DAC beachcroft

The European General Data Protection Regulation

A guide for businesses located outside of the European Union

Contents

Rhiannon Webster
Partner, Insurance Advisory
T: +44 (0) 20 7894 6577
E: rwebster@dacbeachcroft.com

Jade Kowalski
Associate, Insurance Advisory
T: +44 (0) 20 7894 6744
E: jkowalski@dacbeachcroft.com

On 4 May 2016, a milestone moment was reached in data protection law in Europe. The General Data Protection Regulation, named in the unmemorable way "Regulation (Europe) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data" was published in the Official Journal of the European Union. We refer to it in this guide as the **"GDPR"**. This marks the start of a two year journey towards its application in all the Member States of the European Union on 25 May 2018. The GDPR will replace the current European data protection law: Data Protection Directive 95/46/EC (the **"Directive"**).

This new law not only has huge ramifications in Europe, but also across the world. A key distinction between the existing European data protection landscape and the GDPR is its extra-territorial effect. The application of current European data protection law is dependent on where the organisation controlling the purpose and the manner of the processing of personal data (known as the **"Data Controller"**) is established. Many have argued that this allows global organisations to avoid compliance with European data protection law, even when processing personal data of European citizens, simply by locating their business outside of Europe.

In contrast, the GDPR significantly expands the breadth of European data protection law. It still applies to organisations established within Europe but also to those who:

- offer goods or services to European residents (irrespective of whether a fee is charged); or
- monitor the behaviour of European residents as far as that behaviour occurs in Europe.

For a detailed analysis of the territorial scope of the GDPR please see page 12.

> Many organisations located outside of the EU will, for the first time, be subject to all the grey areas of European data protection law, which could entail a complete change in culture

Many organisations located outside of the EU will suddenly find themselves within the scope of European data protection law. These organisations will, for the first time, be subject to all the grey areas of European data protection law, which for many could entail a complete change in culture. The GDPR will require substantial changes for businesses that are already complying with the current regime and therefore those who previously fell outside the scope have a much steeper path to climb.

An introduction to the GDPR from a UK based law firm would not be complete without at least an acknowledgment of the effect of Brexit. The UK may have voted to leave the EU but formal separation proceedings cannot begin until it notifies the EU of its intention to invoke Article 50 of the Lisbon Treaty. On current timescales, the UK could leave the EU by March 2019 at the earliest. Consequently, there would be at least ten months where UK data controllers and data processors would have to abide by all the provisions of GDPR and companies located outside of the EU targeting goods and services at UK citizens would need to comply. In reality, exiting the EU could take much longer than two years and the general view in the UK, including from our Information Commissioner is that even after a Brexit, UK data protection standards would have to be equivalent to the GDPR.

This guide provides an overview of the key requirements of the GDPR for those companies located outside of the EU. It seeks to provide advice on the practical steps that can be taken now in order to start the process of ensuring GDPR compliance by 25 May 2018.

HOME

Hans Allnutt
Partner, Global
T: +44(0)20 7894 6925
E: hallnutt@dacbeachcroft.com

> What companies located outside of the EU might not be aware of is that they may also fall within the scope of the GDPR and its breach notification requirements

For most companies that suffer data breaches or cyber-attacks in Europe, there is no strict legal requirement to notify either regulators or data subjects. Therefore, data breaches often go unreported with companies facing limited financial and reputation exposure as long as the breach is not made public.

Recent regulatory guidance and a greater sense of corporate responsibility has increased the number of breaches that are reported in Europe, but the GDPR will bring in compulsory notification obligations for all companies which suffer data breaches. These are requirements that are familiar to companies suffering breaches outside of the EU, but companies in Europe are now taking steps to be breach prepared and the sales of dedicated cyber and breach response insurance is on the rise.

What companies located outside the EU might not be aware of is that they may also fall within the scope of the GDPR and its breach notification requirements. If the breached data came via an establishment in Europe (which could be as basic as a server or website), or if the company located outside of the EU held the data to offer goods or service or to monitor European citizens' activities, then there will likely be notification requirements.

It is crucial that companies located outside of the EU are aware of their potential exposure to the GDPR. The prospect of fines for non-compliance of up to 4% of annual worldwide turnover or

HOME

€20m, and a 72-hour regulatory notification requirement, are forcing companies to consider what they would do in the event of a significant breach.

- How will we independently investigate a cyber-attack or incident?
- Who can we go to for legal advice at short notice?
- What do we need to know in order to inform our regulators?
- How do we contact data subjects who are no longer customers?
- What is our media strategy?
- How are we going to respond to claims for compensation?

DAC Beachcroft's Cyber & Data Risk team regularly responds to cross-jurisdictional data breaches and cyber incidents. Our contact details are:

24/7 breach response hotline - +44 (0)800 3029215

24/7 breach response email - DataRisk@dacbeachcroft.com

> The prospect of fines for non-compliance of up to 4% of annual worldwide turnover or €20 million are forcing companies to consider what they would do in the event of a significant breach

HOME


HOME

Summary

Wider Scope

- Expanded territorial scope to govern companies (a) targeting goods and services at European residents; and (b) monitoring the behaviour of European residents
- For those caught by this new scope, but without an establishment in Europe, they must appoint a representative in Europe.

Data Subject Rights

European data protection law provides **data subject**s with a number of rights, many of which have been enhanced under the GDPR. They include:

- Right of subject access
- Right of data portability
- Right of erasure
- Right to object to profiling and direct marketing

Enforcement

- Fines for the most serious breaches of up to 4% of worldwide turnover or €20,000,000, whichever is higher
- **Supervisory authorities** in Europe also will have the power to (i) audit and (ii) require organisations to cease **processing personal data**.

Fair processing notices

- **Data subject**s need to be provided with notices telling them how their data will be **processed**. The GDPR introduces more specific and comprehensive requirements for content and format of these notices.

Consent

- Consent is not always required to **process personal data** but, when it is required, the GDPR introduces a much higher threshold, meaning there will only be limited circumstances when it may be relied upon.

Accountability

- The GDPR introduces a new principle of accountability which will mean new requirements for both European and non-EU organisations alike. It means organisations need to demonstrate their compliance with the GDPR through policies and procedures which can be inspected on request. Records of data **processing** must also need to be maintained.

Security

- Appropriate security needs to be in place to protect **personal data.** Those parties **processing personal data** on your behalf need to be subject to robust prescriptive contracts.
- The relevant **supervisory authority** needs to be notified within 72 hours where a security breach is likely to result in a risk to the rights and freedoms of individuals.
- **Data subjects** to be notified of data breaches where there is a high risk to their rights and freedoms.

Data Protection Officers

- A data protection officer (**"DPO"**) must be appointed if you carry out large scale systematic monitoring of individuals, or large scale **processing** of **special categories** of **personal data.**
- The **DPO** must be independent, and must not be instructed on how to carry out his/her role and must report directly to the highest level of management.

Best of the rest

- An independent European Data Protection Board is to replace the Article 29 Working Party and will comprise senior representatives of the national **supervisory authorities**. Its obligations include issuing opinions and guidance, ensuring consistent application of the GDPR and reporting to the European Commission.

HOME

Some Key Definitions

Organisations located outside of the EU would be easily forgiven for thinking that European data protection law has a language all of its own. It is important to understand the meaning of key terms as these definitions determine which organisations, activities and data are caught by the GDPR.

The GDPR applies to any **"processing"** of **"personal data"**. **"Processing"** is any operation which can be performed on **personal data**, whether or not automated, such as collection, use, disclosure or even mere storage.

"Personal data" is any information relating to a **"data subject"** 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 **data subject**. Broadly, anything which identifies a living individual is captured.

A **data subject** is the natural person about whom **personal data** relates.

Additional safeguards apply to **special categories of data.** These are **personal data** relating to health, sex life or sexual orientation, racial or ethnic origin or religious or philosophical beliefs, political opinions, trade union membership or genetic or biometric data.

The **"data controller"** is the natural or legal person who, alone or jointly with others, determines the purpose and means of **processing** of **personal data**. The **data controller** must comply with all obligations set out in the GDPR.

The **"data processor"** is the natural or legal person who **processes personal data** on behalf of a **data controller**. A **data processor** is a third party such as an IT provider. Employees of a **data controller** are not **data processors**. The GDPR introduces direct obligations on **data processors** for the first time.

Enforcement of the obligations of the GDPR against **data controllers** and **data processors** will be carried out by a **"supervisory authority"**. There will be a **supervisory authority** established in every Member State in the European Union.

HOME

Principles

Under the GDPR, a **data controller** must comply with the seven principles of data protection. These principles are the core values that underpin European data protection law:

Principle 1: Personal data must be **processed** lawfully, fairly and in a transparent manner. This means that the **data controller** must:

- not breach any statutory or contractual obligations when **processing** the **personal data**;
- provide a **data subject** with a "fair processing notice" which sets out how **personal data** will be used (see page 15); and
- ensure that it can rely on a relevant processing condition (see page 14).

In practice, this means that a **data controller** must:

- have legitimate grounds for **processing personal data;**
- ensure that it is transparent and open with **data subjects**; and
- not **process personal data** in a way which wouldn't be expected by the **data subject**.

Principle 2: Personal data must be collected for specific, explicit and legitimate purposes and not be further **processed** in a manner that is incompatible with those purposes.

This links to Principle 1. Once **personal data** has been obtained for a particular purpose, it should not be **processed** for a different, incompatible purpose.

Principle 3: Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are **processed.** This means that the categories of **personal data processed** should be relevant to the purpose.

Principle 4: Personal data must be accurate and up to date. This requires **data controllers** to put in place policies and procedures for ensuring that **personal data** is accurate and updated as required.

Principle 5: Personal data must be retained for no longer than is necessary.

Principle 6: Personal data must be **processed** in a manner that ensures appropriate security and protects against unauthorised or unlawful **processing** and against accidental loss, destruction or damage, using appropriate technical or organisational security measures (see page 22).

Principle 7: The **data controller** must be responsible for, and be able to demonstrate compliance with, the other principles. This principle is known as the "accountability" principle and is new under the GDPR (see page 18).

Scope

Extra Territorial Effect

The GDPR expands the territorial reach of European data protection law. It will not only apply to **data controllers** and **data processors** established in Europe but also to those which:

- offer goods or services to European residents (irrespective of whether a fee is charged); or
- monitor the behaviour of European residents as far as that behaviour occurs in Europe.

Offering goods or services

When assessing if a business established outside of Europe is offering goods or services to **data subjects** in Europe, consideration needs to be given to whether the business is:

- offering services in a language or currency of a member state;
- enabling European residents to place orders in such other language; or
- referencing European customers in its publications.

If one or more of these conditions are present, this may make it "apparent that the **data controller** envisages offering goods or services" to European residents and it is likely to be considered to be subject to the GDPR. However the GDPR makes it clear that merely having a website which is accessible by European residents is insufficient, unless the website includes a functionality which monitors the behaviour of European residents.

Monitoring behaviour

Monitoring the behaviour of European residents will include tracking European residents on the Internet in order to create profiles or to analyse or predict preferences and behaviour (if the behaviour takes place in Europe). This means that any organisation which uses persistent cookies to build a profile of the users of a website will be caught if the users of the website are European citizens.

HOME

Consequences

A large number of businesses previously operating outside the scope of European data protection law will now be caught by the GDPR and therefore they should be in the process of assessing whether their activities will bring them within the scope of the GDPR. If they are caught, some obligations of the GDPR, such as the appointment of a **DPO**, will affect the organisation as a whole. Other obligations, such as the requirement to provide fair processing notices will only affect the part of the organisation targeting European citizens.

A few examples are set out below:

Situation	Caught by the existing law?	Caught by the GDPR?
Australian social media company with no European group companies, targeting the service at individuals in Europe.	No	Yes
Singapore retailer with e-commerce website, in the English language, accessible by European citizens. The company only delivers to addresses in Singapore.	No	No
Hong Kong retailer with e-commerce website, in English language, which allows purchases and deliveries to European citizens in their local currency.	No	Yes
Canadian website which uses cookies which monitors behaviour and sends targeted marketing to IP addresses, which include those from European citizens.	No	Yes

Requirement to appoint a representative

Businesses outside of Europe that are caught by the GDPR will need to appoint a representative established in Europe, who shall act on behalf of the **data controller** or **data processor**. This role of representative is onerous: they will have to liaise with the relevant **supervisory authority** and accept liability for breaches of the GDPR. In reality this role is likely to be taken by group companies within Europe when such a company exists.

A representative is not required if the **processing** is:

- occasional;
- does not include large scale **processing** of **special categories of data**; and
- is unlikely to result in a risk to the rights and freedoms of **data subjects**.

The representative may itself also be subject to enforcement action in the event of non-compliance by the **data controller**.

Practical steps

Analyse the **processing** carried out by your organisation to determine whether it will be caught by the scope of the GDPR. This will involve considering whether or not your organisation:

(a) offers goods or services to European citizens; or

(b) monitors the behavior of European citizens.

If your organisation is caught by the GDPR, you should:

- implement a compliance plan; and
- appoint a representative.

HOME

Processing Conditions

A **data controller** must be able to rely on a "processing condition" when **processing personal data**. This forms the legal basis for the **processing.**

The processing conditions set out in the GDPR include:

- the **data subject** has given consent to the **processing** of his or her **personal data** for one or more specific purposes. The threshold for providing valid consent under the GDPR is very high;

Consent

Consent is just one way of justifying the **processing** of **personal data** and it will be much harder to obtain consent under the GDPR. In practice, consent is only likely to be valid if the **processing** is truly optional. Therefore organisations should be looking to rely on the other processing conditions.

- **processing** is necessary in order to enter into, or for the performance of, a contract with the **data subject**;
- **processing** is necessary for compliance with a legal obligation imposed on the **data controller**; or
- **processing** is necessary for the purposes of legitimate interests of the **data controller** or a third party, except where such interests are overridden by the interests of the **data subject**.

If the **processing** is of a **special category of data,** an additional processing condition must also be satisfied. These are different from the processing conditions for **personal data** and include:

- the **data subject** has given explicit consent to the **processing**;
- the **processing** is necessary for the purposes of obligations under employment law; or
- the **processing** is necessary in order to protect the vital interests of the **data subject** or another person.

Legitimate interests

Care should be taken when relying on the "legitimate interests" processing condition. This requires an assessment of the interests of the **data controller** and the potential impact on the **data subject's** privacy: essentially a subjective opinion, which could have financial impact if the **supervisory authority** disagrees.

Practical steps

For each processing activity that is caught by the GDPR, an analysis of the relevant processing condition which can be relied on should be carried out.

For audit purposes, internal records should be maintained.

HOME

Fair Processing Information

A **data controller** must provide detailed information to **data subjects** regarding any intended **processing** of **personal data**. This information is usually given in a "fair processing notice", or "privacy notice".

Data controllers must have transparent and easily accessible notices and provide information in a concise form, using clear and plain language.

A privacy notice must contain specific information including:

- the identity of the **data controller**;
- the purpose of the **processing**;
- the contact details of the **data controller**;
- the contact details of the data protection officer (if any);
- the legal basis of the **processing**;
- the data retention period;
- a reference to the **data subject**'s rights under the GDPR; and
- information on international transfers and the safeguards applied to such transfers.

Where the **personal data** is not obtained directly from the **data subject**, the notice should also identify the source of the **personal data**.

Practical steps

Many organisations outside of the EU already provide privacy notices. However, these should be reviewed and amended in preparation for the implementation of the GDPR.

It is likely that a large degree of preparatory work will be required to establish the required information before it can be translated into privacy notices.

Where **personal data** is received from a third party, the recipient will need to give consideration as to how a notice can be provided to the **data subject**, particularly where the arrangements with the third party limit the circumstances in which the **data subject** can be contacted directly. Contractual arrangements with such third parties may therefore need to permit the provision of an appropriate privacy notice.

It is common practice for the privacy notice to be provided using a layered approach with shorter privacy notices contained in documents such as application forms which direct **data subjects** to a longer form notice on the **data controller's** website. This approach will still be permissible under the GDPR.

HOME

Data Subject Rights

The GDPR provides European citizens with rights over and above those already provided under the existing data protection regime.

Right	Detail	Caught by the GDPR?
Right to object to profiling	**Data subjects** have a right not to be subject to a decision based solely on profiling which produces a legal or other similarly significant effect. Profiling is defined as "any form of automated **processing** of **personal data** consisting of the use of **personal data** to evaluate 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 or interests, reliability or behaviour, location or movements". The restriction does not apply if the decision is: ■ necessary for a contract; ■ expressly authorised by law; or ■ has the explicit consent of the **data subject**. There is an absolute restriction on profiling using **special categories of data** unless the **data subject** has given explicit consent or it is necessary for reasons of substantial public interest. In circumstances where profiling is permitted, the **data controller** must implement suitable measures to safeguard the **data subject's** rights and interests.	■ Conduct an analysis of all current profiling activities and determine which will require explicit consent (those profiling activities which use **special categories of data** and those profiling activities which are not necessary for a contract or required by law). ■ Implement or update privacy notices to refer to profiling activities. These will need to be tailored to the particular profiling in order to specify any likely effect on the **data subject**.
Right of Data Portability	The GDPR introduces a new right of data portability for **data subjects**. On request, a **data controller** must: ■ provide the **data subject** with a copy of his or her **personal data** which was provided to the **data controller** (not data which has been generated by the **data controller** itself) in a structured, commonly used and machine readable format; and ■ not hinder the **data subject's** transmission of **personal data** to a new **data controller**. Where technically possible, a **data subject** also has a right to require that their **personal data** is transmitted directly between **data controllers**. The right of data portability only applies where: ■ **personal data** is **processed** by automated means; and ■ the **data subject** has provided consent to the **processing**; or ■ the **processing** is necessary to fulfil a contract.	■ Review **personal data** on systems to establish how they can be provided to the **data subject** and to your competitors(!) on request. ■ Delete **personal data** that is no longer required. ■ Establish policies and procedures for responding to requests from **data subjects**.

Right	Detail	Caught by the GDPR?
Right of erasure	The GDPR provides **data subjects** with a new enhanced right to request erasure of their **personal data** without the need to prove substantial unwarranted damage or distress or inaccuracy. **Data controllers** must delete **personal data** on request where specified grounds apply. Such grounds include: ▪ where the **personal data** is no longer necessary for the original purpose for which the **personal data** was collected/**processed**; and ▪ if the **data subject** withdraws their consent and no other legal ground for **processing** applies. However, there are a number of grounds on which **data controllers** can rely to keep **personal data**. These include: ▪ compelling legitimate grounds; ▪ compliance with a legal obligation; or ▪ establishment, exercise or defence of legal claims.	▪ A data retention policy should be implemented to define the legal and regulatory reasons for retaining categories of **personal data** for specified periods of time. This policy needs to be implemented into both new and existing systems. ▪ Policies and procedures should be put in place documenting how erasure requests are to be handled. ▪ Prioritise transition of **personal data** from historic systems onto new systems which can be built to incorporate data retention and destruction rules.
Access, notification and restriction, and direct marketing	**Data subjects** have a right to: ▪ receive their **personal data** in response to a subject access request in an intelligible format within one month of request; ▪ rectification of their **personal data** if it's inaccurate; ▪ extensive information about the way their **personal data** is being **processed** including the legal basis of the **processing**, the period of data storage, information about access and other rights over the data (including the right to lodge a complaint with a **supervisory authority**), details of any transfers outside of Europe and safeguards applied to such transfers, as well as contact details of the **data controller's** data protection officer; ▪ prevent **processing** of their **personal data** in certain defined circumstances; and ▪ object to direct marketing.	▪ Implement subject access request policies and procedures. ▪ Develop new policies for prompt rectification of **personal data** and a procedure to cease **processing** where applicable. ▪ Implement a policy for dealing with marketing objections and maintain a suppression list.

Accountability

Accountability overview

The GDPR introduces a new principle of accountability. It means **data controllers** need to demonstrate they comply with the GDPR through policies and procedures , which will need to be produced to a **supervisory authority** on request.

Both **data controllers** and **data processors** are obliged to maintain records of **processing** activities. Such records need to include details such as data retention periods, extra EEA transfers of **personal data** and the recipients of **personal data**. These also need to be made available to a **supervisory authority** on request.

Practical steps

- An audit should be undertaken of all systems **processing personal data** and the purposes for which the **personal data** are **processed**. Detailed records should be kept to record this activity, its outcomes and any action to be taken.
- A programme of ongoing monitoring should be established.
- All existing data protection policies and procedures should be reviewed in light of the new principle of accountability.

Data protection by design and by default

The GDPR introduces the concepts of data protection by design and by default.

'Data protection by design' requires **data controllers** to implement appropriate technical and organisational measures to protect the rights of the **data subject** and ensure compliance with the GDPR, having regard to the technology required to meet this obligation and the costs of implementation of the same, the nature, scope and purpose of the **processing**, as well as the risks posed to the **data subject** of the **processing** activities. Pseudonymisation is referred to as a good example of data protection by design (see page 22 for further detail).

'Data protection by default' means **data controllers** must implement appropriate technical and organisational measures to ensure that only **personal data** that is necessary for **processing** for a specific purpose is **processed**. To ensure compliance, **data controllers** should take into account:

- the amount of **personal data** collected;
- the extent of the **processing**;
- the period of storage; and
- the accessibility to that data.

Data controllers should ensure that, by default, **personal data** is not made available or accessible to an indefinite number of individuals.

Practical steps

- All new systems should be built using data protection by design and by default. In practice this will mean ensuring that there is the technical functionality to implement the requirements of the GDPR. For example, systems should be capable of searching for and extracting all **personal data** of a particular **data subject** in order to comply with the right of data portability.
- Organisations should visibly embed data protection in their culture at every level (e.g. by reference to data protection in corporate values and training of employees).

HOME

Data protection impact assessments

The GDPR introduces a requirement for data protection impact assessments (**DPIAs**) to be performed where **processing** activities present a "high risk" to the rights and freedoms of **data subjects.**

Particular activities will trigger the need to carry out a DPIA prior to the **processing** of that **personal data**. The list is non-exhaustive and includes:

- activities which are systematic and extensive and which use automated **processing** of **personal data** in order to evaluate, analyse or predict behaviour; and
- the large scale **processing** of **special categories of data**.

In addition, each **supervisory authority** is required to establish and make public a list of the types of **processing** activities which do and do not require a DPIA.

The DPIA should contain:

- a description of the **processing**, including the legitimate interest pursued by the **data controller**;
- an assessment of the necessity and proportionality of the **processing**;
- an assessment of the risks to the rights and freedoms of **data subjects**; and
- the safeguards and measures to protect against those risks.

The DPIA should be reviewed whenever there is a change to the risks presented by the **processing** operations.

If a DPIA indicates that the **processing** would result in a high risk to a **data subject**, in the absence of steps taken by the **data controller** to mitigate the risk, prior consultation with the **supervisory authority** is required.

> "The mandatory requirement to carry out a DPIA in certain circumstances will add an extra compliance step in the process of rolling out new data projects"

Practical steps

- Prepare a template DPIA and train relevant employees to use it.
- Begin to carry out a DPIA in relation to each new data **processing** project and ensure that outcomes and compliance steps are documented and actioned.
- Look out for guidance from **supervisory authorities** on when a DPIA will or will not be required.

HOME

Data Protection Officers

Position under the GDPR

The GDPR obliges both **data controllers** and **data processors** to appoint a data protection officer (**DPO**) in three situations:

- where they are a public body;
- where core activities require regular and systematic monitoring of **personal data** on a large scale; and
- where core activities involve large scale **processing** of **special categories of data**.

Group companies can appoint a single **DPO**, provided the **DPO** is easily accessible from each establishment.

DPOs must be selected on the basis of professional qualities and expert knowledge of data protection law but do not need to be legally qualified. **DPOs** can either be an employee or contractor.

DPOs must be informed of all data protection issues within the organisation in a proper and timely manner, be provided with the necessary resources to carry out his/her tasks and have access to all **personal data** and **processing** operations.

The minimum duties of a **DPO** include:

- informing and advising the **data controller** or **data processor** and employees **processing personal data** of their obligations;
- monitoring compliance with the GDPR and any other relevant EU or national legislation;
- cooperating with the applicable **supervisory authority** and acting as the contact point for any issues that arise; and
- advising on **DPIAs** and monitoring their impact.

The **DPO** shall be independent from the **data controller** or **data processor** that appoints him or her, and specifically must not be instructed on how to carry out the required tasks listed above. The **DPO** must report directly to the highest level of management and shall not be dismissed or penalised for performing his/her tasks. This effectively provides the **DPO** with a special "protected status" within an organisation, and may create challenges for employers if there is a need to take legitimate performance management or other action against a **DPO** in the context of the employment relationship.

Practical steps

- Review the current job specification of your organisation's **DPO** and consider whether it is appropriate in light of new requirements specified in the GDPR.
- Consider the practical issues surrounding the **DPO** appointment (e.g. independence, separate function to legal, separate budget, report directly to the board).
- Consider any jurisdictional issues involved with the appointment and whether multiple **DPOs** should be appointed to cover different jurisdictions.
- Depending on the size of your organisation, consider whether the **DPO** is likely to require a support team in order to carry out their role effectively and meet all the obligations of the GDPR.

HOME

International Transfers

Both the current European data protection law and the GDPR prohibits transfers of **personal data** outside the European Economic Area (EEA) unless there is adequate data protection measures in place.

A transfer is permitted if:

- the jurisdiction has been deemed adequate by the European Commission;
- an approved mechanism is used (e.g. model clauses); or
- a derogation applies (e.g. consent of the **data subject**).

In addition, under the GDPR:

- the European Commission can deem a particular sector (e.g. financial services) in a particular jurisdiction as adequate;
- binding corporate rules are specifically acknowledged;
- there are two new approved mechanisms of transfer – reliance on an approved code of conduct or an approved privacy seal; and
- a new derogation has been inserted which permits a transfer when in the legitimate interests of the **data controller** and where:
  - the transfer is not repetitive and only concerns a limited number of **data subjects**; and
  - the **data controller** has assessed the transfer, adduced safeguards and has a "compelling" legitimate interest that is not outweighed by the interests or rights and freedoms of the **data subject**.

Importantly, **supervisory authorities** are prohibited from requiring additional notification or approval of a transfer if the transfer is made under a European Commission decision of adequacy or appropriate safeguards specified in the GDPR are met.

Transfers to the United States

Transfers of **personal data** to US companies who signed up to the Safe Harbor scheme were considered adequate by the European Commission until October 2015, when the European Court of Justice declared the Safe Harbor agreement to be invalid. After months of negotiations, this has now been replaced by the Privacy Shield, applications for which have been open to US companies since 1 August 2016. The GDPR does not materially change the situation for transfers of **personal data** from the EEA to the US.

Practical steps

- Companies outside of the EU only need to consider these restrictions if they are exporting **personal data** from within the EEA to outside the EEA. If the **personal data** for example is collected via an Australian website, so that the **data subject** puts their data straight onto the Australian website, the **personal data** is not being exported outside the EEA, as it was never in the EEA in the first place.
- If however, the **personal data** was collected by the Australian organisation on a UK based website and then sent across to Australia, these restrictions need to be considered and appropriate measures put in place.

HOME

Security and Breach Notification

Security measures

Personal data must be **processed** in a way that ensures appropriate security, including protection against unauthorised or unlawful **processing** and against accidental loss, destruction or damage, using technical or organisational measures. This obligation applies to both **data controllers** and **data processors**.

The GDPR requires **data controllers** and **data processors** to balance the changing state of technology, the costs of implementation, the risks presented by the **data processing** and consequences of breach for **data subjects**, and implement a level of security appropriate to the risk, including:

- pseudonymisation and encryption of **personal data**;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to quickly restore the availability and access to **personal data** in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of security measures.

The GDPR introduces definitions of anonymous and pseudonymous data.

Anonymous data is defined as "information which does not relate to an identified or identifiable natural person or to **personal data** rendered anonymous in such a manner that the **data subject** is not or no longer identifiable". Anonymous data is not subject to the requirements of the GDPR.

"Pseudonymisation" means 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 non-attribution to an identified or identifiable natural person.

Despite being considered **personal data** (and therefore being generally subject to the GDPR's requirements), the use of pseudonymisation as a data security method is supported by the GDPR because it is recognised as being able to "reduce the risks to the **data subjects** concerned".

Practical steps

All organisations (whether a **data controller** or **data processor**) should be carrying out a review of the security measures in place to ensure that they are appropriate to the nature of the data held, and the risk of impact on **data subjects** if a breach were to occur. Particular regard should be had to whether it is appropriate to pseudonymise or encrypt the data. It should also be highlighted that this should not be a one off task – the review process should be carried out regularly to ensure the security measures remain effective and appropriate in light of changing technology.

- Where possible, **personal data** that is no longer required for provision of services or regulatory reasons should be anonymised. This will take it outside the scope of the GDPR and will allow businesses to use such data as they choose.
- Where **personal data** cannot be anonymised, businesses are advised to apply pseudonymisation as a security measure.

Breach notification

The GDPR introduces mandatory **personal data** breach reporting to all companies for the first time in Europe.

Data controllers will be obliged to report breaches to the relevant **supervisory authority** "without undue delay, and where feasible, not later than 72 hours" after it first becomes aware of the breach. If the notification is made after 72 hours it should be accompanied by reasons for the delay.

However, it is not necessary to notify a **personal data** breach where it is "unlikely to result in a risk to the rights and freedoms" of **data subject**s.

Personal data breaches must also be notified to **data subjects** where the breach "is likely to result in a high risk" to the rights and freedoms of **data subjects**.

However, notification to **data subjects** is not required if:

- the **data controller** has implemented appropriate security measures that render the **personal data** unintelligible to any unauthorised person, such as encryption;
- the **data controller** has taken subsequent measures to ensure the high risk to **data subjects** does not materialise; or
- it would involve disproportionate effort, in which case a public communication will suffice.

Practical steps

- Organisations based outside of the EU will be well versed in breach notification requirements and will likely be much better placed than European organisations to respond. However, policies and procedures should be reviewed to ensure that the specific requirements of the GDPR (e.g. timescales) are met when a breach relates to **personal data** of European citizens.

Enforcement

The GDPR gives real teeth to the enforcement powers of European regulators.

Powers

Supervisory authorities have a wide range of powers including the ability to:

- carry out audits; and
- issue orders to cease operations; notify **data subjects** of a breach, rectify, restrict or erase **personal data**, suspend or prohibit **processing** or order suspension of data flows to third countries.

Criminal sanctions

Member states can put in place criminal sanctions for infringements of the GDPR.

Fines

Fines can be imposed for "any infringement" of the GDPR.

A warning should only replace a fine in the case of a minor infringement or where a fine would be deemed a "disproportionate burden to a natural person".

The GDPR provides a list of the considerations a **supervisory authority** shall take into account when assessing the level of fine to be imposed. These include:

- nature, seriousness and length of the infringement;
- nature of the **processing** and categories of data involved;
- number of **data subjects** affected and level of damage suffered;
- evidence of intention / negligence;
- mitigation;
- relevance of previous infringements; and
- other relevant aggravating or mitigating factors.

When imposing fines **supervisory authorities** must ensure they are "effective, proportionate and dissuasive".

The level of fine applicable depends on the provision of the GDPR that has been breached. For breaches of more minor obligations, fines can be up to EUR 10,000 or, in the case of an undertaking, up to 2% of worldwide annual turnover of the preceding financial year, whichever is the higher.

For breaches of more serious obligations (such as **processing** without a relevant processing condition or failing to respond to a request from a **data subject**), fines can be up to EUR 20,000,000 or in the case of an undertaking, 4% of total worldwide annual turnover in the preceding financial year, whichever is greater. The fine may be levied by reference to the turnover of an "undertaking".

The GDPR introduces some uncertainty by its use of the word "undertaking". It is an open-ended concept, which encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed. If there is a breach of competition law, fines levied on an undertaking are based on its turnover in the relevant market affected by the conduct. If the relevant market is worldwide the fine is based on the worldwide turnover of the undertaking. If the relevant market is smaller (e.g. one country) the fine will be levied by reference to the turnover in that smaller market.

Practical steps

- The increase in fines and the range of circumstances in which they can be imposed will mean that data protection compliance needs to regularly be on the boardroom agenda.
- Start taking all the practical steps in the other sections of this guide to avoid a monetary penalty notice!
- Consider whether current insurance policy covers new liabilities and consider purchasing a specific cyber product if required.

HOME

Compensation

The GDPR provides that **data subjects** have a right to a judicial remedy against **data controllers** and **data processors**.

Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the **data controller** or **data processor** for the damage suffered.

Therefore, damages will be available for pure distress claims arising from breaches of the GDPR and claims can be brought both against **data controller**s and **data processors**. A **data processor's** liability is limited to damage caused by its **processing** where it has not complied with its specific obligations under the GDPR or acted contrary to the lawful instructions of the **data controller**.

Where multiple **data controller**s or **data processors** are involved in data **processing**, if any one of them is responsible for any of the damage, then it will be responsible to the **data subject** for all of the damage. The party which compensates the **data subject** will have the right to claw back compensation from the other **data controller**s or **data processors** for the damage caused by their breach.

Practical steps

- Start taking all the practical steps in the other sections of this guide to avoid a compensation claim.

> "The burden of proof is on the party that is responsible for the event which has caused the damage"

Our Data Protection Team

Rhiannon Webster

Rhiannon is the head of DAC Beachcroft's information law advisory practice. She holds the ISEB qualification in data protection law.

Rhiannon advises on a full range of data protection issues and offers strategic advice on large projects such as implementing global IT platforms, data protection issues in new technologies such as cloud services, telematics, big data initiatives and the internet of things and data security breach management including representing clients in their communications with the ICO and other regulators. She has a much sought-after practical and commercial approach to providing data protection advice.

Hans Allnutt

Hans leads DAC Beachcroft's cyber risk and breach response team. He is an expert on cyber risk, data breach incidents and insurance policies. He has advised on a wide range of breaches and cyber incidents arising out of extortion demands, acts by malicious employees, software errors and third party negligence. He advises companies from a variety of sectors including retail, financial services, tech & telecoms, charities, higher education and healthcare.

Jade Kowalski

Jade is a Senior Associate in our insurance advisory team and an expert in data protection. Jade regularly advises clients on a range of data protection issues including drafting privacy policies and complex data sharing arrangements. She has notable experience in undertaking privacy impact assessments in advance of the roll out of new technologies and managing data transfer projects across multiple jurisdictions. Jade holds the BCS Professional Qualification in Data Protection (formerly ISEB).

HOME

Our Expertise

DAC Beachcroft's information law practice covers the provision of data privacy, confidentiality, freedom of information and data security breach management advice.

We are in an era where vast quantities of information are stored electronically and businesses are seeking to develop deeper insights into their customers and markets in order to gain a competitive advantage. We now see our clients purchasing technology and expertise which enables them to incorporate new types of data from inside and outside an organisation in a way that is easier to access and manage and is ultimately more insightful than ever before.

Queries range in size, from the very small, when all it takes is a quick call to us, to the major projects – we have experience of dealing with them all

HOME

Our Global Reach

Our experience has shown that the key to success in a multi-jurisdictional legal project is having strong relationships with overseas counsel who are experts in their field. DAC Beachcroft has built a carefully selected panel of trusted advisers who are specialists in providing regulatory, distribution and data protection advice. More importantly, the overseas counsel we work with understand the insurance industry and are commercial in the advice that they provide.

We have a great relationship with our trusted advisers, having worked with them on repeated instructions and having hosted a number in our London office when visiting the UK. We are also happy to work with your preferred advisers if required.

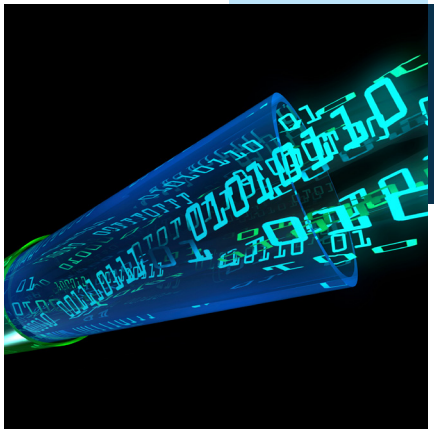
Our panel of overseas counsel covers the following jurisdictions:

Americas	Europe			APAC
Brazil*	Austria	Guernsey	Norway	China
Canada*	Belgium	Hungary	Poland	Hong Kong
Chile*	Bulgaria	Ireland*	Portugal	New Zealand*
Colombia*	Cyprus	Isle of Man	Romania	Singapore*
Ecuador	Czech Republic	Israel	Russia	UAE
Mexico*	Denmark	Italy	Scotland	
	Egypt	Jersey	Slovakia	
	Finland	Kazakhstan	Spain*	
	France	Lithuania	Sweden	
	Germany	Luxembourg	Switzerland	
	Gibraltar	Malta	Turkey	
	Greece	Netherlands	Ukraine	

*DAC Beachcroft office or association.

HOME

We also work with local counsel in many other jurisdictions and our panel is growing all the time, so please ask if there is another jurisdiction in which you need assistance.



Asia Pacific Europe Latin America North America