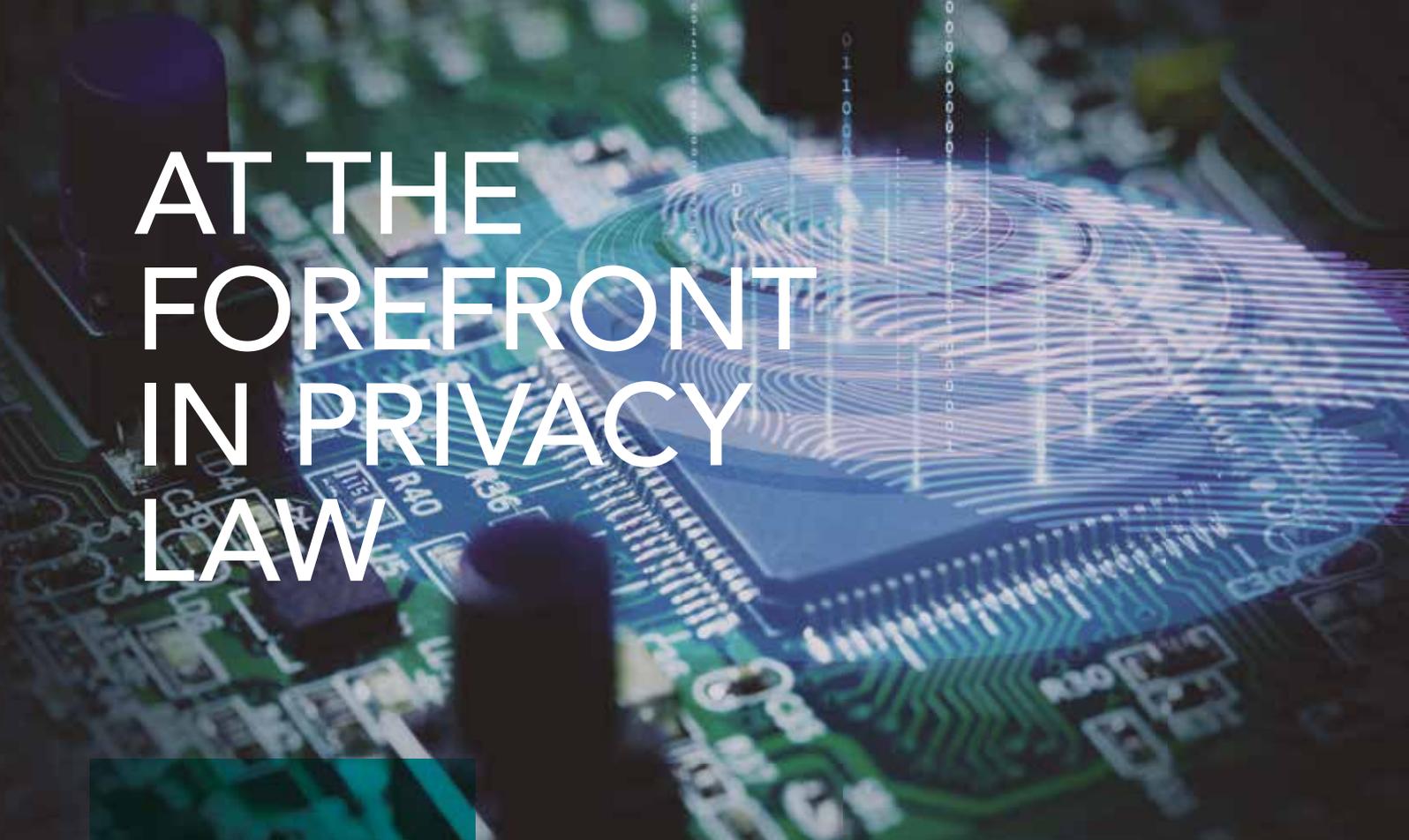


Guide to
GDPR for the funds industry





AT THE FOREFRONT IN PRIVACY LAW

HIGHLY RANKED IN
DATA PROTECTION &
INFORMATION LAW

— *Chambers UK 2018*

“They are fast and responsive,
and they’re able to co-
ordinate advice across
jurisdictions in an easy-to-
understand format.”

— *Chambers UK 2018*

RANKED AMONG
THE BEST IN DATA
PROTECTION, PRIVACY
AND CYBERSECURITY

— *The Legal 500 UK 2018*

Attuned to the evolving digital landscape.

Our privacy and cybersecurity lawyers handle the most challenging global matters concerning data protection, privacy, information security and e-commerce including the GDPR. We work together to help clients across a range of sectors navigate the legal considerations, compliance risks and practical issues raised by the GDPR and by the complex and interconnected global privacy and information security regulatory framework.

TALENT. TEAMWORK. RESULTS.

SIDLEY

AMERICA • ASIA PACIFIC • EUROPE
sidley.com

Attorney Advertising - Sidley Austin LLP, One South Dearborn, Chicago, IL 60603.
+1 312 853 7000. Prior results do not guarantee a similar outcome. MN-7691

Contents

Introduction	4
<hr/>	
Application of the GDPR	5
Material scope	5
Territorial scope	7
<hr/>	
GDPR Principles and Accountability Requirements	9
The seven GDPR principles	9
Accountability under the GDPR	12
<hr/>	
Cybersecurity, Data Breaches and Vendors	15
Information security measures	15
Personal Data Breaches	16
Vendor management	17
Conclusion	18
<hr/>	
Data Privacy Rights	19
Timing and costs	19
Right to Access Personal Data	20
Right to Erasure	21
Right to Restriction of Processing	21
Right to Data Portability	21
Right to Object	22
<hr/>	
Disclosing Data and International Transfers under the GDPR	25
Sharing Personal Data	25
Security	24
International transfers	25
Practical steps to take	27
<hr/>	
Lead DPA and Enforcement	28
Lead DPA	28
The “one-stop-shop” mechanism	28
DPA enforcement powers and fines	29
Remedies for Data Subjects	29
Liability	50
<hr/>	
Appendix A: Glossary	31
<hr/>	
Appendix B: Obligations of Controllers and Processors	34
Key Obligations on Controllers under the GDPR	34
Key Obligations on Processors under the GDPR	34
<hr/>	
Appendix C: List of lawful grounds for processing Personal Data	35
Lawful basis for processing Personal Data	35
Lawful basis for processing Sensitive Personal Data	35
Lawful basis for processing criminal data	36
<hr/>	
Appendix D: Information to be provided to Data Subjects	37
<hr/>	

Introduction

What is the GDPR and why is it relevant?

The GDPR, or the General Data Protection Regulation, is a new EU data privacy law that comes into force on 25 May 2018. The GDPR is intended to provide a single harmonised data privacy law that applies across the EU and is appropriate for the use of Personal Data in the 21st century. The GDPR imposes many new data protection requirements on the collection, use and disclosure of Personal Data which will be relevant to firms and imposes significant fines of up to 4% of annual worldwide turnover.

When the GDPR becomes effective on 25 May 2018 it will replace the EU's Data Protection Directive 95/46/EC (the "Directive") which has been in force since the 1990s. The Directive is implemented into the national data protection laws in each of the EU Member States, which in the UK is the Data Protection Act 1998.

The Directive was drafted in a different century and while it generally worked well there has been a growing recognition by regulators and industry that a new data protection law is required which is relevant to the growth of technology and innovation in a world of Big Data, cloud computing and the Internet of Things. As a result, a proposal for the GDPR was first published back in 2012 and after four years of discussion and negotiation the text of the GDPR was published in the Official Journal of the EU in May 2016. A key principle of the discussions on the GDPR was that it should harmonise data protection laws throughout the EU and apply not only to European businesses but also to businesses outside of the EU that process Personal Data related to the offering of goods or services to individuals in the EU or monitor such individuals and so have a broad extra-territorial effect.

As firms in the private equity, venture capital and fund industry ("firms") have considerable amounts of Personal Data in their day to day operations, whether relating to employees, investors or other individuals, for example, borrowers and debtors, the GDPR will be very relevant to firms that have European based businesses and European investors.

The Chapters below describe how key parts of the GDPR will apply to firms and key obligations and issues for firms to consider in dealing with the GDPR.

Brexit

Despite the UK's June 2016 referendum to leave the EU the GDPR will still come into force in the UK on 25 May 2018. The UK is in the process of finalising the Data Protection Bill which will implement the GDPR in the UK. Even after the UK leaves the EU on 29 March 2019, the Data Protection Bill will still remain in force and the extra-territorial scope of the GDPR means that many UK firms that are processing Personal Data of employees or investors in the EU will still come within its scope.

On 9 January 2018 the European Commission published a "notice to stakeholders" confirming that as from the 20 March 2019 the UK will be considered a third country (i.e. not in the EU). This means that the UK will likely be seeking an adequacy determination by the European Commission in order to ensure the ongoing free-flow of data from the EU to the UK (see Chapter 6 below on Disclosing Data and International Transfers). According to the UK government, the UK Data Protection Bill will ensure that the UK's legal framework for data protection is aligned with the new EU data protection standards under the GDPR (at least upon its inception).

So it is clear that the GDPR will be a key regulation for firms both in the build up to the GDPR becoming effective on 25 May 2018 and for many years ahead. Important guidance on the GDPR has been and will continue to be published and over time this will be supplemented by regulatory enforcement actions and cases such that the GDPR and its impact on firms will need to be closely monitored.

Application of the GDPR

When does it apply and to whom?

The GDPR applies to the “*Processing*” of “*Personal Data*” by a “*Controller*” or “*Processor*” by organisations “*established*” within the EU or outside the EU if their data processing activities relate to the offering of goods or services to individuals in the EU or to the monitoring of such individual’s behaviour. The latter provisions expand the territorial scope of the GDPR well beyond the EU and firms will need to consider which of their operations fall within scope of the GDPR.

Firms have a number of different legal structures with operations located globally with different types of investors and with different service providers who again can be located globally. So understanding exactly when the GDPR applies is a key issue for firms to determine as a threshold matter. It is also important for firms that are investing in portfolio companies to understand when the GDPR may apply to such companies.

Material scope

Article 2 of the GDPR governs the material scope of the GDPR which applies to the Processing of Data wholly or partly by automated means. The GDPR also applies to the Processing of Personal Data not by automated means which form part of a Filing System. So the GDPR applies to Processing of Personal Data in electronic form and also to paper documents to the extent they form part of a Filing System.

Processing

The act of “*Processing*” Personal Data is very broadly defined under the GDPR and includes any operation or set of operations which is performed on Personal Data such as collection, recording, organisation, structuring, storage,

adaptation or alteration, use, disclosure by transmission and deletion.¹ So virtually any activity in relation to Personal Data will amount to Processing.

Personal Data and Data Subjects

Personal Data is defined under Article 4(1) of the GDPR and includes any information in relation to an identifiable person who can be directly or indirectly identified, in particular, by reference to an identifier. This definition provides for a wide range of personal identifiers such as a Data Subject’s name, location data, identification number, online identifiers or one or more factors specific to the physical, physiological and social identity. So data on employees of a firm is likely to be Personal Data under the GDPR if it is possible to identify the employee from the data such as name, job title, contact details, personnel file, appraisal or business communications.

Firms with individual investors in the EU are likely to be processing the Personal Data of such individual investors. More specifically, when an individual chooses to invest in a fund, they will typically be required to provide Personal Data in

¹ Article 4(2) of the GDPR.

the form of their:

- name;
- address;
- date of birth;
- contact information;
- payment details; and
- tax residence information (for US FATCA and CRS purposes).

For identification purposes and to fulfil contractual and regulatory obligations (such as for anti-money laundering obligations), individual investors may also be asked to provide Personal Data in the form of their:

- photograph identification;
- information regarding their source of funds and wealth;
- employment and income information;
- information on dependents; and
- investment objectives.

Where a corporate entity is the investor in the fund, such entity typically also provides Personal Data in relation to its directors, members, shareholders, other beneficial owners or other individuals working for the corporate investor. This Personal Data may include name, address, date of birth, nationality and identity verification documents.

Sensitive Personal Data

The GDPR refers to Sensitive Personal Data as “*special categories of personal data*”.

Article 9 of the GDPR defines Sensitive Personal Data as any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of Genetic Data, Biometric Data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

To the extent a firm collects any Sensitive Personal Data, the legal grounds which it can use under the GDPR to process such data are limited and may require obtaining the individuals explicit Consent as well as applying higher security standards to such Sensitive Personal Data.²

Position on criminal data under Article 10

Article 10 of the GDPR provides that the Processing of Personal Data relating to criminal convictions and offences is permitted where carried out: (i) in reliance on one of the legal grounds under Article 6(1) of the GDPR; and (ii) where under the control of official authority or when authorised by EU or Member State law (e.g. the UK's draft Data Protection Bill).

Under the Data Protection Bill, organisations are permitted to process criminal history data if a condition from Schedule 1 of the Data Protection Bill and a condition from Article 6 of the GDPR are met.

The conditions in Schedule 1 of the Data Protection Bill require that the Processing of criminal history data is necessary for the purposes of performing or exercising an organisation's obligations or rights in connection with one of the following:

- employment;
- health and social care;
- the prevention and detection of a crime (including fraud, terrorist financing or money laundering);
- counselling;
- pensions;
- insurance;
- the political sphere

In addition to meeting one of the substantive conditions in Schedule 1, organisations will also need to have in place an appropriate policy document that explains its procedures for securing compliance with the principles of Article 5 of the GDPR in relation to the Processing of Personal Data, and that explains its policies as regards erasure and retention of the data.

Such policy document should be retained and the Controller's records of Processing (as required under Article 30 of the GDPR) should also explain which condition from Article 6 GDPR is being relied upon to justify the Processing.

Controller and Processors

The GDPR applies to a **data Controller** and a **data Processor** that falls within the territorial scope of the GDPR as discussed in the next section. A data Controller is the entity which, alone or jointly with others, determines the purposes and means of the Processing

² Article 9(2) of the GDPR.

of Personal Data. A firm will determine the purposes for which it processes its employee data and Personal Data it holds on individual investors or on individuals at corporate investors and as such a firm will be a data Controller.

A data Processor is a natural or legal person which processes Personal Data on behalf of the Controller, that is it processes Personal Data on the instructions of the data Controller and does not determine the purposes or means for which the Personal Data are processed. Vendors providing services to the firm, such as a payroll provider, cloud computing provider and a fund administrator would typically be acting as data Processors. However, a data Processor may also act as a data Controller in respect of certain activities where it does determine the purposes and the means of Processing, for example, where it has its own regulatory obligations which require it to carry out its own anti-money laundering checks.

While a data Controller, such as a firm who falls within the territorial scope of the GDPR, is subject to all the obligations and requirements under the GDPR a data Processor is subject to a smaller number of requirements which are set out in the Chapter 4 and Appendix B below.

Territorial scope

One of the main changes under the GDPR is the extension of the territorial scope to include in certain cases Controllers and Processors that are not established within the EU. It is important to note that firms who were previously outside the scope of the Directive may now be captured under the GDPR if they fall within the territorial scope test and, if so, will need to ensure their Processing activities are GDPR-compliant.

The territorial scope test

Article 3 of the GDPR governs the territorial scope. According to the territorial scope, the GDPR applies if one of the following conditions are satisfied:

- **Establishment in the EU:** The Processing of Personal Data in the context of the activities of an establishment of a Controller or a Processor in the EU, regardless of whether the Processing takes place in the EU or not.
- **Data subjects in the EU:** The Processing of Personal Data of Data Subjects who are in the EU by a Controller or a Processor not established in the EU, where the Processing activities are related to:
 - the **offering of goods or services**, irrespective of whether a payment of the Data Subject is required, to such Data Subjects in the EU; or
 - the **monitoring of their behaviour** as far as their behaviour takes place within the EU.

Establishment of a Controller or Processor in the EU

The GDPR will apply to the Processing of Personal Data in “*the context of the activities of an establishment of a controller or a processor*” in the EU, “*regardless of whether that processing takes place in the Union or not*”.³ An “*establishment of a controller or processor in the EU*” relates to the effective and real exercise of activity through stable business arrangements.⁴ This means that not only are EU based firms caught by the ‘establishment’ test, but the test also extends to firms that have a representative office located in the EU or other type of physical presence in the EU.

Importantly, where Controllers and Processors established in the EU are processing Personal Data outside of the EU, the data must be processed in accordance with the GDPR. This is particularly relevant for firms with an establishment in the EU that use non-EU administrators or other service providers, for example, for investor anti-money laundering and sanctions screening services. It is also relevant for EU firms and service providers which outsource Processing functions such as human resources and/or payroll services to intra-group affiliates or service providers outside the EU.

As the GDPR applies to EU Controllers and Processors of Personal Data of “*data subjects who are in the Union*”, the Personal Data of non-EU citizens who are in the EU, as well as EU citizens in the EU, will fall within the scope.

³ Recital 22 of the GDPR.

⁴ Recital 22 of the GDPR states that an ‘establishment implies the effective and real exercise of activity through stable arrangements’ and that ‘legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.’

Controllers or Processors not in the EU

The GDPR will also apply to the Processing of Personal Data by a Controller or Processor not established in the EU where the Processing activities are related to offering of goods or services to Data Subjects in the EU or the monitoring of their behaviour where the behaviour takes place within the EU.

Key to determining whether a non-EU organisation is offering goods or services to Data Subjects in the EU is the business' intention, and whether it is apparent that an offer to a Data Subject located in the EU was "*envisaged*".⁵ This means that firms should determine whether investors based in the EU are being targeted.

The following could be an indication that a firm is targeting EU investors:

- marketing materials are in another European language other than the local language;
- Euro denominated fund offerings;
- the use of currency or a language generally used in a Member State with the possibility of ordering goods or services in that language; or
- using references to investors in a Member State to promote any goods or services.⁶

Recital 23 of the GDPR states that the "*mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention*". Merely having a website or email advertising that it is not targeted at European investors but might be seen by them or telephone numbers on a website that have an international prefix are weaker indications that a firm is offering goods or services to investors in the EU.

The term "*offering*" will only be within the scope of the GDPR if Personal Data is actually processed. Any related Processing of Personal Data, for example, receiving information from an individual investor in the EU in the context of on-boarding would constitute Processing activities

related to the offering of goods or services in the EU.

Monitoring behaviour taking place in the EU

The recitals to the GDPR make clear that where Data Subjects are located in the EU and are "*tracked on the internet*" this will constitute monitoring and bring the relevant entity within scope of the GDPR. Data Controllers may 'track' Data Subjects for the purposes of creating profiles in order to analyse or predict personal preference, behaviours and attitudes.⁷

Websites that use tracking cookies and apps that track usage may be caught to the extent that the information they collect (for example, IP address data), in aggregate, renders an individual identifiable. This may be particularly relevant when firms are conducting due diligence on, or preparing for the sale of, any portfolio entity operating a technology or web based business.

A number of firms may satisfy the GDPR territorial scope test on account of their marketing activities. Such firms will need to ensure that they comply with the marketing provisions of the GDPR and relevant European e-marketing laws, including the requirement to notify Data Subjects of the Processing and to respond effectively to Data Subjects' requests not to have their Personal Data processed for direct marketing purposes. This may require reviewing website content and layout and implementing effective marketing Consents and opt-out mechanisms.

It should also be noted that Article 27 of the GDPR requires in-scope Controllers and Processors without an establishment in the EU to "*designate in writing a representative in the Union*" unless the relevant data Processing is: occasional; does not include, on a large scale, Processing of special categories of data or criminal history data; and "*is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing*".

⁵ Recital 23 to the GDPR.

⁶ Recital 23 to the GDPR.

⁷ Recital 24 to the GDPR.

GDPR Principles and Accountability Requirements

How to show compliance under GDPR

The GDPR requires data Controllers to be responsible for and be able to demonstrate compliance with the seven GDPR principles relating to the Processing of Personal Data which include: (i) lawfulness, fairness and transparency; (ii) the purpose limitation; (iii) data minimisation; (iv) accuracy of the data; (v) storage limitation; (vi) integrity and confidentiality; and (vii) accountability.⁸ This means that firms must now be able to demonstrate compliance under the GDPR.

The seven GDPR principles

The GDPR imposes seven core principles that apply to the ability to use and retain Personal Data that will be relevant to firms. These Seven principles include the fair and lawful Processing principle, purpose limitation principle, data minimisation principle, accuracy principle, storage limitation principle, security principle and accountability requirements as discussed below.

Lawfulness, fairness and transparency

Article 5(1)(a) of the GDPR requires that Personal Data is processed “*lawfully*”, “*fairly*” and in a “*transparent*” manner. This principle imposes a key compliance burden on firms. The requirement to process Personal Data “*fairly*” is extensive and places an obligation on firms to inform Data Subjects of certain information regarding how their Personal Data will be

processed. For example, the identity of the Controller, the purposes of the Processing, the recipients of the data and their data protection rights.⁹ The information to be provided to Data Subjects are set out in Appendix D. The “*lawful*” requirement obliges a firm to process Personal Data in reliance on one or more legal grounds specified in Article 6 (for Personal Data) and Article 9 (for Sensitive Personal Data) of the GDPR (see Appendix C). Three of the most relevant legal grounds in Article 6 for firms include: (i) where necessary to accomplish legitimate interests pursued by the firm or by third parties; (ii) where Consent from the Data Subject has been obtained; and (iii) where necessary to comply with an EU or Member State law.

The legitimate interest ground will involve the firm assessing that its legitimate business

⁸ The data protection principles are set out in more details in article 5 (1) of the GDPR

⁹ Articles 13 and 14 of the GDPR.

interests do not override privacy considerations of the Data Subjects. In particular, the firm would need to objectively assess whether the purposes for which the Personal Data are being processed are valid, such purposes can only be achieved by Processing of Personal Data, and the Processing is proportionate to the end pursuit. Under the GDPR, however, Data Subjects have a right to object to Processing based on legitimate interests and the firm must cease Processing unless it can demonstrate compelling reasons not to (see Chapter 5).

In relation to Consent the requirements for valid Consent are enhanced under the GDPR (i.e. Consent must be informed and freely given, which means that the Data Subject must have a genuine choice as to whether to Consent or not) and Data Subjects can withdraw their Consent at any time. As a result, firms should consider where possible to rely on an alternative legal ground such as, legitimate interest.

In relation to the legal ground of where it is necessary to comply with an EU or Member State law, the GDPR makes it clear that it does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those Data Subjects subject to it. As such, it would include common law obligations.¹⁰ This legal ground could be helpful to firms where the Processing of the Personal Data is required to comply with EU regulatory requirements such as, carrying out anti-money laundering checks on investors.

Firms should ensure that they have the appropriate data privacy notices, website privacy policies and data protection policies in place in order to comply with the transparency requirements under the GDPR both for employees but also for investors, for example in data privacy notices in an investor subscription agreement. Firms should also review the legal grounds that best apply to their different Processing activities.

Purpose limitation

Article 5(1)(b) of the GDPR provides that Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose. Any further Processing is not permitted unless the Data Subject has consented to the new purpose.

Purpose limitation is described by the Article 29 Working Party as being the “cornerstone of data protection” and provides (in its Opinion 03/2013) that the principle is designed to offer a balanced approach: “an approach that aims to reconcile the need for predictability and legal certainty regarding the purposes of the processing on the one hand and the pragmatic need for some flexibility on the other”.

However, there are exceptions to this purpose limitation principle. For example, if the further Processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes then in accordance with Article 89(1) - the further Processing will not be considered “incompatible”. Recital 50 provides further clarity in determining whether a purpose of further Processing is compatible with the initial purpose. It states that the Data Controller should consider: (i) any link between the purposes; (ii) the context in which the Personal Data is collected; and (iii) the reasonable expectations of the Data Subject based on the relationship between the parties; (iv) the nature of the Personal Data; (v) the consequences of the further Processing; and (vi) the existence of appropriate safeguards.

Data minimisation

The GDPR requires that Personal Data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed. Data that is unnecessary for the specific purpose previously identified by the data Controller should not be collected and stored “just in case” or because “it might be useful later”. There must be a foreseeable contingency that gives an objectively justifiable reason for storing data. Where Sensitive Personal Data are concerned it is particularly important to make sure only the minimum amount of information required is collected and retained given the adverse consequences should the protection of this data be compromised. For example, in its guidance, the Article 29 Working Party specifically identifies data minimisation as a concern in relation to systems for electronic health records in terms of deciding which categories of medical data should be collected and stored for which periods of time.

It should be noted that this is not an obligation to limit data Processing to an absolute minimum but rather an obligation to minimise data collection to an adequate level with regard to

¹⁰ Recital 41 of the GDPR.

the purposes of Processing. Firms may wish to consider creating a master list of databases including the purpose of the database, the type of Personal Data contained on the database, the business owners, who has access, security requirements and location of the databases. This approach will assist firms in identifying whether irrelevant and excessive Personal Data are being processed through the databases.

Accuracy

Under the GDPR, Personal Data should be accurate and, where necessary, kept up to date. Further, every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Data subjects have a number of rights under the GDPR in relation to this principle:

- Data Subjects can request that a Controller rectify inaccuracies in Personal Data held about them. If Personal Data are incomplete, a Data Subject can require the Controller to complete the data, or to record a supplementary statement.
- when a Data Subject disputes data accuracy, an organisation is required to restrict the Processing of the Personal Data during the period by which this is verified.

It should be noted that there are no exemptions to this principle and firms should consider whether there are appropriate mechanisms in place to ensure Data Subjects have an opportunity to update their Personal Data, e.g. an annual audit of employee information to ensure current address, bank account details and other Personal Data held is up-to-date and accurate. The frequency at which Personal Data is updated depends on the information which the data are used for. For example, employee payroll records could be updated when there is a pay rise. Similarly, records should be updated for an investor change of contact details so that communications are sent to the correct address. Further, where information is held only for statistical, historical or other research reasons, updating this type of information may defeat the purpose of holding it. The GDPR specifies that the erasure or rectification of inaccurate Personal Data must be implemented without delay. As such, firms should have in place appropriate procedures and responsibilities to ensure compliance. This should include an appropriate procedure to respond to Data Subject access

requests. Firms should institute procedures to ensure that they are taking reasonable steps to check Personal Data for accuracy, i.e. does the Personal Data originate from the Data Subject concerned or another source? It is particularly important where data is received from third parties to ensure that the data received is accurate.

Storage Limitation

Under the principle of “*Storage Limitation*”, Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. Whilst there is no guidance on what is meant by the concept “*for no longer than is necessary*” the indefinite retention of Personal Data is not recommended and, Recital 39 of the GDPR requires that the storage of Personal Data be limited to a strict minimum. Indeed, prolonged retention gives rise to more practical difficulties under GDPR as for however long the Personal Data are stored, it will potentially be caught by the exercise of rights under GDPR for instance data portability, the right to erasure, the right to rectification and the right to Restriction of Processing. In particular, the right of subject access will create significant additional burdens on organisations if large amounts of historic data are stored which are not necessary. . In practice, the appropriate retention period is likely to depend on a combination of the purpose for which the Personal Data was obtained and its nature, the surrounding circumstances (i.e. if Personal Data is obtained as a result of a relationship between the firm and the Data Subject, whether it is necessary to retain that data once the relationship has ended), any legal or regulatory requirements (e.g. MIFID II), or agreed industry practice.

Integrity of personal information

The GDPR requires that Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures which is discussed in Chapter 4 below.

Adhere to codes of conducts and/ or certification schemes

Article 24(3) of the GDPR, supplemented

by Recital 77, provides that adherence to approved codes of conduct and certification mechanisms may help demonstrate compliance with the accountability obligation. Therefore, data Controllers can expect codes of conducts and certification mechanisms to specify the measures required in order to comply with their accountability obligations. Signing up to a code of conduct or certification scheme is not obligatory. Currently, there are no approved codes of conduct or certification schemes under the GDPR although these will likely appear over the next couple of years.

Accountability under the GDPR

The notion of accountability is about requiring a proactive, systematic and on-going approach to data protection and privacy compliance through the implementation of appropriate data protection measures.¹¹

Article 24 of the GDPR codifies the accountability obligation. It requires data Controllers to “implement appropriate technical and organisational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR”. The GDPR itself provides very little guidance in this regard but essentially it means that data protection should be embedded in the business. Article 24(2) provides that data Controllers should implement appropriate data protection policies where appropriate in relation to Processing activities. Implementing those policies alone will certainly not achieve compliance with the accountability obligation. Rather, firms will be required to implement a range of measures as needed to ensure compliance with all of their obligations under the GDPR.

Data Protection by design and by default

Data Controllers must implement technical and organisational measures such as pseudonymisation to ensure that data protection principles are met. It also means that by default only the minimum amount of Personal Data is processed. These concepts “aim at building privacy and data protection into the design specifications and architecture

of information and communication systems and technologies”¹² and ensuring that data Controllers consider data privacy issues throughout the lifecycle. Article 25(2) of the GDPR provides that data minimisation applies to not only the amount of data collected, but also the “extent of their processing, the period of their storage and their accessibility”.¹³

Going forward, data protection issues should be considered by firms at the outset of developing a new system or Process. Generally speaking, it will also be important for firms to consider how compliance with Data Subject rights may be incorporated into new systems (for example, how firms will comply with the data portability requirements or the right to erasure). There are a number of advantages for taking a privacy by design approach including the potential to identify problems at an early stage and actions taken by the firm are less likely to be privacy intrusive and have a negative impact on Data Subjects.

Use of Data Privacy Impact Assessment (DPIA)

Article 35(1) of the GDPR sets out the requirement for a data Controller to carry out a data protection impact assessment in advance of the Processing where the Processing uses new technologies and is likely to result in a high risk for Data Subjects. This may be relevant to certain firm activities such as where it decides to carry out extensive monitoring of its employees. Article 35(3) of the GDPR provides that a data protection impact assessment must be required in the case of:

- Where there is systematic, extensive evaluation of personal aspects including profiling;
- Large scale Processing of Sensitive Personal Data;
- A systematic monitoring of a publicly accessible area on a large scale (such as CCTV and other public monitoring).

In addition, organisations must carry out a DPIA when:

- Using new technologies; and

¹¹ Article 29 Working Party Opinion 03/2010 on the principle of accountability, WP 173 00062/10/EN, adopted on 13 July 2010.

¹² European Data Protection Supervisor, Giovanni Buttarelli, Value of the EU Data Protection Reform against the Big Data Challenges, keynote address, Berlin, May 4, 2015.

¹³ Article 25(2) GDPR.

‘Another key concept of accountability is the appointment of DPOs. Article 37 of the GDPR requires for the first time that all data Controllers and data Processors, where their respective data Processing activities fall within specific criteria (set out below), appoint a DPO for their organisation.’

- The Processing is likely to result in a high risk to the rights and freedoms of Data Subjects.

Article 35(4) of the GDPR requires the supervisory authority to publish a list of activities in relation to which an impact assessment should be carried out. If the firm has appointed a Data Protection Officer (DPO), the firm should seek the advice of that officer when carrying out the data protection impact assessment. Indeed, Article 36(1) of the GDPR states that where the outcome of the impact assessment indicates that the Processing involves a high risk which cannot be mitigated by the Data Controller, the supervisory authority should be consulted prior to commencing the Processing. A DPIA involves balancing the interests of the firm against those of the Data Subject. Article 35(7) of the GDPR states that such an impact assessment should contain as a minimum:

- A description of the Processing operations and the purposes, including, where applicable, the legitimate interests pursued by the Controller;
- An assessment of the necessity and proportionality of the Processing in relation to the purpose;
- An assessment of the risks to Data Subjects; and
- The measures in place to address risk, including security and to demonstrate that organisations comply.

Record of Processing activities

The GDPR requires data Controllers and data Processors (together with their representatives) to maintain records of their Processing activities to help demonstrate compliance with the GDPR. These records must include as per Article 30(1) of the GDPR (amongst others):

- The name and contact details of the Data Controller;

- The purposes of the Processing; and
- A description of the categories of Data Subjects and of categories of Personal Data.

The GDPR requires that records be in writing which includes electronic form, and that they be made available on request.¹⁴ The obligation to keep records of Processing activities does not apply to organisations with fewer than 250 employees unless:

- The Processing is likely to result in a risk of the rights and freedoms of Data Subjects;
- The Processing is not occasional; and
- The Processing includes special categories of data referred to in Article (9(1) GDPR or criminal convictions data in Article 10.

While some firms may have fewer than 250 employees, keeping a data Processing record and carrying out a data mapping exercise may be helpful as a way of assessing what Personal Data the firm has and who has access to that Personal Data and so can be an important tool in meeting the GDPR Principles including accountability. For firms with more than 250 employees, completing and maintaining a record of Processing activities is an important GDPR requirement.

Appointment of a DPO

Another key concept of accountability is the appointment of DPOs. Article 37 of the GDPR requires for the first time that all data Controllers and data Processors, where their respective data Processing activities fall within specific criteria (set out below), appoint a DPO for their organisation. It also sets out what that role entails, and creates employment protection for actions taken as a result of a DPO exercising his/her function. Article 28 requires that the DPO

¹⁴ Article 30(3) and Article 30(4) GDPR.

be “involved, properly and in a timely manner, in all issues which relate to the protection of personal data”.

A DPO must be independent, whether or not they are an employee of the respective legal entity (which is not required, an external contractor can carry out this role provided they similarly comply with the requirements set out above) and must be able to perform their duties in an independent manner.

The DPO is expected to play a key role in fostering a compliance culture within the organisation and is expected to help implement essential elements of the GDPR. These include understanding and upholding Data Subjects’ rights, implementing data protection by design and by default, maintaining and updating records of Processing activities (currently a legal requirement of DPOs in some EU countries), understanding and championing security of the Processing of Personal Data and notification, management and communication of security breaches to the supervisory authority.

Article 37 of the GDPR states that a data Controller or a data Processor shall be required to appoint a DPO in any case where:

- They are a public authority;
- The core activities of the Controller or the Processor consist of Processing operations which, by virtue of their nature, their scope and their purposes, require regular and systemic monitoring of Data Subjects on a large scale; or
- The core activities of the Controller or Processor consist on a large scale of special categories of data (i.e. Sensitive Personal Data) and Personal Data relating to criminal convictions and offences (emphasis added).

Many firms will not be required to have a DPO as there is not systematic monitoring of Data Subjects on a large scale or large scale Processing of special categories of data. However, guidance published by the Article

29 Working Party states that even where businesses do not strictly meet the criteria to appoint a DPO businesses are encouraged to appoint a DPO on a voluntary basis as a matter of good practice (i.e. in accordance with the principle of accountability).¹⁵ However, it should be noted that were a firm to voluntarily appoint a formal DPO, the guidance indicates that the appointment of a DPO on a voluntary basis must comply with the same requirements under Articles 37 to 39 of the GDPR as if the designation had been mandatory. Such requirements include, for example:

- the DPO must be independent – the DPO can hold another position but must be free from a conflict of interests. For example, they could not hold a position within the organisation which determined the purposes and means of data Processing, such as the head of Marketing, IT or Human Resources;
- the business must ensure the DPO exercises its functions independently and reports to the highest level of management;
- the business must not dismiss or penalise the DPO for performance of its tasks;
- the level of expertise required of the DPO must be commensurate with the sensitivity, complexity and amount of data processed - for example, the level of expertise should be greater where processing large quantities of Sensitive Personal Data and/or carrying out extensive profiling activities;
- the DPO must have expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR; and
- the personal qualities of a DPO should include integrity and high professional ethics – the DPO’s primary concern should be enabling compliance with the GDPR.

¹⁵ Article 29 Working Party Guidelines on Data Protection Officers ('DPOs'), WP 243, adopted on 13 December 2017 (as last revised and adopted on 5 April 2017).

Cybersecurity, Data Breaches and Vendors

Dealing with cyber security and vendors under the GDPR

The GDPR requires both Controllers and Processors to implement appropriate information security measures to secure Personal Data and to undertake specified remedial steps in relation to any Personal Data Breaches that occur. Firms also need to include in contracts with vendors GDPR data Processing provisions where vendors process personal Data Subject to the GDPR.

Information security measures

Requirements under Article 32 of the GDPR

The GDPR obliges data Controllers and Processors to “implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk”. Article 32(2) of the GDPR provides that when assessing the appropriate level of security, the data Controller or Processor must take into account the risks that are presented by the Processing, such as “accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed which may in particular lead to physical, material, or nonmaterial damage”.¹⁶

As such, an evaluation of the risks presented by the Processing should be carried out, including “the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons”.¹⁷ According to Recital 75 of the GDPR, possible risks to the

rights and freedoms of Data Subjects may result from, inter alia, the Processing of Sensitive Personal Data. Hence, firms should assume that when processing Sensitive Personal Data, the risks involved are higher as compared to where the organisation is processing “regular” Personal Data. Measures should then be implemented to mitigate such risks, taking into account the “state of the art, [and] the costs of implementation”.¹⁸

Article 32(1) of the GDPR suggests various technical and organisational measures that may be considered appropriate for a data Controller or Processor to implement in order to comply with the GDPR’s information security requirements. These include:

- The pseudonymisation¹⁹ and encryption of Personal Data;

¹⁶ Article 32(1) of the GDPR.

¹⁷ Pseudonymisation is one method by which a data controller or data processor can mitigate and reduce information security risks to data. Pseudonymisation is considered a privacy-enhancing technique because according to Recital 28 of the GDPR, its application to Personal Data “can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.”

¹⁶ Recital 83 of the GDPR.

¹⁷ Article 32(1) of the GDPR.

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- A Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing (e.g. an audit Process).

Recital 78 of the GDPR provides further guidance as to the measures which could be implemented and these include, inter alia:

- Minimising the Processing of Personal Data;
- Pseudonymising Personal Data as soon as possible;
- Transparency with regard to the functions and Processing of Personal Data;
- Enabling Data Subjects to monitor the Processing of their Personal Data.

Overall, the GDPR does not impose prescriptive data security measures, but rather emphasizes a risk-based approach to compliance, which firms and other vendors can tailor according to the nature of the activities and the types of Personal Data that are being processed. Also, the GDPR does not include specific data security requirements that apply to the Processing of Sensitive Personal Data (as opposed to “regular” Personal Data).

Personal Data Breaches

If the security of Personal Data is compromised or breached, this may potentially generate significant adverse effects on the firm and on Data Subjects (whether employees or investors), potentially resulting in physical, material and non-material damage (including, for example, discrimination, identity theft, fraud, and financial loss). As a result, the GDPR requires organisations to report Personal Data Breaches to relevant DPAs unless an exception to such obligation applies.

Personal Data Breach

The GDPR defines a Personal Data Breach broadly as a “breach of security leading to the accidental or unlawful destruction, loss, unauthorized disclosure of, or access to,

personal data transmitted, stored, or otherwise processed”. According to the guidelines published by the Article 29 Working Party on Personal Data Breach notification under the GDPR²⁰ (“Breach Guidelines”), Personal Data Breaches typically fall in one of the following categories:

- Confidentiality breaches - where there is an unauthorised or accidental disclosure of, or access to, Personal Data;
- Availability breaches - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data;
- Integrity breaches - where there is an unauthorised or accidental alteration of Personal Data.

Time scales for

Under Article 33(1) of the GDPR, data Controllers faced with a Personal Data Breach must notify the relevant DPA “without undue delay” and, where feasible, no later than 72 hours after the data Controller becomes aware of the breach. If a Personal Data Breach is not reported within 72 hours, the Controller must provide a reasoned justification for the delay.

As a result, the GDPR requires firms to notify data breaches to the relevant DPA, unless the breach is unlikely to result in a risk of adverse effects taking place. Where there is a likely high risk of adverse effects, the firm may also have to communicate the breach to the affected Data Subjects. Processors must, without undue delay, notify all Personal Data Breaches to the relevant Controller (i.e. the firm).

Exception

Data Controllers are exempted from notifying a Personal Data Breach to the relevant DPAs if they are able to demonstrate that the Personal Data Breach is unlikely to result in a risk for the rights and freedoms of Data Subjects.²¹ In assessing the level of risk, the following factors should be taken into consideration:

- Type of Personal Data Breach: is it a confidentiality, availability, or integrity type of breach?

²⁰ Article 29 Working Party, Guidelines on Personal Data Breach notification under Regulation 2016/679, WP 250, adopted on 30 October 2017 (as last revised and adopted on 6 February 2018).

²¹ Pseudonymisation is the process of de-identifying data so that a coded reference or pseudonym is attached to a record to allow the data that to be associated with a particular individual without the individual being identified.

- 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.
- Ease of identification of Data Subjects: the risk of identification may be low if the data were protected by an appropriate level of encryption. In addition, pseudonymisation can reduce the likelihood of Data Subjects being identified in the event of a breach.
- Severity of consequences of Data Subjects: especially if Sensitive Personal Data are involved in a breach, the potential damage to Data Subjects can be severe and thus the risk may be higher.
- Special characteristics of the Data Subjects: Data Subjects who are in a particularly vulnerable position (e.g. children) are potentially at greater risk if their Personal Data are breached.
- Number of affected individuals: generally speaking, the more individuals are affected by a breach, the greater the potential impact.
- Special characteristics of the data Controller: for example, if a breach involves data Controllers who are entrusted with the Processing of Sensitive Personal Data (e.g. health data), the threat is presumed to be greater.
- Other general considerations: assessing the risk associated with a breach can be far from straightforward. Therefore the Breach Guidance refers to the recommendations published by the European Union Agency for Network and Information Security (ENISA), which provides a methodology for assessing the severity of the breach and which may help designing breach management response plans.

Notifying Affected Individuals

In addition to notifying the relevant DPA, in certain cases firms may also be required to communicate the Personal Data breach to affected individuals, i.e. when the Personal Data Breach is likely to result in a “*high risk*” for 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.

It should be noted that the accountability requirements in the GDPR summarised in Chapter 3 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, organisations should seek to minimise the collection and retention of Personal Data, and especially where Sensitive Personal Data are collected and retained, ensure that those data are encrypted or otherwise made unintelligible to unauthorised parties, to the greatest extent possible.

Vendor management

Firms must also ensure that any data Processors (e.g. third-party vendors who process Personal Data of a firm) engaged by the firm comply with appropriate security requirements to fulfil the integrity principle. Firms should ensure that vendors they appoint:

- implement appropriate technical and organisational measures (discussed above) to protect Personal Data;
- are bound by written GDPR-compliant data Processing provisions which are set out in detail in Article 28 of the GDPR. These data Processing terms should (among other things) provide that the Processor:

‘As a default position, organisations should seek to minimise the collection and retention of Personal Data, and especially where Sensitive Personal Data are collected and retained, ensure that those data are encrypted or otherwise made unintelligible to unauthorised parties, to the greatest extent possible.’

- only processes data on the instructions from the Controller;
- implements appropriate technical and organisational security measures;
- notifies the Controller of any Personal Data Breach without undue delay;
- will allow the Controller to conduct audits of the Processors compliance; and
- only appoint its own vendors (sub-Processors) upon notice to the Controller.

Firms should also ensure that when onboarding a new vendor, that the vendor prior to selection has met the requirements of the vendor management program, including completing a vendor questionnaire which includes an information security assessment. GDPR-compliant vendor contracts, including the Article 28 provisions, should be in place by 25 May 2018 with **all** vendors whose data Processing activities extend beyond 25 May 2018 and which process Personal Data which falls within the territorial scope of the GDPR as discussed in Chapter 2 above.

Conclusion

The steps firms should take to comply with the GDPR's data security requirements will largely be dictated by its internal assessment of the

risks for Data Subjects' privacy associated with a particular data Processing activity. When processing Sensitive Personal Data, firms will need to implement a relatively greater level of security around such data, and be able to demonstrate that the implemented security measures are "*appropriate*" in light of the risks.

A complicating factor is that, in addition to the GDPR's general requirements on data security, firms may have to consider data security-related obligations that are (or will be) imposed at EU Member State level. As most EU Member States are still in the process of adopting their supplementary laws to the GDPR, it is advisable to closely monitor the introduction of country-specific data security requirements in those EU Member States that are of (most) relevance to organisations.

Importantly, firms will need to put in place policies and procedures that allow the organisation to satisfy mandatory Personal Data Breach notification requirements in the GDPR. This may include developing, implementing and testing formal incident response plans that catalogue how the organisation would respond in the event of a Personal Data Breach. Firms will also need to consider implementing a vendor management program and amending contracts with vendors (that fall within the territorial scope of the GDPR) to include Article 28 data Processing provisions.

‘A complicating factor is that, in addition to the GDPR’s general requirements on data security, firms may have to consider data security-related obligations that are (or will be) imposed at EU Member State level.’

Data Privacy Rights

Disclosing data and international transfers under the GDPR

The GDPR largely retains the data privacy rights which exist under the Directive (e.g. the right of access) but more importantly introduces a number of potentially significant new data privacy rights (e.g. the right to erasure). These extensive data privacy rights are reflective of one of the key intentions of the GDPR, to “*put individuals in control of their data*”.²² As a result, firms may find themselves subject to such a Data Subject request from, for example, their employees and/or investors or even borrowers or debtors. As the scope of the GDPR Privacy Rights is extensive, firms should determine and document in advance how best to manage and respond to a request to exercise such privacy rights.

This Chapter aims to assist firms when responding to a request from a Data Subject to exercise the following Data Subject rights under the GDPR:

- Right to Access Personal Data (Article 15)
- Right to Erasure (Article 17)
- Right to Restriction of Processing (Article 18)
- Right to Data Portability (Article 20)
- Rights to Object (Article 21)

This Chapter does not cover a Data Subject's right to information (Articles 13 and 14, GDPR), the right to rectification (Article 16, GDPR), nor a Data Subject's right not to be subject

to a decision based solely on automated Processing (e.g. profiling) which produces legal effects or similarly significantly affects Data Subjects (Article 22, GDPR). Further, pursuant to Article 23 of the GDPR, EU Member States are permitted to introduce further legislative restrictions in respect of the various Data Subject rights where such measures are necessary and proportionate to safeguard inter alia national security. As such, the content of this Chapter is subject at all times to country-specific requirements as provided for in national Member State laws.

Timing and costs

The GDPR requires that a Data Subject rights request 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

²² European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation), 25 Jan 2012, p. 2 (footnote omitted), available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

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 judicial remedy.

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

Right to Access Personal Data

What is the right?

Article 15 of the GDPR grants Data Subjects the right to request access to their Personal Data that are processed by the data Controller (e.g. a firm). This right of subject access, which also exists under the Directive, requires data Controllers to confirm whether or not they are processing the Data Subject's Personal Data and, where this is the case, provide the Data Subject with a copy of the Personal Data, together with the information as prescribed under Article 15(1) of the GDPR.²³

What are the limitations and/or exemptions?

The right of subject access is not an absolute right and there are a number of limitations to the right, including:

- **Limitation (1)** - where complying with the right of subject access would **adversely affect the rights and freedoms of others**.²⁴ 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, a firm (as a data Controller) should first consider whether the disclosure would adversely affect: (a) the rights of any third-party (e.g. where the information to be

disclosed includes a third-party's Personal Data); and/or (b) the rights of the firm and in particular, its intellectual property rights. However, even where such an adverse effect is anticipated, the firm cannot simply refuse to comply with the access request. Instead, the firm would need to take steps to remove or redact information that could impact the rights or freedoms of others.

- **Limitation (2)** - where the data Controller demonstrates that it is **not in a position to identify the Data Subject**,²⁵ except where the Data Subject provides additional information enabling his or her identification.²⁶ If the firm has reasonable doubts concerning the identity of the individual making the request, the firm may request the provision of additional information necessary to confirm the identity of the Data Subject.
- **Limitation (3)** - where the data Controller demonstrates that the request is **manifestly unfounded or excessive**, in particular because of its repetitive character.²⁷ However, in the absence of guidance and/or case law to provide parameters around the scope of these exemptions, a strict interpretation should be considered for the concept of "*manifestly unfounded*" with repetitive requests being documented in order to fulfil the burden of proof as to their excessive character.
- **Limitation (4)** - where a data Controller processes **large quantities of information** concerning the Data Subject²⁸ (as would likely be the case in respect of a firm and its employees), the Controller can request that the Data Subject specify the information or Processing activities to which the request relates. However, caution should be exercised when requesting further information from the Data Subject as it is likely that under the GDPR (as is the case under the Directive), a data Controller will not be permitted to narrow the scope of a request itself.

²³ Article 15(1) of the GDPR states that the following information be provided to a Data Subject exercising his/her right of subject access: (i) the purposes of the processing; (ii) the categories of Personal Data processed; (iii) the recipients of the Personal Data; (iv) the retention period or the criteria used to determine the retention period; (v) the existence of the other Data Subject rights as well as the right to lodge a complaint with the supervisory authority; (vi) the source of the Personal Data where not collected from the Data Subject; (vii) the existence of automated decision-making (including Profiling) as well as meaningful information about the logic involved, the significance and the envisaged consequences for the Data Subject; and (viii) the appropriate safeguards implemented where Personal Data are transferred outside of the European Economic Area (EEA).

²⁴ Article 15(4) of the GDPR.

²⁵ Articles 11(2) and 12(2) of the GDPR.

²⁶ Article 11(2) of the GDPR.

²⁷ Article 12(5) of the GDPR.

²⁸ Recital 63 of the GDPR.

Right to Erasure

What is the right?

Article 17 of the GDPR introduces a statutory right for Data Subjects to have their Personal Data erased without undue delay where:

- the Personal Data are no longer needed for the purpose for which they were collected or processed;
- the Data Subject withdraws Consent and there is no other legal ground for the Processing;
- the Data Subject has objected under the general right to object to the organisation processing their Personal Data and there are no overriding legitimate grounds justifying the organisation processing their Personal Data (see below);
- the Personal Data are unlawfully processed by the Controller (e.g. there may not be an appropriate legal ground for the Processing, the data may be inaccurate or inadequate information may have been provided to the Data Subject);
- erasure of the Personal Data is required under a legal obligation in EU or EU Member State law (e.g. employment laws requiring data to be deleted after a certain period); or
- Personal Data were processed in connection with an online service offered to a child.

What are the limitations and/or exemptions?

There are a number of exemptions to the right of erasure, including where Processing of the Data Subject's Personal Data is necessary for:

- exercising the rights of freedom of expression and information;
- compliance with an obligation under EU or EU Member State law;
- the public interest or the exercise of the Controller's official authority;
- public interest in the area of public health;
- archiving or research purposes; or
- the establishment, exercise or defence of legal claims.

In addition, the Limitations (2) – (4) as identified in the section on Right to Access above may apply.

Right to Restriction of Processing

What is the right?

Article 18 of the GDPR sets out a Data Subject's right to restrict the Processing of his or her Personal Data in certain circumstances. The Restriction of Processing means that, with the exception of storage, the Personal Data can only be processed:

- with the Data Subject's Consent;
- for the establishment, exercise or defence of legal claims;
- for the protection of the rights of another natural or legal person; or
- for the reasons of important public interest of the EU or an EU Member State.

What are the limitations and/or exemptions?

A Data Subject can only exercise the right where:

- the Data Subject contests the accuracy of the Personal Data;
- the Processing of the Personal Data is unlawful but the Data Subject prefers that the Processing is restricted rather than the data being erased;
- the Controller no longer needs the Personal Data for the purposes of the Processing but the Data Subject requires it for the establishment, exercise or defence of legal claims; or
- the Data Subject has objected to the Processing under the general right to object (see below) pending verification as to whether the legitimate grounds of the Controller override those of the Data Subject.

In addition, the Limitations (2) – (4) as identified in the section on Right to Access above may apply.

Right to Data Portability

What is the right?

Where a Data Subject has provided Personal Data to a data Controller, Article 20 of the GDPR grants the Data Subject a right to receive such Personal Data back in a structured, commonly-used and machine-readable format, and to have those data transmitted to a third-party data Controller without hindrance.

What are the limitations and/or exemptions?

A Data Subject can only exercise their right to data portability, where: (a) the data Controller is processing their Personal Data either based on the Data Subject's Consent, or where the Processing is necessary for the performance of a contract with the Data Subject; and (b) the Processing is carried out by automated means.

Article 20(2) of the GDPR limits the requirement for a Controller to transmit Personal Data to a third-party data Controller to where this is "technically feasible". The Guidance states 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".²⁹

Limitations (1) - (4) (as identified in the section on Right to Access) apply equally to the right to data portability and the same considerations should be made as set out above. With regards to Limitation (1), the Guidance states that in the context of the right to data portability, this is intended in principal to avoid the transmission of third-party Personal Data to a new data Controller, where the recipient-Controller intends to use such Personal Data for other purposes (e.g. for marketing). However, the Guidance states that irrespective of whether the data includes Personal Data of a third-party, this does not prevent such data from constituting data which concerns the requestor and as such, all such data should be provided - possibly in a redacted form. The Guidance specifically addresses the reference to intellectual property rights in Recital 63 of the GDPR and states that a data Controller should not reject a data portability request on the basis of the infringement of another contractual right and a potential business risk cannot in and of itself serve as the basis to refuse a request for data portability. In such a case, limited and/or redacted data sets should be transmitted in response to the data portability request.

Right to Object

What is the right?

Article 21 of the GDPR sets out a Data Subject's right to object to the Processing of their Personal Data. This right includes the right to object to:

- Processing where the Controller's legal basis for the Processing of the Personal Data is either where necessary in the public interest or where in the legitimate interests of the Controller ("**general right to object**");
- Processing for direct marketing purposes (the "**right to object to marketing**"); and
- 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 to object to research**").

What are the limitations and/or exemptions?

A firm would **not** need to comply with a request to exercise the general right to object where it can demonstrate either:

- compelling legitimate grounds for the Processing which override the interests of the Data Subject; or
- that the Processing is necessary for the establishment, exercise or defence of legal claims.

There is an exemption to the right to object to research where the "*processing is necessary for the performance of a task carried out for reasons of public interest*".³⁰

In addition, the Limitations (2) – (4) as identified in the section on Right to Access above may apply.

Firms should consider developing guidance for employees on how to identify and handle a GDPR Data Subject rights request where received. Such guidance could also be combined with specific training.

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

³⁰ Article 21 of the GDPR

Disclosing Data and International Transfers under the GDPR

The global nature of the private equity, venture capital and fund industry means that firms will routinely share Personal Data with fund managers, administrators, regulators, vendors, other third parties and investors including transfers outside of the EEA. These transfers must be compliant with GDPR. The GDPR will apply to both one-off decisions to share Personal Data and the routine sharing of Personal Data, whether intra-group or with a third-party, and there are a number of steps and considerations firms should take before and during any disclosure of Personal Data and transfers from the EEA.

Sharing Personal Data

Before sharing Personal Data, the following key factors should be considered:

- the objectives of the sharing and whether the objective can be achieved without sharing the Personal Data or by anonymising it. This should be an on-going evaluation;
- the scope of the Personal Data that needs to be shared. Avoid sharing excessive or irrelevant Personal Data;
- the recipients of the Personal Data (i.e. who needs access to the Personal Data and what they will use the Personal Data for);
- when the Personal Data should be shared (i.e. should the sharing be on-going or only in response to a particular event);
- how the Personal Data should be shared (see discussion on Security below);
- whether the sharing presents any specific risks to the Data Subjects, for example individual investors or representatives of institutional investors; and
- whether the proposed sharing is covered by a relevant information notice (e.g. an online privacy policy, employee or investor privacy notice). Where an existing data protection notice does not cover the intended sharing a new data protection notice must be provided to the Data Subjects.

In order to demonstrate compliance with these requirements, firms should record decisions to and reasoning for sharing Personal Data (see discussion on Practical Steps to Take below and Chapter 3 on Accountability for further detail).

In addition, Personal Data must be processed fairly and lawfully. Further to general compliance with local laws, the GDPR provides a number of circumstances under which the sharing

of Personal Data may be fair and lawful (as discussed in further detail in Chapter 3):

- the Data Subject has provided freely given, specific, informed and unambiguous Consent to the sharing, (which Consent may be withdrawn at any time). Generally, this Consent should be recorded in writing. However, Consent is not an appropriate means of justifying the Processing of Personal Data in all contexts, especially in employment contexts given the imbalance in power which exists between an employer and the employee;
- the sharing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- the sharing is necessary for compliance with a legal obligation. Where the Personal Data is to be shared in compliance with a legal obligation then this should be a European legal obligation; and
- the sharing is necessary for the purposes of the legitimate interests of the firm or the third-party to which the Personal Data is being disclosed. This is probably the broadest justification for the sharing of Personal Data but it is not without restriction: the condition would not apply where the sharing is unwarranted because it prejudices the rights and freedoms or legitimate interests of the Data Subject.

The GDPR also makes a distinction between Personal Data and Sensitive Personal Data.³¹ The GDPR sets a higher bar for organisations to meet in order to justify the Processing and sharing of Sensitive Personal Data. Sensitive Personal Data can only be shared if one of a limited number of legal grounds are satisfied as set out in Appendix C. The most relevant legal grounds for firms include: receipt of explicit Consent of the Data Subject to the sharing in question; necessary for compliance with law; where the Personal Data has already been “*manifestly made public*” by the Data Subject³²; or if the sharing is necessary for the

establishment, exercise or defence of legal claims.

It should be noted that there is also the potential for national Member State laws to provide derogations and exemptions to the above requirements. For example, potential exemptions for special category data (e.g. criminal conviction data) which firms and their investments may process in the context of AML checks. However, at the present time, few Member States have implemented national laws on the GDPR and this area should be closely followed for further developments. The legal grounds that can be used to process criminal data are set out in Appendix C.

Security

Any disclosure of Personal Data within an organisation or to a third-party must be done securely. Where there are regular or large scale transfers to a third-party that is acting as a data Controller, firms should consider entering into a data sharing agreement with the recipient which sets out a common set of rules to be adopted by the organisation disclosing the Personal Data and the recipient. In the UK, ICO has in its guidance on data sharing recommended that the agreement should as a minimum set out the following:

- the potential recipients of the Personal Data;
- the Personal Data to be shared and the purpose(s) for the sharing;
- the quality and security of the Personal Data;
- Data Subjects’ rights (e.g. procedures for dealing with access requests, correction of inaccuracies and queries, right to erasure);
- termination of the data sharing agreement;
- retention and deletion of shared Personal Data; and
- sanctions for failure to comply with the agreement.

Firms must also be satisfied that the recipients to which Personal Data is being disclosed has implemented adequate safeguards to protect the Personal Data, including having technical measures and security standards in place, policies and other arrangements in place confirming a commitment to data security (as discussed in Chapter 4 above), the territory in which any Processing by the recipient will take

³¹ Article 4 of the GDPR.

³² Article 9(2) of the GDPR.

‘Entry into (and compliance with) SCCs is a way for parties to fulfil their obligations with respect to transfers of Personal Data from the EEA as required by the GDPR. SCCs are relatively quick to implement, given their standard form, only the Appendices to describe the data transfer require amendment.’

place (see discussion on International Transfers below) and the harm that would occur if a data security incident occurred.

International transfers

The GDPR maintains the restrictions in the Directive on the transfer of Personal Data to countries outside the EEA that are deemed by the European Commission to not provide an adequate level of protection, such as the U.S., unless: (i) the transfer is made to an “adequate jurisdiction”; (ii) the data exporter has implemented a lawful data transfer mechanism; or (iii) an exemption or derogation otherwise applies. In addition to the data sharing requirements discussed earlier in this chapter, an international transfer of Personal Data will create additional obligations on firms who share Personal Data outside the EEA.

Where a firm is to transfer Personal Data from the EEA, whether it be within the group or to third parties, the transfer must meet one of the following criteria:

- **Adequate Jurisdiction** – the GDPR provides that an international transfer may take place where the European Commission has decided that the third country in question ensures an adequate level of protection. A finding of adequacy can also be made under GDPR in respect of a territory or Processing sector within a third country or an international organisation (e.g. the financial sector). Countries currently deemed adequate by the Commission are: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.³³ This list should

be monitored for changes. As discussed in the Introduction in Chapter 1, following Brexit in March 2019 the UK will be deemed a third country unless and until an adequacy finding is made by the European Commission in relation to the UK.

- **Model Contracts** – otherwise known as Standard Contractual Clauses (SCCs), model contracts are effectively a European standard form data transfer agreement and are an existing transfer mechanism under the Directive and remain available under GDPR. Such SCCs can usually be prepared relatively quickly. However, in some European countries (e.g. Switzerland) it is also necessary to file the Model Contracts with local DPAs and obtain their approval to the data transfer. Model Contracts allow for data exports from the EEA because the data importer and data exporter agree in the Model Contract to be bound by rigorous contractual obligations and EU data protection laws to protect the exported Personal Data. There are two forms of Model Contracts available (i.e. that allow for transfers between):

- (i) two Controllers (so-called Controller-to-Controller Model Contracts); and
- (ii) a data exporter who is a Controller, on the one hand, and a data importer who is a Processor, on the other hand (so-called Controller-to-Processor Model Contracts).

Entry into (and compliance with) SCCs is a way for parties to fulfil their obligations with respect to transfers of Personal Data from the EEA as required by the GDPR. SCCs are relatively quick to implement, given their standard form, only the Appendices to describe the data transfer require amendment. In addition, SCCs require no public statement or declaration from the organisation. However, logistically,

³³ European Commission, Adequacy of the protection of personal data in non-EU countries, available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

the potential need for a large number of SCCs to cover various data flows of an organisation and the need to update said contracts to reflect changing data flows can mean SCCs become impractical. The standard form of the SCCs can also be an issue given there is no flexibility in the language and any amendments may result in the SCCs not being deemed to provide an adequate level of protection.

- **EU-U.S. Privacy Shield** – the Privacy Shield permits firms in the EU to transfer Personal Data to certifying U.S. organisations. In order for a US organisation to certify to the Privacy Shield, it must be regulated by either the Department of Transport or the Federal Trade Commission, and must comply with the Privacy Shield Principles, a set of seven privacy principles that generally align with data protection standards reflected in privacy laws in many jurisdictions. The Privacy Shield also requires compliance with 16 binding supplemental principles, and provides the organising principles for an organisation's data protection program.³⁴ These include recourse mechanisms for Data Subjects who have privacy concerns or otherwise believe the certifying organisation has failed to comply with its commitment under the Privacy Shield. Committing to the Privacy Shield is enforceable under U.S. law by the U.S. Federal Trade Commission and the Department of Transportation.

- **Binding Corporate Rules (BCRs)** – BCRs are given statutory recognition by the GDPR as an appropriate safeguard for transfers of Personal Data for the EEA. BCRs are effectively a global code of practice and program based on European data protection standards that, once approved, allow an international organisation to transfer Personal Data to its other group companies in third countries such as, parents, subsidiaries and affiliates under common control.

Under GDPR, the process for approval of BCRs is more streamlined, requiring the approval of just one Lead Data Protection Authority for BCRs to apply in all EU

Member States. BCRs must be legally binding and the GDPR prescribes the detailed content which must be included in a BCR, including: (i) their legally binding nature; (ii) how information on BCRs is provided by Data Subjects; and (iii) any international data transfers.

Whilst BCRs could be a one-stop solution to the problem of free flow of information between group members of international firms, the approval of BCRs will still require significant investment and resources.

- **Codes of Conduct/Certification Mechanism** – transfers to inadequate jurisdictions may also be possible under the GDPR if the importer has signed up to suitable Codes of Conduct. However, there is limited guidance on this solution at present. Currently no codes of conduct have been adopted and it may be some time before this becomes a viable solution to consider.

Where the country outside the EEA to which Personal Data is to be transferred is not considered adequate, and in the absence of any of the safeguards discussed above, certain exemptions may apply to permit the transfer, for example: (i) obtaining the explicit Consent of the individual Data Subject, although for firms this is unlikely to be a practical or long-term solution to achieve compliance; (ii) isolated transfers are also permitted under the GDPR in limited circumstances, in these cases, the relevant DPA and the individual concerned must be informed, however, again, this is unlikely to be a practical solution for firms; and (iii) in limited situations, there may also be the ability for a firm to rely on derogations such as the transfer being “*necessary for the purpose of compelling legitimate interests*”. However, as with the derogation for isolated transfers, the GDPR imposes stringent requirements on those who seek to rely on this exemption and as such, it is unlikely to provide a long-term solution for most organisations.

International transfers from the EEA are technically allowed with the Consent of the Data Subject concerned. However, it may be difficult for firms to obtain valid Consent (because the requirements for valid Consent are onerous as discussed in Chapter 3) and where, for example, the Personal Data are received from a third-party and not directly from the Data

³⁴ Privacy Shield Framework, available at: <https://www.privacyshield.gov/article?id=Requirements-of-Participation>

Subject. Therefore, other exemptions should be considered for systematic international transfers of Personal Data.

Finally, it is important to note that the GDPR expressly states any judgment or decision of a court or administrative authority of a Third Country which requires a Controller or Processor to transfer or disclose Personal Data will only be enforceable if based on an international agreement between the requesting country and the European Union or relevant Member State.³⁵

Practical steps to take

There are a number of practical steps which should be considered by firms to ensure compliance with the GDPR requirements around disclosing Personal Data including international transfers of Personal Data from the EEA:

- **Data mapping.** Firms should consider mapping all Personal Data being transferred, including transfers outside the EEA to identify where Personal Data is going and why. This exercise should capture any data shared internally across the organisation or externally with third-party vendors and may, for example, include the following:
 - **Employee Personal Data** – some international firms will undertake routine sharing of employee Personal Data (i.e. across a centralised human resources system or payroll) across their offices;
 - **Investor Personal Data** – investor Personal Data shared between entities, for example, through CRM systems; and
 - **Third-party vendors** - Personal Data will often also be shared with third-party vendors, for example, passport information to KYC/AML vendors and

IT service providers. Large, global vendors are likely to be located in third countries.

- **Determine the best mechanism to provide adequate safeguards for the transfer.** Firms should consider which of the current international data transfer solutions offer the most appropriate solution to the different Processing activities undertaken. In some instances, the most appropriate solutions include reliance on “adequate jurisdictions” or putting Model Contracts in place between group entities.
- **Maintain a record.** The GDPR requires both data Controllers and data Processors to maintain a record of any transfers of Personal Data to a Third Country and details of what adequacy decision or international data transfer solution has been applied in respect of each transfer.
- **Other key steps.** A firm in considering transfers of Personal Data from the EEA should also consider a number of ancillary requirements under the GDPR:
 - **Third-party vendors** - check vendor contracts contain provisions which cover international transfers;
 - **Data subject rights** - check privacy notices provided to Data Subjects, such as employees or investors, give information on any cross-border data transfers and the mechanism used to legalise the transfer;
 - **Ongoing obligation** – the GDPR is not an issue which will disappear from 25 May 2018, it requires ongoing compliance. Firms should keep an eye out for any new systems or business activities introduced after 25 May 2018 to ensure appropriate data transfer solutions are adopted in relation to any cross-border transfers of Personal Data from the EEA.

³⁵ Article 45 of the GDPR.

Lead DPA and Enforcement

Under Article 56 of the GDPR, a Controller and Processor that carries out “*Cross-border Processing*” will be primarily regulated by a single DPA where the Controller or Processor has its Main Establishment. DPAs also have extensive enforcement powers while the GDPR also gives Data Subjects a number of remedies. Firms with European operations should determine if they carry out Cross-border Processing and, if so, which is their Lead DPA.

Lead DPA

One of the aims of the GDPR was to enable a business that operates in different EU Member States to have to deal with one Lead DPA where it has Main Establishment known as the “One-Stop-Shop” mechanism.

The “one-stop-shop” mechanism

Article 4(23) of the GDPR defines “Cross-border Processing” as either:

- Processing of Personal Data which 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
- Processing of Personal Data which takes place in the context of the activities of a single establishment of a Controller or Processor in the EU but which substantially affects or is likely to substantially affect Data Subjects in more than one Member State.

In determining whether the Processing falls within scope, Guidance published by the

Article 29 Working Party³⁶ states that DPAs will interpret “substantially affects” on a case-by-case basis taking into account the context of the Processing, the type of data, 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
- involves the Processing of a wide range of Personal Data.

Assuming a firm is engaged in Cross-border Processing, it will need to carry out the Main Establishment test. If a Controller has establishments in more than one Member State, its Main Establishment will be the place of its “*central administration*” (which is not defined) unless this differs from the establishment in which the decisions on the purposes and means of the Processing are made and implemented, in which case the Main Establishment will be the latter.³⁷

For Processors, the Main Establishment will also be the place of its central administration.

³⁶ Article 29 Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, WP 244, adopted on 13 December 2016 (as last revised and adopted on 5 April 2017).

³⁷ Article 4(16)(a) of the GDPR.

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 Guidance published by the Article 29 Working Party makes it clear that the GDPR does not permit “*forum shopping*” and that where a company does not have an establishment in the EU, the “*one-stop-shop*” mechanism does not apply and it must deal with DPAs in every EU Member State in which it is active.

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: (i) the establishment of the Controller or Processor subject to the investigation is in the concerned DPA’s Member State; (ii) Data Subjects in the concerned DPA’s Member State are substantially or are likely to be substantially affected by the Processing of the subject of the investigation; or (iii) a complaint has been lodged to that DPA.³⁸ Concern has been raised over this wide definition, as it could result in multiple DPAs becoming involved in any given case and in turn compromising the efficient decision-making of the EDPB where case referrals are numerous.

DPA enforcement powers and fines

DPAs are afforded a number of powers under Article 58 of the GDPR. These include investigative powers (e.g. to carry out data protection audits) and corrective powers (e.g. to impose a temporary or definitive limitation, including a ban on Processing, and order the suspension of international data flows). DPAs also have the power to impose administrative fines.

The GDPR provides for a two-tier structure for administrative fines. The first tier relates to offenses under Article 83(4) and are subject to fines of up to the greater of €10 million, or two percent of annual worldwide turnover. Such offences include, for example, infringements of the requirements around data protection by design and by default, data Processing records, data security and Personal Data Breaches, DPOs and DPIAs. As such, this level of fine is

primarily concerned with functional, operational, or administrative infringements. The second tier relates to offenses under Article 83(5) and are subject to fines of up to the greater of €20 million, or four percent of annual worldwide turnover. Such offences include, for example, infringements of the requirements around the data protection principles, Data Subject rights, and international transfers. In each case, the administrative fines imposed pursuant to Article 83 must be “*effective, proportionate and dissuasive.*”³⁹

Remedies for Data Subjects

The GDPR strengthens the remedies available to Data Subjects and include:

- **the right to lodge a complaint with a DPA** - if a Data Subject considers that the Processing of his Personal Data does not comply with the provisions of the GDPR. The threshold to make such a complaint is low; and the Data Subject need only “*consider*” that the Processing of Personal Data relating to him is contrary to the GDPR;⁴⁰
- **the right to an effective judicial remedy against a DPA;**⁴¹
- **the right to an effective judicial remedy against a Controller or Processor** - where the Data Subject considers that their rights under the GDPR have been infringed as a result of the Processing of their Personal Data in non-compliance with the GDPR.” The GDPR provides that any such proceedings may be brought in either the Member State in which the Controller or Processor has an establishment, or the Data Subject’s habitual residence;
- **the right to compensation** – for any person who has suffered material or non-material damage as a result of an infringement of the GDPR, the reference to “*material or non-material damage*” in Article 82 seems to mean that compensation may be recovered for both financial and non-financial losses; and
- **the right to be represented by a body, organisation, or association.**

³⁸ Article 4(22) of the GDPR.

³⁹ Article 83(1) of the GDPR.

⁴⁰ Article 77(1) of the GDPR.

⁴¹ Article 78 of the GDPR.

‘Under the GDPR, a Controller may be liable for the damage caused by any Processing that does not comply with the provisions of the GDPR.’

Liability

Under the GDPR, a Controller may be liable for the damage caused by any Processing that does not comply with the provisions of the GDPR. By contrast, a Processor may be liable only for the damage caused by its failure to comply with the obligations of the GDPR “specifically directed to processors” or if the Processor has “acted outside or contrary to lawful instructions of the controller.”

The GDPR also introduces a form of joint and several liability. Article 82(4) of the GDPR

states that “*where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are ... responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the Data Subject.*” The provision entitles the aggrieved Data Subject to obtain full compensation from one particular Controller or Processor, leaving it to that Controller or Processor to deal with the apportionment of liability.

Appendix A

Glossary

Article 29 Working Party	An independent EU advisory body on data protection and privacy composed of representatives from the national DPAs of the EU Member States, the European Data Protection Supervisor, and the European Commission. It has advisory status.
Binding Corporate Rules	Defined in Article 4(20) of the GDPR as “ <i>personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity</i> ”.
Biometric Data	Defined in Article 4(14) of the GDPR as “ <i>personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data</i> ”.
Consent	Defined in Article 4(11) of the GDPR as “ <i>any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her</i> ”.
Controller	Defined in Article 4(7) of the GDPR as “ <i>the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law</i> ”.
Cross-border Processing	Defined in Article 4(23) of the GDPR as “ <i>either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State</i> ”.
Data Subject	See definition for “ <i>Personal Data</i> ” below.
Directive	Directive 95/46/EC of the European Parliament and the Council 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.

European Economic Area (“EEA”)	The EEA consists of the 28 Member States of the European Union together with Iceland, Liechtenstein, and Norway.
Filing System	Defined in Article 4(6) of the GDPR as “ <i>any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis</i> ”.
Genetic Data	Defined in Article 4(13) of the GDPR as “ <i>personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question</i> ”.
ICO	The Information Commissioner's Office in the United Kingdom, is a non-departmental public body which reports directly to Parliament and is sponsored by the Department for Digital, Culture, Media and Sport.
Lead DPA	The DPA where the Controller or Processor has its Main Establishment capable of making legally binding decisions for cross-border cases.
Main Establishment	Defined in Article 4(16) of the GDPR as “(a) <i>as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;</i> (b) <i>as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation</i> ”.
Personal Data	Defined in Article 4(1) of the GDPR as “ <i>any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person</i> ”.
Personal Data Breach	Defined in Article 4(12) of the GDPR as “ <i>a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed</i> ”.

Processing or Process	Defined in Article 4(2) of the GDPR as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.
Processor	Defined in Article 4(8) of the GDPR as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.
Profiling	Defined in Article 4(4) of the GDPR as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.
Pseudonymisation	Defined in Article 4(5) of the GDPR as “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.
Restriction of Processing	Defined in Article 4(3) of the GDPR as “the marking of stored personal data with the aim of limiting their processing in the future”.
Sensitive Personal Data	Defined in Article 9(1) of the GDPR as “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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”.
Third Countries	Countries outside of the EEA.

Appendix B

Obligations of Controllers and Processors

Key Obligations on Controllers under the GDPR

	Obligation	Chapter
1.	Comply with the GDPR data protection principles (including establishing a legal ground to process the Personal Data and providing adequate information to Data Subjects as well as other accountability obligations)	3
2.	Maintain a data Processing record	3
3.	Carry out DPIAs where required	3
4.	Appoint a DPO where required	3
5.	Respond to Data Subject rights (e.g. right of subject access and right to erasure)	5
6.	Implement appropriate technical and organisational measures	4
7.	Notify Personal Data Breaches to DPAs and Data Subjects where required	4
8.	Implement data protection by design and by default	3
9.	Appoint a data protection representative in the EU, where not established in the EU	2
10.	Include specific data Processing provisions in agreements with data Processors and take steps to only use Processors that implement appropriate technical and organisational measures	4
11.	Implement a data transfer solution where carrying out international transfers of Personal Data	6

Key Obligations on Processors under the GDPR

	Obligation	Chapter
1.	Implement appropriate technical and organisational measures	4
2.	Notify Personal Data Breaches to Controllers where required	4
3.	Appoint a data protection representative in the EU, where not established in the EU	2
4.	Include specific data Processing provisions in agreements with Controllers	4
5.	Maintain a data Processing record	3
6.	Appoint a DPO where required	3
7.	Implement a data transfer solution where carrying out international transfers of Personal Data	6

Note: in addition to the direct obligations on Processors set out above, Processors will be subject to a number of contractual obligations via the data Processing agreement (e.g. to assist Controllers respond to Data Subject requests)

Appendix C

List of lawful grounds for processing Personal Data

Lawful basis for processing Personal Data⁴²

-
1. The Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes

 2. The Processing is necessary for the performance of a contract

 3. The Processing is necessary for compliance with a legal obligation to which the Controller is subject

 4. The Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person

 5. 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

 6. The Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third-party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child

Lawful basis for processing Sensitive Personal Data⁴³

-
1. Explicit Consent of the Data Subject, unless reliance on Consent is prohibited by EU or Member State law

 2. The Processing is necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement

 3. The Processing is necessary to protect the vital interests of a Data Subject who is physically or legally incapable of giving Consent

 4. The Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the Processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third-party without Consent

 5. Data manifestly made public by the Data Subject

 6. The Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

⁴² Article 6 of the GDPR.

⁴³ Article 9 of the GDPR.

-
7. The Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures.

 8. The Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

 9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

 10. Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR
-

Lawful basis for processing criminal data⁴⁴

-
1. Must have a lawful basis under Article 6 of the GDPR (please see the table on “Lawful basis for processing Personal Data” above)

 2. Must be carried out only under the control of official authority or when the Processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects

 3. Even if a firm has a condition for processing offence data, it can only keep a comprehensive register of criminal convictions if a firm is doing so in an official capacity.
-

⁴⁴ Article 6 and 10 of the GDPR.

Appendix D

Information to be provided to Data Subjects

-
1. Identity and contact details of the Controller (and where applicable, the Controller's representative) and the data protection officer

 2. Purpose of the Processing and the lawful basis for the Processing

 3. The legitimate interests of the Controller or third-party, where applicable

 4. Categories of Personal Data
*Only applies if data was **NOT** obtained directly from Data Subject

 5. Any recipient or categories of recipients of the Personal Data

 6. Details of transfers to third country and safeguards

 7. Retention period or criteria used to determine the retention period

 8. The existence of each of Data Subject's rights

 9. The right to withdraw Consent at any time, where relevant

 10. The right to lodge a complaint with a supervisory authority

 11. The source the Personal Data originates from and whether it came from publicly accessible sources
*Only applies if data was **NOT** obtained directly from Data Subject

 12. Whether the provision of Personal Data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the Personal Data
*Only applies if data was obtained directly from Data Subject

 13. The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

* Article 13 and 14 of the GDPR

About the Sponsor

Sidley

Sidley is a premier law firm with a practice highly attuned to the ever-changing international landscape. The firm advises clients around the globe, with more than 2,000 lawyers in 20 offices worldwide.

We maintain a commitment to providing quality legal services and to offering advice in data protection, litigation, transactional and regulatory matters including in financial services.

SIDLEY CONTACTS

William Long

Partner

T: +44 20 7360 2061

E: wlong@sidley.com

Geraldine Scali

Counsel

T: +44 20 7360 2086

E: gscali@sidley.com

CONTRIBUTORS

Vishnu Shankar

Associate

Francesca Blythe

Associate

Denise Kara

Associate

Eleanor Dodding

Associate



[@bvca](#)



www.linkedin.com/bvca



[bvcacomms](#)



[BVCA Communications](#)



www.bvca.co.uk



bvca@bvca.co.uk