IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

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

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 2

EU OVERVIEW

William R M Long, Francesca Blythe, Lauren Cuyvers, Denise Kara, Eleanor Dodding, Matthias Bruynseraede, Subhalakshmi Kumar 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 The GDPR, which repealed the Data Protection Directive 95/46/EC (Directive),[3] regulates the collection and processing of personal data across all sectors of the EU economy and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 protection authorities (DPAs) 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.

A key development in 2023 relates to international transfers and the launch of the EU–US Data Privacy Framework (DPF). In particular, on 10 July 2023, the European Commission issued its Final Implementing Decision granting the US adequacy with respect to companies that subscribe to the EU–US DPF. Importantly, entities relying on SCCs or BCRs are also able to rely on the analysis in the Decision as support for their transfer impact assessments required by the *Schrems II* decision regarding the equivalence of US national security safeguards and redress.

In 2023, the European Data Protection Board (EDPB) adopted and updated various guidelines including on the calculation of administrative fines under the GDPR, on personal data breach notifications under the GDPR, on certification as a tool for data transfers, on the application of Article 65(1)(a) GDPR, on the use of facial recognition technology in the area of law enforcement under the GDPR and a new Data Protection Guide to help SMEs become GDPR compliant, which was a key initiative of the EDPB's 2021–2023 Strategy.

Set out in this chapter is a summary of the main provisions of the GDPR accompanied by commentary regarding guidance provided by the EDPB and by its predecessor, the EU's

1 William R M Long, Francesca Blythe and Alan Charles Raul are partners, Lauren Cuyvers, Denise Kara and Eleanor Dodding are senior managing associates, Matthias Bruynseraede is a managing associate and Subhalakshmi Kumar is an 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.

former Article 29 Working Party (WP29) (which, since 25 May 2018 was replaced by the EDPB). At the end of this chapter, we address some topical issues on cloud computing, cybersecurity obligations and whistle-blowing hotlines.

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 final guidance on the territorial application of the GDPR on 12 November 2019. The guidance largely reaffirms prior interpretations, which were complemented by more recent EDPB guidelines on the interplay between the application of Article 3 on the territorial scope of the GDPR with the provisions on international transfers as per Chapter V (international transfers) of the GDPR which is discussed in more detail in Section II.iv.

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 decision in 2018 from the Court of Justice of the European Union (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.[6]

4 EDPB Guidance on controllers and processors, pp. 26–27.

5 Recital 22 of the GDPR.

6 CJEU, *SRB v. EDPS*, T-557/2.

Unfortunately the ruling does not address the question of liability between the parties. This decision was reaffirmed in EDBP Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Guidance on controllers and processors). Currently, case C-683/21 with preliminary questions to clarify the concepts of (joint) controllers, processors and administrative fines is pending before the CJEU. The Advocate General's (AG) Opinion, issued on 4 May 2023, is consistent with the Guidance on controllers and processors and further argues that a controller can be fined if a processor intentionally or negligently breaches the GDPR, if the processor acted in accordance with the controller's instructions, irrespective of whether the controller itself processed the personal data;[7]

b processor: a natural or legal person who processes personal data on behalf of the controller: in the Guidance on controllers and processors, the EDPB recalls that not every 'service provider' that processes personal data in the course of delivering a service is a 'processor' within the meaning of the GDPR. The EDPB considers that the categorisation of 'processor' does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. The EDPB reminds that a case-by-case analysis is necessary to ascertain the degree of influence each entity effectively has in determining the purposes and means of the processing;[8]

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

d establishment: the effective and real exercise of activity through stable arrangements in a Member State;[9]

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 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. However, in April 2023, the General Court of the EU held in case T-557/20 (*SRB v. European Data Protection Supervisor* (EDPS)) that pseudonymised data transmitted to a data recipient will not be considered personal data if the data recipient does not have the means to re-identify the data subjects. If the recipient of the data does not hold information enabling it to re-identify the individuals and has no legal means available to access such information (regardless whether the sender has these re-identification means at their disposal), the data can be considered

7 Advocate General's Opinion, C-683/21, ECLI:EU:C:2023:376, paragraph 97.

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

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

anonymous data and will therefore, not be subject to the requirements of the GDPR. However, the EDPS has appealed the judgment, and this is currently pending before the EU Court of Justice; 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 requirements that existed previously under the Directive have been replaced under the GDPR by an obligation to maintain a record of 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 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.

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: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;[10]

b the purpose limitation principle: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;[11]

c data minimisation principle: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;[12]

d accuracy principle: 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 is inaccurate in relation to the purposes for which it is processed is erased or rectified without delay;[13]

e storage limitation principle: 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 is processed;[14]

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

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

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

13 WP29, 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, p. 6.

14 id., pp. 9–11.

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

Article 35(1) of the GDPR imposes an obligation on controllers to conduct a data protection impact assessment (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 that is based on automated processing, including profiling, and produces legal effects concerning the data subject or similarly significantly affecting the data subject;

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 DPA 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 DPA 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.[15]

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[16] 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 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, which 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. This personal data is 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 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;

15 WP29, 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, p. 6.

16 id., pp. 9–11.

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;

h innovative use or applying new technological or organisational solutions; for example, combining use of fingerprint 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; and

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 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.[17] In practice, this means controllers are required to continuously assess the risks created by their processing activities 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.[18]

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 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.

17 id., p. 6.

18 id., p. 14.

In October 2020, the EDPB published its final guidelines on data protection by design and by default.[19]

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 Guidelines on Data Protection Officers, noted that 'core activities' can be considered key operations[20] 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 '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.[21]

DPOs must be appointed on the basis of their professional qualities and expert knowledge of data protection law and practices.[22] 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.[23]

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 the DPA.[24]

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.[25] The DPO can hold another position but must be free from a conflict of interests, meaning that the position cannot lead him or her to determine the purposes and the means of the data processing. For example, the DPO could not hold a position within the controller

19 EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default adopted on 20 October 2020.

20 WP29, Guidelines on Data Protection Officers (DPOs), WP 243, as last revised and adopted on 5 April 2017, p. 20.

21 id., p. 7.

22 Article 37(5) of the GDPR.

23 WP29 Guidelines on Data Protection Officers (DPOs), WP 243, as last revised and adopted on 5 April 2017, p. 12.

24 Article 37(7) of the GDPR.

25 CJEU, X-FAB Dresden, C-453/21, ECLI:EU:C:2023:79; Icelandic DPA, 4 August 2022, Case 2020061979, original only available in Icelandic, accessible at https://www.personuvernd.is/urlausnir/akvordun-um-stodu-personuverndarfulltrua-landspitala; Italian DPA, 9 June 2022, Case 9794895, original only available in Italian, accessible at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9794895.

organisation that determined the purposes and means of data processing, such as the head of marketing, IT or human resources or the chief executive, chief operating, chief financial or chief medical officer. Recent EU and EU Member State case law confirm these principles and even held that a conflict of interest existed for DPOs that were also appointed as defence counsel or board member.

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 DPA; and

e act as the contact point for the DPA on issues concerning processing.[26]

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.[27]

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.[28] In 2020[29] and 2021,[30] the Belgian DPA reiterated the position that a DPO appointment should account for possible conflicts of interest as per the EDPB guidance on DPOs. Both the decisions laid down certain conditions for the organisations, which should be kept in mind while appointing a DPO and considering whether there is a conflict of interest:

a the positions should be identified which could be incompatible with the function of DPO;

b the internal rules should be drawn out to avoid conflicts of interests;

c the entire organisation should be informed that the DPO has no conflict of interests with regard to their function as a DPO; and

d it should be ensured that the job description of the DPO is sufficiently specified and detailed, even if this position is normally filled internally.

26 Recital 97 of the GDPR.

27 Article 39 of the GDPR.

28 Article 37(4) of the GDPR.

29 WP29 Guidelines on Data Protection Officers (DPOs), WP 243, as last revised and adopted on 5 April 2017, p. 5.

30 APD/GBA – AH-2019-0013 (Belgium), original only available in French, accessible at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf.

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 final guidance on this lawful ground in April 2019 (later updated in October 2019) in which a very narrow interpretation of contractual necessity was adopted;[31]

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.[32]

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.[33] 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

31 APD/GBA – DOS-2020-03763 (Belgium), original only available in Dutch, accessible at https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-141-2021.pdf.

32 EDPB Guidelines 2/2019 on the processing of persona data until Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, adopted 9 October 2019 (version 2.0).

33 Article 6 of the GDPR.

accepting or declining the terms offered or declining them without negative effects.[34] 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.[35]

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 DPA; 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 is 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.[36] 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.[37] These exceptions, according to the EDPB should be interpreted narrowly.[38]

34 WP29, Guidelines on consent under Regulation 2016/679, WP259, as last revised and adopted on 10 April 2018, p. 3. EDPB Guidelines 05/2020 on consent under Regulation 2016/679 adopted 4 May 2020, (Version 1.1), p. 5.
35 ibid.
36 ibid.
37 Article 14(3) of the GDPR.
38 Article 14(5) of the GDPR.

The EDPB notes that, 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.[39]

EU data protection authorities are becoming increasingly strict in applying Articles 13 and 14 of the GDPR in turn, requiring controllers to make more granular disclosures. For example, the legal bases should be aligned with the processing purposes and the categories of personal data processed.

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.[40] 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.[41] Further, the EDPB in its Controller and Processors Guidance makes clear that entering into a data processing agreement should not be a 'pro-forma' exercise of restating the provisions of the GDPR. The data processing agreement should contain the specific details on how the requirements will be met and the level of security for the processing. The EDPB adds that the contract should take into account 'the specific tasks and responsibilities of the processors' and that 'there is no need to impose particularly stringent protections and procedures' where only minor risks to the rights and freedoms of the data subject are relevant.[42]

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, unauthorised 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,[43] 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

39 WP29 Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018, p. 25.

40 id., p. 7.

41 Article 32 of the GDPR.

42 Article 28(4) of the GDPR.

43 EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 7 July 2021 (version 2.0), p. 34.

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 DPA 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, without undue delay. 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 DPA.

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.[44] 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.[45] 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.[46]

In 2021, the EDPB published complementary guidance on examples regarding personal data breach notifications. This guidance provides specific examples of personal data breaches and whether or not they should be notified to DPAs or affected data subjects. It further provides guidance on the type of technical and organisational measures an organisation can implement to prevent and mitigate such breach.[47]

Exceptions

Controllers are exempted from notifying a personal data breach to the relevant DPA if they are 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: whether the breach involves a compromise in the confidentiality, availability, or integrity of the personal data.

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 is 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 is involved in a breach, the potential damage to data subjects can be severe and thus the risk may be higher.

44 WP29 Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP 250, as last revised and adopted on 6 February 2018, p. 12.

45 ibid.

46 ibid.

47 EDPB Guidelines 01/2021 on Examples regarding Personal Data Breach Notification.

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 is 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 that may help with designing breach management response plans.[48]

Notifying affected data subjects

In addition to notifying the relevant DPA, 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 DPAs, taking account of the risk factors listed above.

The data protection principles 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 is collected and retained, to ensure that the data is 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 processors may not transfer personal data to countries outside of the EEA[49] unless the recipient country provides an adequate level of protection for the personal data.[50] 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 (commercial organisations), the Faroe Islands, Guernsey, the Isle of Man, Israel, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, the United States (organisations that have self-certified to the EU–US Data Privacy Framework) and Uruguay.

Importantly, on 16 July 2020, in the *Schrems II* case, the CJEU invalidated the Privacy Shield. According to the CJEU, the alleged lack of effective judicial or other independent

48 DPB Guidelines on Personal data breach notification under Regulation 2016/679, p. 26, https://ec.europa.eu/newsroom/article29/items/612052.

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

50 Article 45 of the GDPR.

redress for EU residents regarding the data collection and surveillance activities by US national security agencies materially diminished the privacy protections afforded to individuals whose personal data had been transferred to the US by organisations that had certified to the Privacy Shield programme. In turn, the CJEU concluded that the privacy protections afforded to individuals under the Privacy Shield programme were not 'essentially equivalent' to privacy rights afforded to such individuals under EU law. Accordingly, organisations that were relying on their Privacy Shield certification (including data transfers to affiliates, customers and vendors) needed to identify and implement an appropriate alternate legal transfer mechanism (for example, Standard Contractual Clauses (SCCs), binding corporate rules, or perhaps even reliance on informed consent from relevant data subjects or other exemptions under the GDPR, such as for performance of a contract).[51]

Separately, although the *Schrems II* decision did uphold the use of SCCs for purposes of international transfers from the EEA to non-EEA countries, organisations relying on SCCs are now required to carry out a transfer privacy impact assessment that, among other things, assesses whether any laws governing access to personal data in the recipient country impacts the protections provided in the SCCs. Where this assessment reveals that such laws impact the protections provided in the SCCs, organisations will need to consider whether supplementary measures in addition to the protections in the SCCs will need to be implemented. Such supplementary measures are intended to ensure an essentially equivalent level of data protection to that guaranteed in the EEA.

On 18 June 2021, the EDPB issued its long-awaited practice guidance on measures that supplement transfer tools to ensure compliance with the EEA level of protection of personal data. Organisations using SCCs to transfer personal data to a country that has not been deemed to provide an adequate level of data protection will need to carry out a six-step assessment to determine, taking account the circumstances of the transfer, whether they need to implement supplementary measures to ensure that the law of the recipient country does not impinge on the level of protection guaranteed by the SCCs. Where such assessment reveals that appropriate safeguards would not be ensured, organisations are required to suspend transfers of personal data or notify the relevant data protection authority that it wishes to continue transferring data.

Previously, there were two forms of SCCs: 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. The European Commission, on 4 June 2021, adopted a new set of SCCs for international data transfers to take into account the *Schrems II* decision and to align more closely with the requirements under the GDPR.[52] The new SCCs are required to be implemented into new agreements from the repeal date, being 27 September 2021, and organisations can continue to rely on the previous SCCs in existing agreements concluded prior to 27 September 2021 for 15 months following this date (i.e., essentially a transition period of 18 months). The new SCCs take a modular approach to accommodate the diversity of transfer scenarios and now address the following four data transfers: controller to controller; controller to processor; processor to processor; and processor to controller.

51 Article 46 of the GDPR.

52 Commission Implementing Decision (EU) 2021/914 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, https://eurlex.europa.eu/eli/dec_imp/2021/914/oj?uri=CELEC:32021D09&locale=en.

To address certain requirements arising from the *Schrems II* decision, the parties to the new SCCs are to provide a warranty that they have no reason to believe that the laws and practices applicable to the data importer, including any requirements around disclosure to, or access by, public authorities, prevent the data importer from complying with the new SCCs. In giving this warranty, the parties must carry out a transfer privacy impact assessment, taking into account the circumstances of the transfer, the laws and practices in the recipient third country and any supplementary measures implemented.

The new SCCs are expected to be included in a broader commercial contract and additional clauses can be added provided these do not contradict the new SCCs or prejudice the rights of data subjects.

On 25 May 2022, the European Commission published its 'Questions and Answers for the Two Sets of Standard Contractual Clauses'. This clarified some practical aspects for businesses looking to implement the SCCs. For example, the European Commission confirmed that: (1) the SCCs can be incorporated by reference; and (2) the names of the subprocessors should be made known to the controller. The SSCs FAQs also stated that the SCCs are not intended to be used for data transfers to controllers or processors whose processing operations are directly subject to the GDPR, and the European Commission is in the process of developing an additional set of SCCs for this scenario.[53]

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 DPA as providing adequate data protection for transfers of personal data throughout the group. The EDPB has published various documents[54] on binding corporate rules, including a model checklist for the approval of binding corporate rules,[55] a table setting out the elements and principles to be found in binding corporate rules,[56] an explanatory document on processor binding corporate rules, recommendations on the standard application for approval of controller and processor binding corporate

53 id., p. 3.

54 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.

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

56 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.

rules,[57] a cooperation 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. Entities relying on binding corporate rules are still required to carry out a *Schrems II* transfer privacy impact assessment in accordance with EDPB guidance.

Most recently, on 10 July 2023, the European Commission issued its Final Implementing Decision granting the US adequacy with respect to companies that subscribe to the EU–US Data Privacy Framework (DPF). This Decision reflects the European Commission's opinion that the US data protection safeguards set out in Executive Order 14086 on Enhancing Safeguards for US Signals Intelligence Activities address the issues raised by the CJEU in *Schrems II*, including the need for greater limitations and safeguards of surveillance activities and an independent redress mechanism.[58] With regard to the latter, complaints will be initially filed through the appropriate EEA jurisdiction for the individual (i.e., via the DPA), and then transmitted to the US by the EDPB. In the US, there will first be an investigation by the ODNI Civil Liberties Protection Officer followed by the possibility of appeal to the newly created Data Protection Review Court.

The DPF is not one-sided. In satisfaction of the Executive Order, the attorney general has designated the EU/EEA as 'qualifying states' following a detailed legal analysis. This means that they provide appropriate safeguards for US personal data obtained by European national security agencies after the data is transferred to the EU/EEA, and that the EEA countries will permit the transfer of EU personal data to the US for commercial purposes.

The DPF Principles which companies self-certifying to the DPF are required to comply with are substantively the same as the Privacy Shield Principles. This continuity seems appropriate given that the concerns raised in *Schrems II* concerned only national security surveillance and did not take issue with the Privacy Shield Principles. Companies that have maintained their membership in the Privacy Shield will automatically and immediately be part of the DPF. Such Privacy Shield companies will have three months to make conforming changes to reflect references to the DPF in their various relevant policies and other materials. Non-Privacy Shield members that now want to join the DPF, will go through a process that closely tracks the prior Privacy Shield process. This will include drafting an appropriate privacy policy, selecting and identifying a recourse mechanism and self-certifying (after undertaking an appropriate, internal conformity assessment to assure compliance with the DPF Principles). As with the Privacy Shield, the DPF is only available to entities that are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation. Further, whilst 'full adequacy' can only be obtained by self-certification to the DPF, according to the European Commission, companies transferring personal data from the EU to the US are now able to rely on the decision for the US country assessment, when using SCCs or BCRs as the data transfer mechanism.

57 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.

58 European Commission Implementing Decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

In addition to the data transfer solutions identified above, the transfer of personal data outside of the EEA can occur via the use of approved codes of conduct or certification mechanisms or in reliance on a derogation under Article 49 of the GDPR.

Also, the EDPB has published guidelines on the interplay between the application of Article 3 on the territorial scope of the GDPR with the provisions on international transfers as per Chapter V (international transfers) of the GDPR. The new guidance provides a definition of 'transfer' (which is not present in the GDPR), which is any processing that satisfies the following three cumulative criteria:

a a controller/processor is subject to the GDPR for a given processing ('exporter');
b the exporter discloses to another controller/processor/joint controller ('importer'); and
c the importer is located in a third country or is an international organisation, irrespective if the recipient is already subject to the GDPR under Article 3.

Additionally, the EDPB clarifies that if the exporter and the importer are the same entity (e.g., company and its branch) the disclosure should not be regarded as a transfer (i.e., the branch is not a different entity from the company) meaning that the disclosure will not be subject to the international data transfer requirements under Chapter V of the GDPR, but the controller is still accountable for the associated risks of the processing.

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 DPA 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 DPA;

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.

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.[59] The EDPB notes in its guidance on the right of access, which was adopted on 28 March 2023, that the term 'other's' shall also include the controller itself, meaning that the controller can limit its response to an access request on the basis of adverse effects to its own rights (e.g., protection of controller's trade secrets).[60] 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 other individual's personal data, and the rights of the controller and in particular, the controller's 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.[61] 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.[62] The EDPB highlights in its draft guidelines on the right of access that controllers have to assess each request and the respective context on a 'case by case basis' to determine if the request is manifestly unfounded or excessive. In particular, the guidelines emphasise that the 'manifestly unfounded' exemption has a 'very limited scope' essentially covering cases where the requirements of Article 15 of the GDPR are 'clearly and obviously not met'. Further, the EDPB interprets a request as being excessive 'as being linked to the quantity of requested' or 'repetitive' but does not exclude other causes for being considered 'excessive', irrespective of the number of requests.[63]

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.[64]

59 Article 15(4) of the GDPR.

60 EDPB Guidelines 01/2022 on data subject rights – Right of access, version 2, p. 51.

61 Recital 63 of the GDPR.

62 Article 12(5) of the GDPR.

63 EDPB Guidelines 01/2022 on data subject rights – Right of access, p. 53.

64 Article 12(6) of the GDPR.

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 his or her personal data.[65]

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 where the controller:

a is able to demonstrate that the data subject's request for rectification of their personal data they hold is manifestly unfounded or excessive because of its repetitive nature, it can refuse to comply with the data subject's request;[66]

b has reasonable doubts concerning the identity of the data subject making the request, it can request the provision of additional information necessary to confirm the identity of the data subject;[67] and

c 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.[68]

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 is no longer necessary for the purposes for which it is collected;[69]

b the data subject withdraws consent to the processing and there is no other legal ground to rely upon for the processing;[70]

c the data subject objects to the processing and there are no overriding legitimate grounds for the processing;[71]

d the personal data has been unlawfully processed;[72]

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;[73] and

f the personal data has been collected in connection with an online service offered to a child.[74]

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;

65 Article 12(2) of the GDPR.
66 Article 12(5) of the GDPR.
67 Article 12(6) of the GDPR.
68 Article 12(2) of the GDPR.
69 Article 17(1)(a) of the GDPR.
70 Article 17(1)(b) of the GDPR.
71 Article 17(1)(c) of the GDPR.
72 Article 17(1)(d) of the GDPR.
73 Article 17(1)(e) of the GDPR.
74 Article 17(1)(f)) of the GDPR.

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;[75]

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;[76] 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 the data subject's request to access his or her personal data.[77]

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 the restriction of the processing;

c the controller no longer needs the personal data for the purposes of the processing, but it is 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 the 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;[78]

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;[79] and

75 Article 12(5) of the GDPR.

76 Article 12(6) of the GDPR.

77 Article 12(2) and Article 17(3) of the GDPR.

78 Article 12(5) of the GDPR.

79 Article 12(6) of the GDPR.

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 his or her personal data.[80]

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'.[81]

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.[82]

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

a that the right applies to personal data provided by the data subject, whether knowingly and actively as well as the personal data generated by his or her activity;[83]

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);[84] and

c the right is not restricted to data communicated by the data subject directly.[85]

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 (the 'general right to object');

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

80 Article 12(2) of the GDPR.

81 WP29, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), p. 16.

82 WP29, Guidelines on the right to data portability, WP 242, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017), p. 3.

83 id., p. 10.

84 ibid.

85 id., p. 3.

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'.

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

a where the controller can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or where the processing is necessary for the establishment, exercise or defence of legal claims;[86] 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.[87]

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 and 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 incident 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 SCCs or other data transfer solutions and as necessary a transfer impact assessment, as a means to comply with the *Schrems II* decision;

n a 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;

86 Article 21(1) of the GDPR.

87 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' mechanism 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

DPAs, lead DPAs and the 'one-stop shop' mechanism

The GDPR is enforced at an EU Member State level by national or state DPAs. One of the aims of the GDPR is to enable a controller or processor engaging in cross-border processing of personal data across different EU Member States to only deal with one lead DPA. As a result, DPAs have a duty to cooperate on cases with a cross-border component to ensure a consistent application of the GDPR. This is 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 DPA 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 DPAs 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.

Where a controller is engaging in cross-border processing, it will need to identify its 'main establishment'. If a controller has establishments in more than one Member State, its main establishment will be the place of its 'central administration' which is where decisions on the purposes and means of the processing are made. To the extent that the decisions on the purposes and means of the processing are taken in an establishment other than the place of its central administration, the controller's main establishment will be taken to be that establishment.[88]

88 Article 4(16) of the GDPR.

Similarly, a processor's 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 EU, the main establishment will be where its main processing activities are undertaken. The EDPB, in its guidance on lead DPAs, makes it clear that the GDPR does not permit 'forum shopping'[89] and that where a company does not have an establishment in the EU, the 'one-stop shop' mechanism does not apply. In these cases, the relevant organisation must deal with DPAs in every EU Member State in which it is active.[90]

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

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

b data subjects in the concerned DPA's Member State are, 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 DPA.[91]

In the case of a dispute between DPAs, the EDPB shall adopt a final binding decision.[92] In this regard, the EDPB adopted guidelines[93] in May 2023 to clarify the competence of the EDPB and the main stages of the procedure when adopting a legally binding decision. The guidelines include a description of the application procedural safeguards and remedies. The GDPR also promotes cooperation among Member State DPAs by requiring the lead DPA to submit a draft decision on a case to the concerned DPA, where they will have to reach a consensus prior to finalising any decision.[94]

On 4 July 2023, the European Commission proposed a new regulation to streamline cooperation between, and procedural rules in, Member State DPAs when enforcing the GDPR in cross-border cases (Proposed Regulation on Cross-Border Cases). The Proposed Regulation on Cross-Border Cases lays down procedural rules for the handling of complaints filed by individuals in relation to the processing of their personal data; and the conduct of investigations by DPAs in the cross-border enforcement of the GDPR. Among other things, the Proposed Regulation on Cross-Border Cases provides: (1) the information to be included in an individual complaint in order to be valid; (2) the key circumstances to be taken into account when investigating a complaint; (3) procedural rights for the individual who filed the complaint; (4) amicable settlement procedural rules following a complaint and rules around translations of the complaint; (5) procedural rules around cooperation between the lead DPA and other concerned DPAs and information-sharing obligations; and (6) procedural rules for controllers and processors involved in a DPA investigation – including the right to access to

89 WP29, Guidelines for identifying a controller or processor's lead data protection authority, WP244, adopted on 13 December 2016 and revised on 5 April 2017, p. 8.

90 id., p. 10.

91 Article 4(22) of the GDPR.

92 Article 65(1) of the GDPR.

93 EDPB, Guidelines 03/2021 on the application of Article 65(1)(a) GDPR, https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_202103_article65-1-a_v2_en.pdf.

94 Article 60 of the GDPR.

the file, the right to be heard and file written submissions in response to a DPA's preliminary findings, and rules around confidentiality for documents obtained by a DPA in the context of a GDPR investigation.[95]

The CJEU addressed the effect of the application of the 'one-stop shop' mechanism under the GDPR in a recent high-profile decision. The CJEU, in handing down its judgment, outlined that, under certain conditions, a national DPA may exercise its power to bring any alleged infringement of the GDPR before a court of a Member State, despite that DPA not being the lead DPA with regard to the processing in the circumstances. Moreover, the CJEU addressed the conditions governing whether a national DPA, which does not have the status of a lead DPA in relation to an instance of cross-border processing, must exercise its power to bring any alleged infringement of the GDPR before a court of a Member State and, where necessary, to initiate or engage in legal proceedings to ensure the application of the GDPR. In addition, the CJEU outlined that the lead DPA, when exercising its competencies under the 'one-stop shop' mechanism, may not ignore the views of the other DPAs, and confirmed that any relevant and reasoned objection made by one of the other DPAs has the effect of blocking the adoption of the draft decision of the lead DPA.[96]

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 DPAs. The EDPB comprises representatives from all EU DPAs, the EDPS, 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 GDPR came into force, the EDPB has been active in publishing guidance to greater assist companies subject to the GDPR to interpret and apply the GDPR's requirements, and, for the most part, this guidance has been well received by such companies. In addition to guidance published by the WP29 on the GDPR (which have been formally endorsed by the EDPB,[97] the EDPB has finalised guidelines on various aspects of the GDPR, including on codes of conduct and certification mechanisms, the interplay between the territorial scope of the GDPR and its international transfers' framework, personal data breach notification obligations, the right of access, facial recognition technology in the area of law enforcement, the use of virtual voice assistants, and dark patterns on social media.

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

95 European Commission, Proposal for a Regulation laying down additional procedural rules relating to the enforcement of GDPR, https://commission.europa.eu/publications/proposal-regulation-laying-down-additional-procedural-rules-relating-enforcement-gdpr_en.

96 *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA v. Gegevensbeschermingsautoriteit* (Case C-645/19).

97 EDPB, EDPB endorses WP29 GDPR guidelines statement, https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en.pdf.

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 DPAs 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 protection authorities, respectively.[98]

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 worldwide turnover, whichever is the greater.[99] 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. In

98 Article 83(4) of the GDPR.

99 Article 83(5) of the GDPR.

an effort to harmonise the methodology DPAs use to calculate fines for infringements of the GDPR, the EDPB has recently adopted guidance detailing the five steps to be followed by DPAs in this regard:

a step 1: the DPA should identify the processing operation and apply the CJEU case-law on the rules on concurrences violation (i.e., apply the relevant rules to determine how many infringements are in scope in an enquiry and what is the total amount of the administrative fine applicable, which cannot exceed the maximum amount for the most severe infringement).

b step 2: determine the 'starting point for calculation' (i.e., determine the nature, gravity and duration of the infringement, assess whether the entity acted intentionally or negligently, determine the categories of personal data affected and analyse the role of the undertaking to determine an effective, dissuasive and proportionate fine).

c step 3: take into account the aggravating and mitigating circumstances, such as past and present behaviour of the controller/processor, degree of responsibility, previous engagements, which may increase or decrease the fine's total amount.

d step 4: identify the maximum applicable amounts for imposing fines, on the basis of the undertaking's turnover in the preceding year.

e step 5: assess if the final amount of the calculated fine meets the requirements of 'effectiveness, proportionality and dissuasiveness', namely for the purposes of determining proportionality, taking into consideration the undertaking's economic viability, the proof of value loss and the specific social and economic context.

While these guidelines are not targeted towards organisations, organisations who are subject to penalties may find it useful to determine whether the correct methodology was used by a DPA in calculating fines.

DPAs' investigative powers

DPAs 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.

DPAs are not limited to enforcement and investigative powers, but also have corrective[100] and authorisation and advisory[101] powers.

DPAs' corrective powers

Article 58(2) of the GDPR grants DPAs 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 their intended processing operations are likely to infringe provisions of the GDPR;

100 Article 58(2) of the GDPR.

101 Article 58(3) 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.

DPAs' authorisation and advisory powers

DPAs 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.

viii 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 healthcare services, which reveal information about his or her health status'.[102]

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

102 Article 4(15) of the GDPR.

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.[103]

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.

The European Commission, on 3 May 2022, published its proposal for a European Health Data Space (EHDS) Regulation.[104] The draft Regulation – which is expected to come into force, at the earliest, in 2024 and be complementary to the GDPR – seeks to: (1) provide individuals with increased control over, and access to, their electronic health data (EHD); (2) enable the secure cross-border sharing of such EHD between healthcare professionals; and (3) facilitate the trustworthy and secure sharing of EHD for secondary research purposes. As it relates to secondary research, the draft Regulation requires companies processing EHD (data holders) to – on request from a national health data access body (HDAB) – make this data available to other companies (data users) for prescribed purposes (including scientific research and the training and testing of algorithms including as found in AI systems and medtech devices). The access by the data user is, however, subject to the data user having applied for and received a permit from a national HDAB to access the EHD. Upon receipt of a request to disclose EHD, a data holder will have just two months to comply with the request (i.e., convert the EHD into the desired format and upload it onto an interoperable decentralised platform) or otherwise potentially face a fine.

The EDPB and the EDPS have published a joint opinion regarding the draft Regulation and have in particular raised a concern that as drafted, certain of the provisions do not entirely align with the requirements of the GDPR (e.g., the data subject rights granted to individuals under the draft Regulation overlap with the GDPR rights which in turn, may cause legal uncertainty).[105]

ix Artificial intelligence

On 14 June 2023, the EDPB and European Parliament issued a revised version of the draft proposal laying down harmonised rules on artificial intelligence (the AI Act).[106] Following this vote, discussions between the Member States, the Parliament and the Commission (the

103 Recital 35 of the GDPR.

104 Proposal for a Regulation Of The European Parliament And Of The Council on the European Health Data Space, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEXw3A52022PC0197.

105 EDPB and EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf.

106 Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) accessible at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf.

'trilogue') have commenced. It is expected that the AI Act could be adopted by early 2024 and will formally apply from around 2026. There are a number of key amendments which should be noted, including:

a a revised definition of 'AI systems', which is more closely aligned with that of the Organisation for Economic Cooperation and Development (OECD) as 'a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations or decisions that influence physical or virtual environments';

b higher fines of up to €40 million or, if the offender is a company, 7 per cent of the company's total worldwide turnover, for the most serious infringements. The application and interpretation of the AI Act would be overseen from a consistency perspective by the (new) European Artificial Intelligence Office, whose formation, tasks and competencies mimic those of the EDPB. This new European Artificial Intelligence Office will primarily have advisory powers, and national authorities (to be established by the EU Member States) will be tasked with enforcing the AI Act;

c the amended text now also applies to AI foundation (including generative AI) models and defines an AI 'foundation model' as: 'an AI system model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks', a subset of AI foundation models known as 'generative AI' has also been defined to mean: 'foundation models used in AI systems specifically intended to generate, with varying levels of autonomy, content such as complex text, images, audio, or video'. Interestingly, foundation (including generative) AI systems will not be considered to pose an 'unacceptable-risk' or 'high-risk' by default. However, Article 28b of the revised AI Act sets out specific legal requirements to which all foundation AI providers must comply. The key requirements include demonstrating that quality datasets are relied on by AI systems, and a requirement to document and register foundational AI models in an EU database. Generative AI model providers will have to meet additional obligations on top of those that foundational AI model providers must meet, including in relation to user transparency and testing of AI output; and

d the European Parliament has also proposed significant changes to the list of systems categorized as 'high-risk' AI systems under the AI Act, including the addition of AI systems intended to be used by social media platforms that have been designated as 'very large online platforms' in their recommender systems under the EU Digital Services Act. Further, the list of prohibited systems has changed; for example, now AI systems that create or expand facial recognition databases through untargeted scraping and emotion recognition in areas such as law enforcement, border control and employment or education are banned.

Importantly, this new text does make certain amendments in line with the EDPB and the EDPS's proposed recommendations regarding the AI Act, as published in its joint opinion on the European Commission's draft proposal of the AI Act. These amendments include a new article that bans the placing on the market, putting into service or use of biometric categorisation systems that categorise natural persons according to sensitive or protected attributes or characteristics or based on the inference of those attributes or characteristics, in line with the EDPB and EDPS recommendation to ban AI systems using biometrics to categorise individuals into clusters based on ethnicity, gender, political or sexual orientation or other grounds on which discrimination is prohibited under Article 21 of the Charter of

Fundamental Rights. Further, the Parliament has maintained the ban on the use of 'real-time' remote biometric identification systems in publicly accessible spaces, which may be seen as a move to address the EDPB and the EDPS recommendation, to ban any use of AI for automated recognition of human features in publicly accessible spaces.

III DIRECT MARKETING AND PRIVACY

The EU Privacy and Electronic Communications Directive 2002/58/EC (ePrivacy Directive) imposes requirements in relation to the use of personal data for unsolicited direct marketing sent to EU individuals. 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 in principle needs to have the prior opt-in consent of the recipient. However, in the case of emails, there are limited exceptions for email marketing to existing customers where, if certain conditions[107] 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 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).[108] Being an EU directive, the ePrivacy Directive is not directly applicable in EU Member States but has to be implemented into EU Member State domestic law. As a result, the requirements described in this section vary from one EU Member State to another. 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.[109] The ePrivacy Directive was also amended in 2009[110] 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 or gaining access to information stored in the users' equipment. 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 provision of an information society service explicitly requested by the subscriber or user.[111]

The WP29 published an opinion on the cookie consent exemption[112] 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). The WP29 Opinion

107 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.

108 Article 13(3) of the ePrivacy Directive.

109 Recital 20 and Article 4 of the ePrivacy Directive.

110 Directive 2009/56/EC.

111 Article 5(3) of the ePrivacy Directive.

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

dates back to 2012, and DPAs in various EU Member States have since issued (diverging) guidance on when and how cookie consent must be obtained.[113] This has been and remains a key area of focus for certain DPAs from an enforcement perspective and privacy activists. For example, in September 2021 the EDPB established a cookie banner taskforce to coordinate response to complaints concerning cookie banners filed with several EU DPAs. This resulted in a report of the work undertaken by the taskforce being adopted in January 2023.[114] The report sets out the EDPB's assessment of various cookie banner practices including no reject button on the first layer and pre-ticked boxes.

In July 2016, the WP29 issued an opinion on a revision of the rules contained in the ePrivacy Directive.[115]

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.[116] The ePrivacy Regulation will complement the GDPR and provide additional sector-specific rules, including in relation to marketing and the use of website cookies. Whereas the ePrivacy Directive's legal framework is still fairly fragmented because of the national implementation requirements, the ePrivacy Regulation aims to provide a harmonised legal framework that is directly applicable throughout the EU.[117]

The current draft of the ePrivacy Regulation has a number of notable elements, including, among other things, the following: (1) it requires a clear affirmative action to consent to cookies except in a number of limited exceptions (which are broader than the ones foreseen in the ePrivacy Directive[118]); (2) it aligns the consent standard with the consent standard of the GDPR; and (3) it explicitly covers interpersonal communications services such as over-the-top communication services.

The European Commission's original timetable for the ePrivacy Regulation was for it to apply in EU law and have direct effect in Member State law from 25 May 2018, coinciding with the GDPR's entry into force. On 3 June 2020, the Presidency of the Council of European Union published a progress report indicating that substantial progress on the draft ePrivacy Regulation has been as limited as a result of the covid-19 pandemic.[119] This was followed by another progress report on 23 November 2020 which among other things, considered the text too restrictive towards innovation and that it is clear from Member States' reaction that further

113 For example: The French Data Protection Authority issued a recommendation (Déliberation No. 2019-093; rectified) with guidelines regarding the application of Article 82 of the French Data Protection Act of 6 January 1978 to read or write operations in terminals of users (in particular to cookies and other trackers) (original in French).

114 EDPB, Report of the work undertaken by the Cookie Banner Taskforce, https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

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

116 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), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

117 An EU regulation has direct effect in EU Member States' legal orders and does not require implementation into national law.

118 For instance, the use of cookies for IT security, web analytics and software updates would not require the user's prior consent.

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

work is needed on the file.[120] Further iterations of the ePrivacy Regulation were published by the Portuguese presidency on 5 January and 10 February 2021.[121] On 28 March 2022, a draft was agreed by the EU Council. As a result of limited recent developments, the ePrivacy Regulation is now not expected to come into force before at least 2024. A potential transition period of 24 months means that the ePrivacy Regulation would then not come into effect before 2026 at the earliest.

IV CLOUD COMPUTING

It has been nearly a decade since the EU's WP29 adopted its guidance on an EU code of conduct for cloud computing.[122] Following the submission by the Belgian DPA, on 19 May 2021, the EDPB approved the EU Cloud Code of Conduct (Cloud Code).[123] The Cloud Code is now the first endorsed pan-Europe code of conduct for cloud service providers addressing all cloud offerings under Article 40 of the GDPR.

The Cloud Code aims to establish good data protection practices for all cloud service models (including software (i.e., SaaS) and platforms (i.e., PaaS) as well as infrastructure (i.e., IaaS), and applies to all B2B cloud services where the cloud service provider acts as a processor under Article 28 of the GDPR. The Cloud Code does not apply to B2C services or any processing activities for which the cloud service provider may act as a controller. However, the Cloud Code can still be relevant for customers of cloud services because they will receive an additional guarantee of compliance with entrusting adherent cloud service providers.

The main objective of the Cloud Code is to provide practical guidance and a set of specific binding requirements (such as requirements regarding the use of subprocessors, audits, compliance with data subject rights requests, transparency, etc.), as well as objectives to help cloud service providers demonstrate compliance with Article 28 of the GDPR.

i Lawfulness of processing

Cloud service providers are required to act in accordance with their controller's instructions and establish documented procedures to comply with duties and internal communication mechanisms.

ii Subprocessing

The Cloud Code contains rules on engaging a new subprocessor including documenting procedures for implementing the flow of the same data protection obligations and appropriate technical and organisational measures down the processing chain.

120 Council of the European Union, ePrivacy Regulation Progress Report, accessible at https://data.consilium.europa.eu/doc/document/ST-12891-2020-INIT/en/pdf.

121 Council of the European Union 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 of Privacy and Electronic Communications, https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf).

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

123 EU Data Protection Code of Conduct for Cloud Service Providers December 2020.

iii International transfers

According to the EDPB, the Cloud Code is not to be used in the context of international transfers of personal data.[124]

iv Right to audit

According to the Cloud Code, cloud service providers are required to implement appropriate and accessible mechanisms for providing evidence of compliance to customers with established confidentiality obligations.

v Personal data breaches

According to the Cloud Code, cloud service providers are required to assist customers in the case of a personal data breach under the GDPR, establish reporting procedures specifying data breach notification obligations and ensure that the customer is able to easily retrieve personal data following any such breach.

On 22 December 2020, the European Union Agency for Cybersecurity (ENISA) announced that it had launched a public consultation on a draft cloud cybersecurity certification scheme as a way of harmonising the security of cloud computing services across the EU and for ensuring transparency on security measures provided by cloud services.[125]

V WHISTLE-BLOWING HOTLINES

The WP29 published an Opinion in 2006 on the application of the EU data protection rules to whistle-blowing hotlines[126] 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 and the publication of the new EU Directive 2019/1937 (the Whistleblowing Directive) introduced on 23 October 2019.[127] Member States had a deadline of 17 December 2021 to transpose the Whistleblowing Directive into their national laws, and while many have now transposed the law, a couple are still in the process of bringing national legislation into force. On 27 January 2022, the European Commission initiated infringement proceedings against Member States that had not transposed the Whistleblowing Directive.

The new Whistleblowing Directive (as implemented into the national laws of EU Member States) requires companies to establish whistle-blowing hotlines and accept reports concerning violations of EU law, while also ensuring a wide protection to whistle-blowers against retaliation.

---

124 The EDPB adopts opinions on first transnational codes of conduct, accessible at https://edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act_en.

125 ENISA, draft EUCS Cloud Services Scheme, available here https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/.

126 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.

127 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, accessible at https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32019L1937.

The Whistleblowing Directive expressly provides that any processing of personal data in compliance with the Whistleblowing Directive, including disclosing personal data to DPAs, must be carried out in compliance with the GDPR. In addition, personal data that is not manifestly relevant for handling a specific report should not be collected or, if accidentally collected, must be deleted without undue delay. As such, it is important for companies subject to the Whistleblowing Directive to consider GDPR requirements when using vendors, such as hotline providers, and requirements on retaining hotline reports in line with the GDPR and international data transfer requirements, particularly in light of the *Schrems II* decision.

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 legal grounds. The most relevant legal basis is where the processing is necessary for compliance with a legal obligation to which the data controller is subject, which is either based on the obligations set out by the Whistleblowing Directive, as implemented in each EU Member State or on the basis of sectoral legislation.

Where the processing is carried out to comply with foreign legal obligations (e.g., arising from the US Sarbanes–Oxley Act), the WP29 previously concluded that such an obligation does not qualify as a legal obligation that would legitimise the data processing in the EU. Therefore, controllers would need to rely on the legal basis of where the processing is necessary for the purposes of the legitimate interests pursued by the 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.

ii 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'.

iii Compliance with data-retention periods

The Whistleblowing Directive does not establish a maximum time frame to hold records of whistle-blowing reports, but determines that the reports should be stored 'for no longer than it is necessary and proportionate' to comply with the requirement imposed by the

Whistleblowing Directive.[128] Also, the Whistleblowing Directive determines that personal data which is manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.[129]

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.

iv 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.

v 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 Whistleblowing 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. Under the Whistleblowing Directive, the implicated person should be respected in accordance with the Charter of Fundamental Rights of the European Union, including:

a the right of access to the file;
b the right to be heard; and
c and the right to seek effective remedy against an unfavourable decision.[130]

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 Whistleblowing 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.

128 Article 18(1) of the Whistleblowing Directive.
129 Article 17 of the Whistleblowing Directive.
130 Recital 100 of the Whistleblowing Directive.

vi 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.

vii 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.

viii 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 WP29 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[131] 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 pretrial e-discovery procedure include consent of the data subject and compliance with a legal obligation. However, the WP29 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

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

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; and

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, as was its predecessor, the Privacy Shield following the *Schrems II* decision in 2020. The Privacy Shield has recently been replaced by the EU–US Data Privacy Framework (DPF). In the absence of any updates from the EDPB to the former WP29's e-discovery working document, it can be assumed that the use of DPF 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.[132] As 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 where:

a 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 because of 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;

132 Article 48 of the GDPR.

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.[133]

VII EU CYBERSECURITY STRATEGY

The Network and Information Security Directive (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.[134]

The main elements of the NIS Directive include:

a requirements for 'operators of essential service' and 'digital service providers';
b Member States to adopt a national cybersecurity strategy;
c Designation of computer security incident response teams (CSIRTs); and
d a cross-border cooperation network.

As with the ePrivacy Directive, the NIS Directive requires EU Member State implementation, and, as such, the NIS framework varies from one EU Member State to another.

i 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.[135] This includes having research and development plans in place or a risk assessment 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,[136] and setting up of at least one CSIRT that is responsible for handling risks and incidents.[137]

133 Article 49 of the GDPR.
134 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.
135 Article 7 of the NIS Directive.
136 Article 8 of the NIS Directive.
137 Article 9 of the NIS Directive.

ii Cross-border cooperation network

Under Directive (EU) 2016/1148,[138] the competent authorities in EU Member States, the European Commission and ENISA formed a cooperation network to coordinate against risks and incidents affecting network and information systems.[139] The cooperation network exchanges information between authorities and also provides early warnings on information security risks and incidents, and agrees 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 (i.e., through NIS implementing legislation) must ensure that public bodies and certain market operators[140] 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.[141] 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. Note that following the adoption of the NIS 2 Directive (see further the following subsection) the NIS Directive will be repealed.

138 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

139 Article 11 of the NIS Directive.

140 Operators of essential services are listed in Annex II of the NIS Directive and include operators in energy and transport, financial market infrastructure, 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.

141 Article 14 of the proposed NIS Directive.

iv NIS 2 Directive

On 17 January 2023, the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (the NIS 2 Directive) entered into force.[142] As an EU directive, it must be implemented into national legislation in order to be fully applicable and enforceable. The deadline for implementation is 17 October 2024. The NIS 2 Directive replaces its predecessor, the NIS Directive, and establishes a minimum level of cybersecurity standards across the EU. The NIS 2 Directive reclassifies covered entities known as 'essential' and 'important' entities. This scope has been updated to include more sectors and services, such as, energy, transport, banking, financial market infrastructure, health, drinking water, digital infrastructure, ICT service management, public administration and space, as well as postal and courier services, waste management, certain manufacturing industries (e.g., medical devices, computers and electrical equipment) and digital providers (online marketplaces, online search engines, social networking services providers). Covered entities subject to the NIS 2 Directive are required to implement various cybersecurity risk-management measures including:

a internal policies on risk analyses and IT security;
b measures on incident handling;
c business continuity plans;
d disaster recovery plans;
e supply chain security measures;
f security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
g policies to measure the effectiveness of cybersecurity risk management measures;
h basic cyber hygiene practices and cybersecurity training;
i policies and procedures concerning cryptography and encryption;
j human resources security and access control measures; and
k the use of multi-factor authentication.

The NIS 2 Directive also extends the reporting obligations regarding incidents that have a significant impact on the provision of a covered entity's services. Providers are now required to submit: (1) an initial notification within 24 hours of having become aware that their services are affected by a significant incident (an early warning), which shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; (2) an incident notification with 72 hours of becoming aware of a significant incident that shall update the information provided in (1) and indicated an initial assessment of the significant incident, including its severity and impact, and, where available, the indicators of compromise (the incident notification); and (3) a final report no later than one month counted from the incident notification at (2). The final report should include a detailed description of: (1) the incident, its severity and impact; (2) the type of threat or root cause that triggered the incident; (3) the applied and ongoing mitigation measures; and (4) the cross-border impact of the incident (where applicable). Further, between the incident notification and the final report, the CSIRT or, where applicable, competent authority may require an intermediate report with relevant status updates. An incident will have a 'significant impact' where it: (1) has caused or is capable of causing severe operational disruption or financial loss for the entity; or (2) has affected or is capable

142 NIS 2 Directive, accessible here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1692096016913.

of causing considerable material or non-material damage to other (natural or legal) persons. These incident reporting requirements will be triggered as soon as there is an incident with significant impact, and irrespective of whether or not personal data is involved.

The NIS 2 Directive requires that Member States designate or establish competent authorities to oversee compliance with the NIS 2 Directive and as such, competent authorities are yet to be confirmed at a Member State level.

EU Member States are competent to set administrative fines, but for 'essential entities' the maximum amount should be at least set at €10 million or 2 per cent of total worldwide turnover, whichever is higher. For 'important' entities, maximum fines should be set at at least €7 million or 1.4 per cent of total worldwide turnover.

Importantly, if senior members of staff, fail to adequately implement cybersecurity risk management measures in line with NIS2 Directive, they can personally be held liable for administrative penalties or other penalties.

v Cybersecurity Act

On 27 June 2019, the EU Cybersecurity Act (the Act) came into force and was applicable from 28 June 2021. The Act created 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 introduced a set of technical requirements and rules for 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.

vi Digital and Operational Resilience Act

On 17 January 2023, the Digital and Operational Resilience Act (DORA) came into force. As a Regulation and Directive, the date of respective application for both is the 17 January 2025. DORA aims to harmonise cybersecurity and resilience of IT systems used by the financial services industry and their third-party service providers.[143]

143 Digital and Operational Resilience Act (Regulation), available here https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&qid=1674125938473.

In scope entities include companies operating in the financial sector (by reference to definitions of entities in other EU legislation) including investment managers and insurance undertakings, and critical third-party providers of ICT-related services, such as cloud platforms or data analytics services.

DORA imposes a number of obligations on financial entities, including but not limited to:

a putting in place an internal governance and control framework to ensure members of management can approve, oversee and be responsible for the ICT risk management framework in place;

b implementing a 'sound, comprehensive and well-documented ICT risk management framework'. DORA sets out specific and prescriptive requirements for this framework including yearly reviews, internal audits and assigning responsibility;

c defining, establishing and implementing an ICT-related incident management process to detect, manage and notify ICT-related incidents and record all ICT-related incidents;

d classifying incidents based on specific criteria (with further guidance expected on materiality thresholds) including number of financial counterparts affected, duration of downtime, geographical spread of incident, data losses, critical of services affected and economic impact; and

e management of ICT third-party service providers, including putting in place certain contractual provisions with theseservice providers. DORA also imposes a dedicated regulatory oversight framework for those third-party ICT service providers who perform 'critical' functions for financial entities, though these entities are yet to be designated.

Companies must notify the relevant competent authorities of a 'major ICT-related incident' which is defined as an ICT-related incident with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity. Notification requirements are layered and include: (1) an initial notification (within 24 hours of becoming aware of the breach); (2) an intermediate report, after the initial notification referred to in point (1), as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed, followed as appropriate by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority; and (3) a final report, when the root cause analysis of the incident has been completed, regardless of whether or not mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates. The timings for these notifications are to be formulated by European supervisory authorities.

Penalties for breaches of DORA will be imposed by competent authorities at the national EU Member State level, and may include criminal penalties, administrative fines and mandatory implementation of remedial measures, as well as triggering individual liability of individuals within financial entities who can be held responsible for a breach of DORA. Members of management can be faced with fines and can even be individually named in public decisions by the competent authority where the authority finds that the non-compliance by the financial entity is attributable to the individual.

The competent authority will be designated at a Member State level depending on the type of financial entity as follows: (1) for insurance and reinsurance undertakings, the competent authority designated in accordance with Article 30 of the Solvency II Directive;

and (2) for insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, the competent authority designated in accordance with Article 12 of Directive (EU) 2016/97.

It is also important to note the hierarchy between DORA and the NIS 2 Directive. DORA provides that it is *lex specialis* to the NIS 2 Directive where it applies to financial entities. In turn, all DORA requirements that apply to financial entities, in particular those on ICT risk and incident management, incident reporting, digital operational resilience testing, information-sharing and ICT third party risk, take precedence over those in the NIS 2 Directive for financial entities. However, DORA only acts as *lex specialis* to NIS 2 Directive with respect to the requirements applicable to financial entities and not with respect to the requirements applicable to ICT third-party service providers that are subject to DORA. In any event, DORA does provide that competent authorities should take note of potential overlapping requirements under the NIS 2 Directive to avoid duplication of requirements.

vii Critical Entities Resilience Directive

On 17 January 2023, the EU Critical Entities Resilience Directive (CER) came into force.[144] The aim of CER is to reduce vulnerabilities and strengthen resilience of critical infrastructure against specific threats including natural hazards, terrorist attacks, insider threats and sabotage. Critical sectors are identified at an EU Member State level and include: (1) digital infrastructure (e.g., cloud computing, data centre services); (2) financial markets (e.g., operators of trading venues and central counterparties; and (3) banking (e.g., credit institutions).

Critical entities will need to, among other key requirements:

a identify relevant risks that may significantly disrupt the provision of essential services (i.e., based on the outcome of the risk assessment);

b take appropriate and proportionate technical, security and organisational measures to ensure resilience (i.e., based on the outcome of the risk assessment); and

c notify disruptive incidents to competent authorities including with: (1) an initial notification of the disruptive incident within 24 hours of becoming aware of an incident; (2) followed by a detailed report no later than one month thereafter. The notification should assist competent authorities to understand the incident, including to assess any cross-border impact of the incident.

EU Member States will also need to have a national strategy to enhance the resilience of critical entities, carry out risk assessments and identify the covered critical entities.

Like the NIS 2 Directive, the CER must be implemented into national EU Member State legislation to be fully enforceable. Sanctions and liability will also be determined at the national level. The deadline for such implementation is 17 October 2024.

viii Cyber Resilience Act

On 15 September 2022, the European Commission proposed the EU Cyber Resilience Act (CRA). The CRA has not yet been formally adopted but will set common cybersecurity standards for connected devices and services placed on the market in the EU and will apply

144 Critical Entities Resilience Directive, accessible here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557&qid=1692100502367.

to companies that manufacture, import or distribute (digital operators) products with digital elements (PDE) that connect to a device or network. While PDE covers (subject to certain caveats) 'any software or hardware product and its remote data processing solutions including software or hardware components to be placed on the market separately', practically speaking, the CRA is targeted primarily at internet of things (IoT) devices, including 'smart' watches and fitness trackers. The most stringent requirements under the CRA apply to manufacturers of PDE and include:

a meeting certain prescriptive cybersecurity requirements as set out in Annex I of the CRA, including to: (1) design, develop, and produce products to ensure an appropriate level of cybersecurity based on the risks; (2) promote data minimisation; (3) embed a 'secure by default' configuration, with the option to reset digital products to their original state; and (4) ensure vulnerabilities can be easily addressed via security updates; and

b notifying ENISA without undue delay and in any event within 24 hours of becoming aware of: (1) any 'actively exploited vulnerability' contained in the in-scope product; and (2) any incident having impact on the security of the in-scope product. These reporting obligations would extend to informing users where 'necessary' of the incident as well as implementing corrective measures to mitigate the impact of the incident.

In terms of enforcement, EU Member States will designate market surveillance authorities to enforce the CRA. The CRA has also introduced a dedicated cooperation group to ensure uniform application of its provisions, and the European Commission is further empowered to enforce and supervise the CRA. Enforcement powers include administrative fines of up to €15 million or 2.5 per cent of total worldwide annual turnover, whichever is higher. It is expected that the final text of the CRA will be agreed in the coming months and that adoption will follow later in 2023. Once finalised, the CRA will apply 24 months after it enters into force.

ix Intersection with the GDPR

While a number of the new laws mentioned above are not directly linked to the GDPR and have a broader scope of coverage beyond personal data, a number will also have implications from a GDPR perspective. For example, in the context of the AI Act any personal data fed into AI models will need to be processed in compliance with the GDPR, which is specifically acknowledged by the AI Act. Other laws, for instance, CRA and DORA confirm they are without prejudice to the GDPR, and the NIS 2 Directive notes, for example, that where cyber threat information and intelligence are exchanged, sharing must comply with the GDPR.

VIII OUTLOOK

The GDPR has recently celebrated its fifth anniversary and has revolutionised how organisations handle personal data. Over the past five years, and in particular the past year, GDPR enforcement trends, regulatory guidance and case law has emerged and shaped the GDPR – including key concepts, such as the concept of 'personal data'. With the newly created Proposed Regulation on Cross-Border Cases, the EU aims to further strengthen and harmonise GDPR enforcement, which may lead to an uptake in enforcement action (in particular cross-border action) and potentially also private (civil) litigation. International transfers have been and are expected to continue to be an area of focus of regulators,

governments and individuals alike. Although the adoption of the DPF this year has been an important and welcomed milestone in a long history of court proceedings before the CJEU scrutinising EU–US transatlantic data transfers, this is unlikely to be the end. It is expected that, like its predecessors, the DPF will be challenged – although there is more optimism for the DPF to withstand scrutiny compared to its predecessors. Another focus of the EU for the next few years will be the regulation of AI, and other digital technologies and tools, to reinforce the EU's digital single market and the EU's position globally as a key player in this area. The EU AI Act is the first of its kind standalone AI legislation globally – and is being monitored by and expected to have significant impact on organisations, governments and individuals inside and outside the EU deploying, developing and offering AI. A core pillar of the EU's digital strategy is to strengthen cybersecurity throughout the EU – and the EU has proposed and adopted various legislative initiatives in this regard, including DORA (which will impose cybersecurity requirements specific to the financial services industry) and the Cyber Resilience Act (which will impose cybersecurity requirements in relation to connected devices). Over the past five years, the GDPR has been at the forefront – and while the GDPR remains a key piece of legislation for the EU's digital economy, there is a myriad of other (adjacent) regulations, such as the AI Act and the new cyber laws, that have recently been adopted and will have a significant impact on businesses inside and outside the EU.

ISBN 978-1-80449-214-7