the requirements of the GDPR that companies will need to carefully consider. Dealing with the GDPR has been made more difficult by the lack of consistency in approach taken at a national level by EU Member States and this remains the case in spite of guidance being published by the EDPB at an EU-level.

Many companies are now undertaking a review of the work undertaken in the run-up to May 2018 to assess their GDPR compliance and to re-evaluate certain decisions (GDPR 2.0). International companies are also taking the one-year anniversary as an opportunity to review their broader privacy compliance programmes and so leveraging work undertaken as part of their initial GDPR project to address, for example, the California Consumer Privacy Act of 2018 (CCPA).

Data subjects in the EU have made use of the substantial data protection rights provided by the GDPR at a rapid pace. For example, an airline has been threatened with a £500 million class action lawsuit in a UK court for non-material damage caused by a security breach. The airline has already pledged to cover any losses suffered by its customers, but a law firm acting for some of the affected individuals has taken the position that under the GDPR, the individuals have a right to further compensation of £1,250 each. A steep increase

115 Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No. 526/2013.

in consumers exercising their privacy rights and a growth in privacy litigation is expected this year and the next. We also expect to see an increase in GDPR-related enforcement action as demonstrated by the recent announcements made by the UK's ICO of its intention to fine British Airways £183 million and Marriott £99 million for cyberbreaches.

A further key development in the framework of European data protection and an area to watch is Brexit and the UK's departure from the EU on 31 October 2019 and its attempts to agree on a potential adequacy agreement with the European Commission in relation to the lawful transfer of personal data from the EEA to the UK. This is because on 31 October 2019, the UK may become a third country and if so will face restrictions on any transfer and processing of personal data of EU data subjects from the EEA to the UK.

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.

GÉRALDINE SCALI

Sidley Austin LLP

Géraldine Scali is a counsel in the London office of Sidley Austin LLP, whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

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.

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and leader of Sidley Austin LLP's highly ranked privacy and cybersecurity practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. He also advises companies on

their digital governance strategies and cyber crisis management. Mr Raul's practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chair of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Technology Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves as a member of the American Bar Association's Cybersecurity Legal Task Force by appointment of the ABA president. He is also a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government and Yale Law School.

SIDLEY AUSTIN LLP

Woolgate Exchange
25 Basinghall Street
EC2V 5HA
London
United Kingdom
Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
wlong@sidley.com
gscali@sidley.com
fblythe@sidley.com

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com
www.sidley.com

an LBR business

ISBN 978-1-83862-062-2