

# Changes to EU Privacy Law The General Data Protection Regulation



# Table of Contents

1   Introduction	3
2   Main Establishment/“One Stop Shop”	4
3   Fines and Penalties; Additional Regulatory Powers	6
4   The Scope of GDPR: Territory	8
5   The Scope of GDPR: Definition of Personal Data	10
6   The Scope of GDPR: Processors	11
7   Consent	13
8   The Right to Erasure (“Right to be Forgotten”)	14
9   The Right to Data Portability	15
10   Accountability: Data Protection by Design and by Default; Privacy Impact Assessments and Records	16
11   Notification of Personal Data Breaches	18
12   Data Protection Officers	19
13   International Transfers	20
14   Representation of Data Subjects	21
Glossary	22

# 1 | Introduction



On 27 April 2016, following a prolonged legislative process over some four years, the European Council and Parliament finally adopted a new data protection law: the General Data Protection Regulation (GDPR). The GDPR was first proposed in January 2012 and will come into force on 25 May 2018, giving businesses some time to ensure their procedures are in compliance.

The GDPR is different not only in substance to its predecessor but also in form. The existing law derives from a directive (Directive 95/46 (the Directive)) which requires transposition into national law (creating differences in detail). The GDPR though is a directly-effective regulation; immediately applicable to those organisations processing European personal data.

Its adoption is part of a more general European cybersecurity and digital market strategy and other legislative initiatives are afoot (such as the Network and Information Security Directive (currently being finalised) or the forthcoming Directive on data protection in the criminal enforcement sector (outside the scope of the GDPR)).

The GDPR aims to harmonise the differing data protection laws in force across the EU. It also aims to simplify the rules for companies in the European digital single market. A much anticipated initiative, the introduction of the ‘one-stop-shop’ whereby companies need only deal with one regulator, is present but proved controversial during the legislative process and as a result was somewhat diluted.

As will be seen there is greater emphasis in the GDPR on rights of individuals, on requirements for consent, on organisations being able to show adherence to the rules under “accountability” principles, a general data breach notification regime and enhanced enforcement regimes with fines of up to four percent of annual global turnover.

This paper:

- Summarises the more material changes brought about by the GDPR (those likely to have a bigger impact).
- Comments on the likely impact of the proposal on businesses.
- Suggests action points that businesses can begin to address in the lead-up to the measure coming into force.

This paper does not summarise or comment on the entirety of the GDPR. It omits, for example, any discussion of provisions where there is in substance little or no difference between the current and the new regimes.

A glossary of common terms is provided at the end of this paper.

# 2 | Main Establishment/“One Stop Shop”

A significant issue with the current law is the disparate transpositions of the Directive into national law together with differing regulatory responses to issues, in particular in cross-border cases. Businesses often have to navigate these differences and deal with more than one regulator.

The GDPR contains provisions attempting to make sure that data controllers (or processors) operating in more than one jurisdiction are regulated by only one national data protection authority (DPA or supervisory authority). The GDPR does this by reference to an organisation’s “main establishment.” For US headquartered (and other multinational) groups with EU affiliates or offices, the enforcing authority would be determined by reference to the “main establishment” within the EU. The lead regulator, in the country of the main establishment, has responsibility to coordinate all proceedings against the controller. This so-called “one-stop-shop” mechanism is aimed at facilitating cross-border data transfers and business.

The GDPR defines “main establishment” as:

- For controllers, the place of the controller’s central administration in the EU, unless the decisions on processing are taken in another establishment in the EU which has the power to implement such decisions, in this case the decision-making establishment shall be considered the main one.
- For processors, it is “the place of its central administration in the EU” or, if there is none, the establishment where the main processing activities take place.

In order to further this “one-stop-shop”, a detailed structure of authority coordination (cooperation and consistency) is set out in the GDPR.

- Individuals can still lodge complaints with their local authority (who may not be the “lead authority” for a particular controller (or processor)).
- That supervisory authority can then request the lead DPA to take action and indeed can provide to the lead authority a draft of a decision on the matter which the lead DPA is obliged to take “utmost account” of in taking action.
- Lead DPAs and “concerned” authorities in other member states are expected to work together on cross-border issues.
- An authority is “concerned” if there is an establishment (not of course the “lead” establishment) of the business in the relevant member state or if there is an effect on a substantial number of individuals there or if any individual lodges a complaint.
- Lead DPAs are obliged to provide other “concerned” authorities with draft decisions they are considering adopting.
- The GDPR sets out a process for occasions where the supervisory authorities disagree, including the creation of a European Data Protection Board (EDPB) which will, inter alia, issue opinions on some decisions.

## Relevant provisions

Articles 4, 56 and 60 to 67.

---

## Our Commentary

Any provision minimising the need of a multinational business to deal with more than one regulator is welcome. However, it remains to be seen whether this goal is in fact achieved in the final text and how the co-ordination between the different authorities will work in practice.



Earlier drafts of the GDPR contained a strong set of provisions entitling only a lead authority to intervene. However, that was significantly watered down. The consistency mechanism in the GDPR still contains wide scope for action to be taken not only by the “lead authority” but also by other authorities should the lead authority decide not to intervene. A multi-national business can thus be left with dealing with an entirely different DPA to its usual lead regulator.

That supervisory authority may on a cross-border issue disagree with the stance that had been taken by the lead authority. The mechanism for formal co-ordination between the different authorities, and adjudication by the EDPB, is novel and it is possible that there will be wide disagreements in practices and in regulatory action. The

lofty goal of a “one-stop-shop” seems to have been missed and it is possible that this formal co-ordination mechanism offers little more than the discussions that have taken place through the Article 29 Working Party or directly between DPAs under the Directive.



## Action Points

Businesses working in many European countries should analyse their activities with a view of determining their place of “main establishment” and following closely regulatory guidance in that country.

Businesses should also identify which other supervisory authorities may be “concerned” with their activities.

Policies developed should adhere to the most clearly applicable guidance.

# 3 | Fines and Penalties; Additional Regulatory Powers

A headline feature of the GDPR is the significantly enhanced ability for DPAs to issue fines. The maximum fine will depend on the particular violation.

The maximum fine will be the higher of 20 million euros or four percent of an undertaking's annual turnover for violations of a number of obligations, including infringing the basic principles for processing and carrying out a transfer to a third country contrary to the GDPR.

Certain other violations will attract fines of up to the higher of 10 million euros or two percent of annual turnover. Examples of the transgressions subject to this lower cap are: not having records in order, not notifying the supervising authority and data subject about a breach, or not conducting impact assessments.

These percentages are upper limits and are not fixed. When considering the fine to impose, the supervisory authority is to take into account the nature, gravity and duration of the breach, amongst other factors.

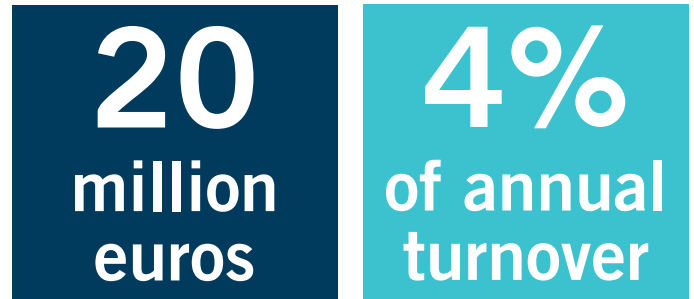
In addition to increased fines, other regulatory powers are enhanced and harmonised. Currently, the powers of the DPAs differ from country to country (the Directive having left choices largely to the individual member states). Going forward, many businesses will find that their supervisory authority has enhanced powers. Of particular note is that under the GDPR, DPAs will all have the following powers:

- To carry out data protection audits.
- To have access to premises (of controllers and of processors).
- To issue "reprimands" for contraventions.
- To order bans or other limitations on particular processing activities.

## Relevant provisions

Recitals 148 to 150. Articles 58, 83 and 84.

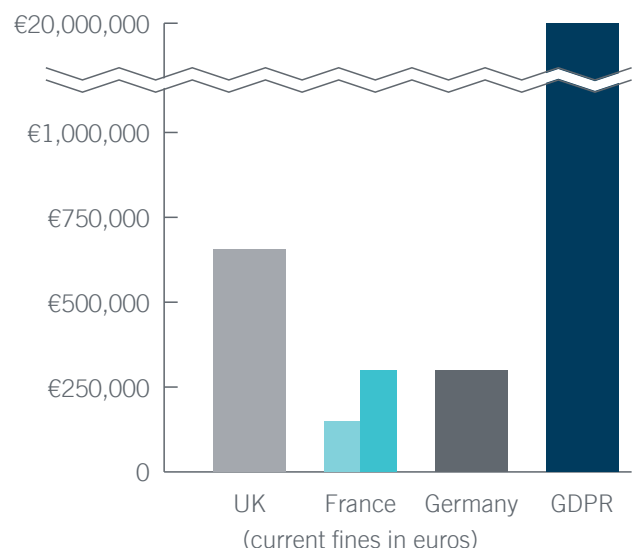
Maximum fine will be the higher of



Significant increase on many member states' current position:

Member State	Current Max. Fine
UK	£500,000
France	€150,000 or €300,000 (for repeat offenses)
Germany	€300,000

Current Fines vs. GDPR Fine



# Our Commentary

The approach supervisory authorities will take when considering these levels of fines, and in the exercise of their powers, remains to be seen and there may well be differences between member states in their attitude.

The potential for fines are pervasive across the GDPR and there can be cumulative fines. For example, a fine for failure to notify a breach can then be followed by a fine for any security failings that led to the breach (each potentially with a separate cap).

Significant fines exist already in some member states and indeed in some (notably, Spain) large fines are kept by the DPA which in turn is used to fund more aggressive enforcement actions. (This can be contrasted with the position in, say, the UK, where monies arising from the limited power of the UK DPA, the ICO, to fine is not kept by the ICO but by the state generally.) But for many member states these powers are a significant increase on the current position. The UK, for example, currently has a maximum fine of £500,000, France has a maximum fine of €150,000 or €300,000 (in the event of a repeat offence) and in Germany the maximum fine is normally €300K but can be higher if the controller can be shown to have profited from the violation.



# 4 | The Scope of GDPR: Territory

The GDPR greatly widens the territorial scope of EU data protection law.

The GDPR will (like the Directive) apply to both controllers and processors established in the European Union.

It will also apply, however, to the processing of personal data of European data subjects where the data controller or processor is outside the EU but where the processing relates to:

- The offering of goods or services to EU residents.
- The monitoring of EU residents.

In order to determine whether goods or services are being offered, it is relevant to consider whether the controller intends to deal with data subjects in the EU. However, the mere accessibility of a website is

insufficient to ascertain such intention. Factors to be considered include the use of a language or currency generally used in the EU, and mentioning EU users or customers.

Monitoring of behaviour includes such activities as internet tracking and profiling.

The GDPR states that where a non-EU controller or processor falls within the GDPR, it should appoint a representative to act on its behalf who should be established in a member state where data subjects targeted by the business are (subject to exceptions such as processing only being occasional, or only small scale processing of special categories of data).

## Relevant provisions

Articles 3 and 27.

## Our Commentary

Europe has some of the stronger data protection rights in the world and it is a consistent feature of much legislative and regulatory activity in this area that those rights (for the protection of EU citizens) should not be avoidable simply on the grounds that the data is processed abroad. The present Directive does contain an extra-territorial reach, but the provision was drafted in the early 90s before the onset of the modern online world of big data.

The Directive is applicable to controllers established in Europe or those established outside Europe but who use equipment within Europe. DPAs and the courts have therefore had to be creative in asserting jurisdiction on the basis of these requirements:

- For example, European regulators have asserted jurisdiction on non-EU websites on the basis that placing cookies on an EU user's device is using "equipment" in the EU.
- A further regulatory reach was illustrated in the 2014 *Google Spain* (Right to be Forgotten) case<sup>1</sup> where Google

<sup>1</sup> *Google Spain SL and Google Inc. V Agencia Española de Protección de Datos and Mario Costeja González* (Case C 131/12, 13 May 2014).



## Action Points

All non-EU companies who target EU residents will need to review their practices to ensure they are in compliance with the GDPR.

If there is not already an EU presence, consideration should be given to appointing a representative within Europe (and to which member state that representative should be located in).



Inc. was found to be subject to the EU rules on the basis that its Spanish marketing affiliate constituted an establishment of the US company within the EU.

But even in light of the *Google Spain* case, the GDPR contains a significant widening of the reach of EU data protection law. There will be less of a need for DPAs and courts to resort to creative means of finding jurisdiction.

The tests of “offering” goods and services to individuals within Europe, or “monitoring” them, should be easier to apply.

A non-EU controller or processor can appoint an EU representative in a member state of its choice. This may well lead to some forum shopping in an attempt to ease any perceived regulatory burden.



# 5 | The Scope of GDPR: Definition of Personal Data

The GDPR makes a number of changes to the definition of personal data. It retains the Directive test that if the subject can be identified ‘directly or indirectly’, by means reasonably likely to be used by someone, then this is personal data. However, there is now express expansion beyond obvious identifiers.

First, pseudonymisation has been explicitly introduced throughout the GDPR. It is defined as processing in a way that removes the link to a specific data subject i.e. the additional identifying information (sometimes called a “key”) is held separately and is subject to technical and organisational measures. Data that has been pseudonymised remains within scope as “personal data” because it can be reassociated with a specific

consumer. However, fully anonymised data falls outside the scope.

Secondly, online identifiers are expressly recognised as a means of identifying individuals. This will include such things as IP addresses and cookie IDs.

Lastly, if used for the purposes of identifying a natural person, genetic and biometric data are now characterised as “special category” data (otherwise known as “sensitive data” in some member states), alongside health and other specially protected types of data.

## Relevant provisions

Recitals 30 and 148 to 150. Article 4.

---

## Our Commentary

The inclusion of pseudonymised data within the scope of the GDPR will be felt within some industries which have relied on pseudonymisation techniques as a means of perhaps avoiding the application of data protection law. An example is the key-coding of clinical trial data which would arguably have taken the handling of that data (on the current law) outside of scope; although the position was always arguable. These arguments now go away. Key-coded data (and other pseudonymised data) is now firmly within scope. However, the GDPR makes concessions to the fact that the processing of pseudonymised data is somewhat less risky and use of these techniques can form part of privacy impact risk reduction.

The introduction of online identifiers within the definition of personal data is an attempt to address and do away with another area of controversy: whether and to what extent use of such identifiers (which do not directly identify an individual in the “real world”) is within the scope of data protection law. However, it remains to be seen whether all arguments are now behind us. Whilst there is express mention of such identifiers (such as IP addresses and cookies) there is no definitive statement



## Action Points

Online businesses engaged in monitoring or tailoring activities based on IP addresses or cookies (or similar) will now have to pay closer attention to EU data protection rules.

that their use will always be deemed to lead to identification of individuals. Rather, the GDPR states (in a recital) that:

*“online identifiers ... may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”*

So the current controversy has not been completely removed. Online identifiers (e.g., IP addresses) may lead to identification (and may therefore be “personal data”), but not necessarily so.

## 6 | The Scope of GDPR: Processors

The Directive (and the GDPR) makes a distinction between “controllers,” who determine the means and the purposes of the processing, and “processors,” who process data for the controller (typically service providers).

Under the current law, only controllers have obligations to DPAs or to individuals and only controllers are subject to fines or enforcement actions. Processors do not, although there will inevitably be some contractual responsibility to the controller (depending on the terms agreed). That will change. The GDPR greatly increases the statutory responsibilities of processors.

For example:

- Processors will have statutory responsibility for security.
- Processors are also subject to enforcement and fines.
- Processors are not permitted to enlist other processors (e.g., sub-contractors) except with the prior permission of the controller.
- Processors will also be responsible for compliance with the international transfer rules.

- Processors, with some exceptions, will also be responsible for keeping detailed documentation of all data processing operations, which must be produced upon request to the relevant DPA.

*As processors become fixed with direct obligations under the GDPR they may seek to allocate some of the resultant risk back onto the controller by contract.*

The GDPR contains a longer prescribed list of what a contract between a controller and processor should contain. In addition to current requirements, amongst others, contracts will now need to contain provisions on the deletion or return of data upon termination and restrictions on appointing sub-processors (i.e., sub-contractors).

### **Relevant provisions**

Articles 28, 30, 32, 44 and 46.

---

## Our Commentary

This change is significant. As processors become fixed with direct obligations under the GDPR they may seek to allocate some of the resultant risk back onto the controller by contract. For example, a processor in the European Union that previously transferred data out of Europe would not have been subject to any enforcement action had

the requirements not been met (only the controller would have been). Now, given direct responsibility for these type of issues, a processor may consider it prudent to get an assurance from the controller that, for example, there are adequate consents or other sufficient means of ensuring a lawful transfer.

Moreover, it will now not only be controllers that will have to ensure compliance with other fundamental data protection principles, but processors also. Again, whilst they too have responsibilities to ensure that exercises such as “privacy by design” or “privacy impact assessments” are carried out when necessary (see below), they may seek to rely on those carried out by the controllers and have the contract allocate risk accordingly.

The application of this sea-change will be difficult, though, in the context of existing contracts since the GDPR does not explicitly address what will happen to those or mention any transitional provisions. Many contracts between controllers and processors may therefore need to be renegotiated.



## Action Points

Processors will begin to look to controllers for assurances that personal data has been collected appropriately and can be used as envisaged, for example, assurances that any necessary consents have been obtained.

Both controllers and processors should review existing contracts and begin a process for replacing them. Particularly old contracts may not have anticipated the changes brought about by GDPR.

Agreements being negotiated now need to be future-proofed. Standard form documents should be revised to take these changes into account.



# 7 | Consent

Consent is a tool often used to justify various processing activities. Whilst consent has always been required to be informed, specific, freely given and revocable, under the current law (at least in some member states) it may often be inferred from circumstances. The GDPR will be stricter: it will require that consent be “unambiguous” by a “clear affirmative action.” This could include ticking a box when visiting a website. However, it is expressly stated that “silence, pre-ticked boxes or inactivity” will not be sufficient. If a data controller relies on consent, the controller has the burden of proof on showing that it was given.

The GDPR contains a limitation that consent cannot be used when there is a “significant imbalance” between

the data subject and the controller. This could be the case, for example, where the controller is a public authority.

Consent will not be freely given if it is unnecessarily tied to the provision of a service.

Where special categories of personal data are concerned (e.g., racial or ethnic origin, political opinions, religious or philosophical belief) processing is generally prohibited unless one of ten exceptions applies. One of those exceptions is that the data subject gives “explicit” consent.

## Relevant provisions

Articles 4 and 7.

---

## Our Commentary

The limitation that consent cannot be relied upon when there is a “clear imbalance” between the data subject and the controller may specifically apply in the context of an employer/employee relationship (which reflects the position currently in some member states).<sup>2</sup> The GDPR mentions in particular a situation where the controller is a public authority.

Perhaps more disruptive of current practice is the suggestion that consent cannot be relied upon if it is tied to the provision of a service: “If you want to buy this download, you consent to us using your data for marketing purposes.” Especially in the context of high demand consumer activities, this type of practice has been relied upon, but DPAs will now be able to stop it.

It would seem that existing consents will still be effective so long as they comply with the new conditions. If businesses have previously collected ‘passive’ consent, e.g., a pre-ticked box, then new consents will need to be collected which represent “clear affirmative action.”



## Action Points

Companies seeking to justify processing activities through consent will need to review their data collection forms and especially the tying-in of consents with service provisions and the use of pre-ticked boxes.

---

<sup>2</sup> The original proposed draft of the GDPR from 2012 had included an express reference to employees in this context.

# 8 | The Right to Erasure (“Right to be Forgotten”)

Individuals will have a new right not present (expressly) in the Directive – the right to require the controller to erase all personal data relating to him where one of a number of grounds applies:

- The data are no longer necessary for the purposes they were collected or otherwise processed.
- The subject withdraws his consent or there is no legal ground for further holding the data.
- The subject objects to the processing of his data and there are no overriding legitimate grounds.

- They have been unlawfully processed.
- Erasure is required for compliance with a legal obligation.

Where the data controller has made the data public, this right would also require the controller to take reasonable steps to inform other controllers that the data subject has requested erasure.

## Relevant provisions

Recitals 65 and 66. Article 17.

---

## Our Commentary

This is a headline-grabbing provision with potentially huge repercussions for social networking and other online businesses. In the *Google Spain* case,<sup>3</sup> a similar right was found to exist by means of a wide judicial interpretation of the current law: the Directive contains obligations on controllers to ensure data is relevant, accurate, not kept for longer than necessary, and rights for individuals to object to data held in breach of these obligations. This has resulted in a multitude of requests being made of Google (in the first two years, approximately 425,000, which is about 580 per day) with approximately 43% of URLs being removed from search results.

Nonetheless, the GDPR language is certainly more direct and arguably much wider with far-reaching implications.

For example, the GDPR allows for the right of erasure where the data have been unlawfully processed. This “catch-all” could result in requests in all manner of situations as there are many ways in which data could be processed unlawfully under the GDPR (for example, issues around the collection of consent or the provision of information in privacy notices).

In addition, the obligation to inform other controllers of the request when the data has been made public seems designed to capture social media sites and the sharing of profiles online. This obligation seems particularly problematic. For example, how is the original controller to go about identifying other controllers once the data is in the public domain?

Lastly, it is worth noting that the existing rules (and how they are being implemented) are controversial. Google

---

<sup>3</sup> *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González*, Case C 131/12, 13 May 2014.



## Action Points

Online businesses and other consumer facing organisations to which this right applies, should begin developing procedures for dealing with requests of this nature.

remains at the forefront of this issue although of course the language is wider than simply applying to search engines. In practice, Google's present policy is to delist a relevant search result from the EU search domains (google.co.uk, google.fr, google.de, etc) and also from the non-EU search domains (especially google.com) when the individual instigating the search is within Europe. Some national regulators, the UK ICO for one, are happy with this stance. However, others (notably the French CNIL) are not. The CNIL has ordered Google to remove relevant results (those deemed "no longer relevant" or inaccurate) from all its search engines. This has resulted in a stark conflict between European fundamental rights to privacy and US constitutional sensibilities around free speech (the First Amendment) and many US commentators are extremely critical of this attempt to export European rules. Google is presently litigating this issue in the French courts.<sup>4</sup>

Whatever the outcome in France of this particular conflict, under the GDPR's "one stop shop" mechanism (see Section 2 above), there should after 2018 at least be a greater possibility to consistency in approach between EU member states.

---

<sup>4</sup> Google announced in May 2016 that it will appeal the CNIL ruling to France's highest court, the *Conseil d'Etat*. A decision from that court is eagerly awaited. The wait may however be prolonged if (as seems possible) the case is referred to the European Court of Justice.

## 9 | The Right to Data Portability

The current law (and the GDPR) already gives a right for the individual to obtain a copy of his data from the data controller (the right of "access"). However, there is an additional right, applicable where that data is stored in an electronic and structured format that is commonly used; namely to have it transmitted to another controller.

It only applies if the controller is relying on consent or on a contract with the individual to justify the

processing. The data must also have been provided to the controller by the data subject.

The right to require that a controller provides the data to a new controller is only applicable "where technically feasible." As such, the GDPR expresses a desire that data controllers should be encouraged to implement interoperable formats that enable data portability.

### **Relevant provisions**

Recital 68. Article 20.

---

## Our Commentary

The intended target of such a provision are social media providers. For example, it would allow users to move from one photo-sharing site to another without hindrance and thus prevent a "lock-in" that is often seen as an issue with such services. This is not strictly a data protection issue (perhaps more a competition law issue) and it is surprising to see this in the GDPR.

There are issues as to how providers are to comply with the provisions for controller-to-controller transfers, which are potentially onerous on controllers. An individual could, it seems, insist that one email provider transfers all archived emails to a replacement provider and indeed to all alternative providers. All of this will be "technically feasible" but there will be a cost.

There are further uncertainties. For example, the right is expressly said to not apply if it adversely affects the rights and freedoms of others. It is in the nature of many social media sites that users can upload not only their own personal data but that also of others. How is a controller expected to assess conflicting rights?



## Action Points

Social media and other organisations expecting to have to deal with requests of this nature, should begin to formulate policies for dealing with them, especially when competitors are likely to be recipients.

# 10 | Accountability: Data Protection by Design and by Default; Privacy Impact Assessments and Records

An important conceptual change in the GDPR is that in return for a loosening of obligations to make regulatory filings in advance of processing, controllers are expected to keep detailed records and to be able to demonstrate compliance with legal obligations and to increasingly embed data protection risk minimisation techniques into their practices. This is referred to as “accountability.”

### **Data Protection by Design**

The GDPR introduces a basic requirement that data controllers implement “appropriate technical and organisational measures” to ensure that personal data meet the requirements of the GDPR (so-called “privacy by design”).

### **Data Protection by Default**

In addition, controllers should ensure that personal data by default is only processed for the purpose for which they have been obtained, and that, by default, the data are not accessible by an indefinite number of individuals (privacy by default). Pseudonymisation is explicitly mentioned as an example of a technique

which can be used to demonstrate adherence to this principle.

### **Privacy Impact Assessments**

Where a proposed processing operation is likely to result in a high risk to the rights of individuals by virtue of its nature, scope, context or purposes, the GDPR requires that a “data protection impact assessment” (or “privacy impact assessment,” PIA) is carried out. Examples are given of where a PIA will be necessary:

- Where there is systematic and extensive profiling of individuals leading to legal or significant effects.
- Where there is large scale processing of special categories of data.
- Where there is a systematic processing of a public area on a large scale.

Where appropriate, as part of such an impact assessment, the controller should consult with data subjects or their representatives. In relation to data about employees, this may necessitate a consultation with works council, for example. Where the assessment determines that there is a high risk, the controller must involve the DPA and obtain their opinion.



## Record Keeping

The GDPR will require all controllers and processors to maintain an extensive amount of documentation, including names and contact details of data protection officers, descriptions of categories of data subjects whose data they hold and so forth. The controller and processor are obliged to make such documentation available to a supervisory authority on request.

There are, though, exceptions for where the controller or processor is an enterprise or organisation with fewer than 250 employees (unless the processing is likely to result in a risk for the rights and freedoms of the data subject, the processing is not occasional, or it includes special categories of data).

## Relevant provisions

Recitals 78, 82 and 90. Articles 5, 25, 30 and 35.

# Our Commentary

Much of the substance of privacy by design, privacy by default and PIAs have long been championed by regulators around the EU and indeed internationally as good practice.


An important contribution to the legislative process that led to the GDPR was a 2009 paper on the “Future of Privacy” from the Article 29 Working Party (a group of EU data protection regulators). This paper, which was part of the European Commission’s pre-legislative consultation), had lamented that the important principles set out in the Directive had often not been:

*“properly embedded in the internal practices of organizations.”<sup>5</sup> They went on to observe that “management ... generally are not sufficiently aware of and therefore actively responsible for the data processing practices in their own organizations” and that “[u]nless data protection becomes part of the shared values and practices of an organization, and unless responsibilities for it are expressly assigned, effective compliance will be at risk and data protection mishaps will continue.”*

These GDPR provisions can be seen as a statutory reflection of the notion that privacy is increasingly embedded into an organisation and that data protection principles should:

*“permeate the cultural fabric of organizations, at all levels, rather than being thought of as a series of legal requirements to be ticked off by the legal department.”*

As the GDPR moves towards its commencement date in May 2018, further regulatory guidance on these important principles can be expected.



## Action Points

Efforts to establish a culture of privacy by design and privacy by default into an organisation’s activities should be accelerated through the process of training and policy development and communication. Projects starting now should take into account these accountability measures.

Businesses should assess whether (or which of) their activities that touch personal data fulfil the criteria for carrying out PIAs, and if so integrate these practices into their development of new products and processes.

This may involve appointing an appropriately senior stakeholder charged with ensuring suitable “accountability.”

<sup>5</sup> *The Future of Privacy*, WP 168, Article 29 Working Party, 1 December 2009.

# 11 | Notification of Personal Data Breaches

The GDPR mandates that, in the event of any personal data breach, the controller must notify the relevant supervisory authority without undue delay, and at any rate within 72 hours where feasible. The only exception is where the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. Where notification is not made within 72 hours, it must when eventually made be accompanied by a reasoned justification. Where a processor becomes aware of a data breach, it is under an obligation to alert and inform the controller without undue delay following the breach.

For certain breaches (where there is likely to be a high risk to the rights and freedoms of the individual) the data subject should also be notified without undue delay (subject to some limited exceptions).

Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data is considered a breach according to the GDPR. This could mean that an employee accessing data not part of their job description is a breach.

## Relevant provisions

Recitals 85 to 88. Articles 33 and 34.

---

## Our Commentary

The current Directive does not contain any obligation to notify data breaches, although one does exist in the telecommunication sector under the e-Privacy directive and there have been some national initiatives (notably in Germany) and much regulatory guidance as to “voluntary” notification (for example, in the UK, the ICO has issued guidance where he expects to be notified of all ‘serious’ breaches).

The introduction of a general obligation is a significant change but reflects a general movement towards such data breach notification laws internationally.

The “where feasible” caveat to the 72-hour time limit is arguably too ambiguous to give much comfort to data controllers who would do all that they can to achieve notification within this short timeframe.



72

Notification of data breach  
must occur within 72 hours



## Action Points

Both controllers and processors will want to review (or begin preparation of) a data breach response plan.

Controllers will want to review existing contracts with service providers and if necessary negotiate amendments to seek obligations to cooperate and assist in responding; for example, requiring the processor to notify in time for it to comply with its own obligations. They will wish to take these types of measures into account in future contracts.

# 12 | Data Protection Officers

Controllers and processors will each be obliged to designate data protection officers (DPO) where:

- The processing is carried out by a public body.
- The core activities consist of regular and systematic monitoring of data subjects on a large scale.
- The core activities consist of processing on a large scale of special categories of data.

The DPO's role will be to advise and monitor GDPR compliance, as well as being the company representative for contact with the supervising authority.

In addition, the DPO must be suitably qualified and must report to the highest level of management. The controller or processor must communicate the identity of the DPO to the relevant supervisory authority and data subjects will have the ability to contact the DPO directly.

The controller or processor must ensure the DPO receives proper support.

## **Relevant provisions**

Articles 37 to 39.

---

## Our Commentary

Some EU countries (including Germany) already have mandatory requirements for the appointment of DPOs, but for other countries this will be a big change. A DPO can be an employee but need not be. Germany already has an industry of external DPOs and this may be expected to arise elsewhere.



### Action Points

Organisations that fall within the qualifying criteria should seek to identify suitable candidates to undertake these important roles.

# 13 | International Transfers

As is well known, the Directive contains a fundamental rule that personal data cannot be transferred unless “adequately” protected. These rules largely remain unchanged. The GDPR contains:

- Mechanisms for approval of “model clauses.”
- The ability for the European Commission to deem “adequate” the laws of other countries or of particular types of transfers to other countries.
- Statutory recognition of “binding corporate rules” (which are now expressly mentioned).
- Derogations to these rules such as reliance on consent, the necessity to transfer data to fulfil a contract with the data subject, the necessity to transfer the data for handling legal claims.

“Safe Harbor,” a scheme allowing transfers to entities in the US that had self-certified to certain principles, was declared invalid by the European Court of Justice in October 2015.<sup>6</sup> The statutory mechanism for a replacement scheme to be adopted remains in the GDPR.

<sup>6</sup> *Schrems v Data Protection Commissioner of Ireland*, Case C-362/14, 6 October 2015.

One notable change though is that the removal from the law of some member states (notably the UK) of a mechanism that was much relied upon in practice; namely, the ability for the controller itself to assess the adequacy of protection without needing to undertake a “formal” step such as “model clauses” or “binding corporate rules”, has been removed. In place of this, a further derogation of ‘legitimate interests’ has been added and may be used where transfer is not repetitive, concerns only a number of data subjects, is necessary for compelling legitimate interests, the circumstances have been assessed and suitable safeguards put in place. The supervising authority must also be informed.

Various countries currently require a prior authorisation before a transfer can take place (even if an approved exception applies). This will no longer be required.

To rely on consent, which now needs to be “explicit,” a controller would need to ensure that the individual was informed of the risks due to the absence of adequate protection.

**Relevant provisions** Articles 44 to 49.

## Our Commentary

The lack of a complete overhaul of the law relating to international transfers might be seen as a missed opportunity. Many in the business community, and some regulators, have long been critical of the Directive rules and had hoped that the GDPR would be more flexible. The UK ICO for example had criticised these rules as being too overbearing; it believes organisations should be able to determine the level of risk incurred when transferring data and be subject to the appropriate penalties should they fail to do so. Businesses in the UK will feel the loss of “self-assessment” keenly.

At the time of writing, a replacement to Safe Harbor (the Privacy Shield) has been published but not yet adopted.



### Action Points

Controllers in those countries which allowed some form of “self-assessment” as to adequacy (for example, the UK) should look to put in place other forms of legitimising data transfers.

Multi-national businesses should look to adopt a comprehensive framework of contracts or to put in place binding corporate rules.

# 14 | Representation of Data Subjects

The GDPR contains a right for the data subject to mandate a representative body (which fulfils certain requirements including that it is not for profit and that it has the public interest as its statutory objective) to exercise some of its rights; namely, to lodge a complaint with the regulator, to seek a judicial remedy against the regulator and to seek an effective judicial remedy against a controller or a processor. In addition, the member states may allow the representative body (mandated by the individual) to exercise the

individual's right to compensation, but this provision is not obligatory.

The GDPR also allows (but does not oblige) a member state to permit the representative body to bring actions directly against regulators, controllers or processors (even without a data subject mandate).

## **Relevant provisions**

Article 80.

---

## Our Commentary

Most prominent EU countries, including Italy, Spain and the UK, do not currently permit actions by consumer associations or the like. Although France permits claims by consumer groups, the limited scope of the law here does not cover data protection breach. Alone amongst the major economies, Germany has recently brought in a law that permits consumer protection associations and other associations to bring class action-like claims against businesses for breach of German data protection law.

Following the entry into force of the GDPR, there will be partial harmonisation in this area, but not full harmonisation since certain important rights are subject to member state discretion.

# Glossary

<b>Article 29 Working Party</b>	The body set up by Article 29 of the Directive to provide guidance on the operation of the Directive. There are 28 members, one from each of the member states.
<b>Binding corporate rules</b>	An internal policy adopted by a group of companies, and approved by European data protection authorities, permitting that group to share personal data (of which a group member is a data controller) amongst its members even outside of the European Union.
<b>Controller</b>	The company, body or other person that determines the purposes and means of the processing of personal data.
<b>Directive</b>	Directive 95/46/EC 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. It is repealed by the GDPR.
<b>Data Protection Authority</b>	See supervisory authority (below).
<b>EEA (European Economic Area)</b>	The European Union together with Iceland, Liechtenstein and Norway.
<b>EU (European Union)</b>	Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.
<b>GDPR (or Regulation)</b>	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). It will come into force on 25 May 2018.
<b>Member state</b>	A member country of the European Union.
<b>Personal data</b>	Data relating to identified or identifiable individuals; the subject of data protection legislation.
<b>Privacy Shield</b>	A proposed scheme, to replace Safe Harbor, under which US entities can self-certify to facilitate the transfer to them of personal data from Europe. At the time of writing it was still under scrutiny.
<b>Processing</b>	Any operation performed on personal data such as collection, recording, consultation, use, disclosure, erasure or destruction.
<b>Processor</b>	The company, body or other person that processes personal data on behalf of the controller; typically, a service provider to the controller.

<b>Pseudonymization</b>	The manipulating of personal data to replace the identifying feature with a “key” which is then needed to attribute that data to a specific data subject.
<b>Safe Harbor scheme</b>	A scheme under which US entities can self-certify to an overarching set of data protection principles and so facilitate the transfer to them of personal data from Europe. It is no longer recognised as a sufficient means of ensuring adequacy as a result of the 6 October 2015 decision of the European Court of Justice in <i>Schrems v Data Protection Commissioner of Ireland</i> .
<b>Standard clauses (or model contracts)</b>	Three different sets of model contracts approved by the European Commission to ensure compliance with the eighth data protection principle.
<b>Supervisory authority</b>	The national authorities (one or more per member state) charged with monitoring the application of the GDPR. Under present law and practice they are often referred to as data protection authorities (DPA).

# Our Team

## **Renzo Marchini**

Author, Special counsel  
London  
+44 20 7184 7563  
renzo.marchini@dechert.com

## **Timothy C. Blank**

Partner  
Boston  
+1 617 728 7154  
timothy.blank@dechert.com

## **Mark Browne**

Partner  
Dublin  
+353 1 436 8511  
mark.browne@dechert.com

## **Charles Wynn-Evans**

Partner  
London  
+44 20 7184 7545  
charles.wynn-evans@dechert.com

## **Dr. Olaf Fasshauer**

National partner  
Munich  
+49 89 21 21 63 28  
olaf.fasshauer@dechert.com

## **Giovanni Russo**

National partner  
Munich  
+49 89 21 21 63 16  
giovanni.russo@dechert.com

## **Sabrina Chekroun**

Associate  
Paris  
+33 1 57 57 80 56  
sabrina.chekroun@dechert.com

## **Jennifer McGrandle**

Associate  
London  
+44 20 7184 7800  
jennifer.mcgrandle@dechert.com

## **Sophie Montagne**

Associate  
Paris  
+33 1 57 57 80 47  
sophie.montagne@dechert.com

© 2016 Dechert LLP. All rights reserved. This publication should not be considered as legal opinions on specific facts or as a substitute for legal counsel. It is provided by Dechert LLP as a general informational service and may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome. We can be reached at the following postal addresses: in the US: 1095 Avenue of the Americas, New York, NY 10036-6797 (+1 212 698 3500); in Hong Kong: 27/F Henley Building, 5 Queen's Road Central, Hong Kong (+852 3518 4700); and in the UK: 160 Queen Victoria Street, London EC4V 4QQ (+44 20 7184 7000). Dechert internationally is a combination of separate limited liability partnerships and other entities registered in different jurisdictions. Dechert has more than 900 qualified lawyers and 700 staff members in its offices in Belgium, China, France, Germany, Georgia, Hong Kong, Ireland, Kazakhstan, Luxembourg, Russia, Singapore, the United Arab Emirates, the UK and the US. Further details of these partnerships and entities can be found at [dechert.com](http://dechert.com) on our Legal Notices page.