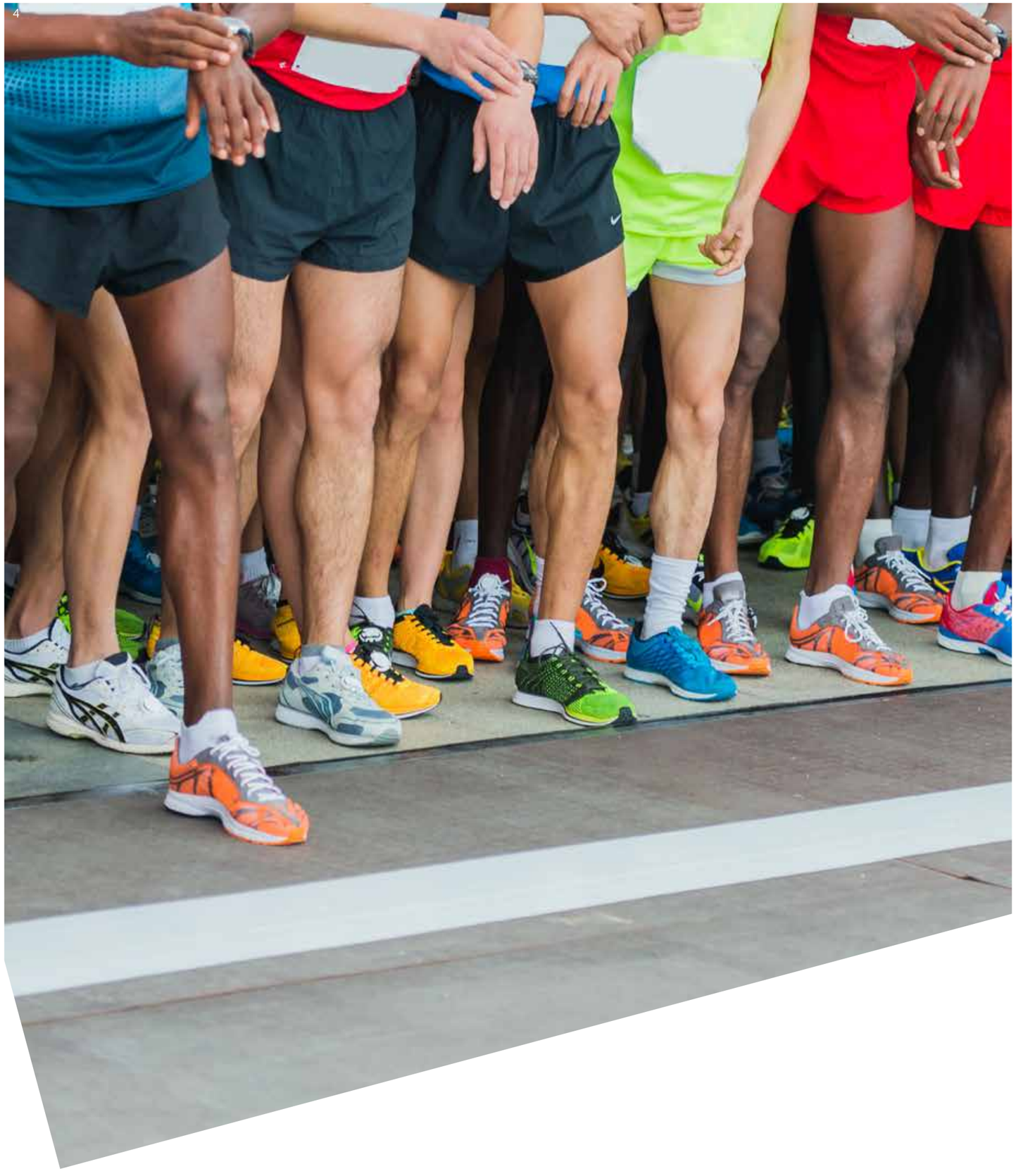
Hogan Lovells

Future-proofing privacy

A guide to preparing for the
EU Data Protection Regulation

Table of contents



The time has come

Eduardo Ustaran

It has taken several years but we have finally made it to the start line. The modernisation of European privacy laws has reached a critical milestone and with the formal adoption of the new data protection framework, we can now begin to lay the foundations for the future.

Influenced by overwhelming technological advances and the Snowden revelations, the EU Data Protection Regulation introduces new accountability obligations, stronger rights and ongoing restrictions on international data flows. Overall, the new framework is ambitious, complex and strict.

Businesses operating in Europe or targeting European customers need to get their act together and start preparing for the new regime. At stake are not only the consequences of non-compliance, but also the ability to take advantage of new technologies, data analytics and the immense value of personal information. From determining when European law applies to devising a workable cooperation strategy with national regulators, there are many intricate novelties to understand and address.

Our guide "Future-proofing privacy" aims to be a useful starting point. 24 authors from 10 European Hogan Lovells offices have contributed their knowledge, efforts and advice to compile a unique resource of practical guidance. We have identified the key issues and explained why they matter. Crucially, we have approached the new framework with a practical mindset, providing concrete suggestions for actions to take now.

Our team's close involvement in the development of this framework has given us the opportunity to point out where the challenges lie and, more importantly, how to deal with them in a responsible and effective way. I am immensely grateful to the entire European team of our leading Privacy and Cybersecurity practice – with a special mention to my co-editor Mac Macmillan – and I hope that this guide is helpful in ensuring that privacy practices can contribute to prosperity and innovation.

Data protection reform - the story until now

The European Union (the "EU") has long been a trail blazer for data protection. When it passed Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Data Protection Directive"), it created what has often been described as a gold standard for data protection.

Although the authors of the Data Protection Directive consciously drafted a technology-neutral instrument, the publication in January 2012 by the European Commission (the "Commission") of a draft proposal (the "Commission draft") for a General Data Protection Regulation (the "Regulation") confirmed the need for a wholesale reform. Following the numerous amendments to the Commission draft proposed by the European Parliament (the "Parliament") in 2014, it was left to the Council of the EU (the "Council") – which shares legislative powers with the Parliament – to put its proposal on the table.

Once this was done, the Commission, the Parliament, and the Council began a negotiation process known as the trialogue in June 2015. During this process the draft of the Regulation approved by the Parliament (the "Parliament draft") and the one agreed within the Council (the "Council draft") were thoroughly debated and following a degree of compromise by all involved, a final version of the Regulation emerged at the end of 2015.

Following its official publication in the early summer of 2016, there will be a two year transition period before it becomes enforceable by data protection authorities ("DPAs"). This may seem like a long time at the moment, but given the number of potential stakeholders in large organisations, and the lead times on IT projects, it may come to seem like not long at all. One thing is certain: after years of negotiations to craft a robust and influential law, the resulting framework will become a focal point of reference for global privacy and data protection compliance, so now is a good time to start planning!

Scope of the application of the law

Quick read

- If an organisation is established in the EU, whether as a controller or processor, the Regulation will definitely apply.
- Non-EU controllers or processors that offer goods or services to, or monitor the behaviour of individuals who are in the EU will also be caught by the Regulation.
- For the law to apply there is no longer a focus on the use of equipment located on the territory of an EU Member State – instead, the focus is on the targeting of individuals in the EU.

Scope of the application of the law

Nils Rauer and Victoria Hordern

What difference does a Regulation make?

Unlike EU 'directives', EU 'regulations' are by nature directly effective in EU Member States and so do not require further implementation into national laws. Previously, European data protection law was governed by the Data Protection Directive. It was the responsibility of Member States to implement the Data Protection Directive into their national law. When the Regulation becomes law, it will apply immediately throughout the EU due to its direct effect. As a consequence, national data protection acts will cease to be relevant for all matters falling within the scope of the Regulation.

Why does this matter?

It is absolutely crucial for organisations to know if they are or are not subject to the Regulation. Since the Regulation strengthens data protection principles, requires organisations to demonstrate compliance and ushers in greater enforcement powers for regulators, it is essential for all organisations, public and private, local, national or global, to understand in what circumstances the Regulation will apply to their use of personal data.

When will the Regulation apply?

The Regulation will be applicable in three situations:

1) Established in the EU

The Regulation applies when an organisation (whether a controller or processor) is processing personal data in the context of the activities of an establishment in the EU, whether the actual processing takes place within the EU or not. This rule retains the concept of processing data in the context of an establishment based in the EU which is included in the current Data Protection Directive. Therefore, the presence in the EU of a branch or subsidiary or only a single individual may all bring the data processing activity (whether the EU presence is acting as a controller or processor) within the scope of the Regulation

What this means

For many organisations (companies, branches, partnerships etc.) based in the EU there is no change since they are already acting as controllers established in the EU and required to comply with the current Data Protection Directive. The Regulation clarifies that it is irrelevant if the actual processing takes place within the EU or not (i.e. the data could be stored on clouds in the US). An organisation established in the EU making decisions about the processing of personal data (wherever that processing occurs) in the context of its activities is caught by the Regulation.

However, now entities that are established in the EU and act as processors when processing client data (e.g. technology service providers) will be required to comply with the Regulation and not just with their contractual obligations to their clients. This will require processors established in the EU to assess what obligations under the Regulation apply to them and take the necessary steps to comply.

2) Individuals in the EU

In order to ensure that organisations cannot avoid their responsibilities under EU data protection law simply through being located outside the EU, the Regulation introduces a new provision which is based primarily on processing the personal data of individuals in the EU. If a non-EU organisation is processing the personal data of individuals in the EU for activities relating to:

– Offering goods or services to such individuals; or

– Monitoring their behaviour

then such non-EU organisations are required to comply with the Regulation.

What this means

All non-EU organisations that collect data on individuals through websites and other remote interactions are now potentially susceptible to the scope of the application of the Regulation. This is the biggest change to the applicable law rule under the Regulation.

Non EU-organisations will need to consider whether they are involved in online offerings of goods and services or monitoring activities that are directed at individuals in the EU. Merely being able to access a website in the EU, or an email address, or contact details or the use of a language used in a non-EU country are not in themselves sufficient to determine the intention by a non-EU organisation to offer goods and services to individuals in the EU. However, it seems that the use of a language or currency generally used in a Member State, the possibility of ordering goods and services in that language, and/or referring to users or customers in the EU are likely to indicate that the controller envisages offering goods or services to individuals in the EU.

In determining whether processing amounts to monitoring of behaviour, the recitals to the Regulation indicate that it should be ascertained whether individuals are tracked on the internet including potential subsequent use of data processing techniques which consist of profiling them, particularly in order to take decisions concerning them or to analyse or predict their preferences, behaviours and attitudes. The language looks primarily designed to catch online behavioural advertising networks (although there will be other services) that create profiles according to the behaviour of a device online (and behind the device, an individual) and then serve up relevant ads. This moves the focus away from identifying 'equipment' located in the EU (as required under the Data Protection Directive) and onto the actual deliberate activity of targeting individuals in the EU.

All non-EU organisations that collect data on individuals through websites and other remote interactions are now potentially susceptible to the scope of the application of the Regulation. This is the biggest change to the applicable law rule under the Regulation.

3) Public International Law

The Regulation applies to controllers not established in the EU but in a place where the national law of a Member State applies by virtue of public international law.

What this means

This is the same rule from the Data Protection Directive and is designed principally to capture data processing by Member States' overseas diplomatic establishments.

Judicial and regulatory support for a broad scope

Recently courts and regulators have indicated their support for a broad interpretation of the rule on the applicability of the law which complements the position under the Regulation. In its decision of May 2014 (known as the Google Spain 'right to be forgotten' decision) the Court of Justice of the European Union (CJEU) found that the advertising sales generated by Google Spain (the local subsidiary of the US company Google Inc.), were sufficiently linked to the Google search activities that the individual affected complained about. Even though Google Spain neither designed nor operated Google's search business in Spain, because the data processing at issue related to the search business which Google Spain's sale of online advertising space helped to finance, this was processing of personal data carried out 'in the context of the activities' of the Spanish establishment. Therefore, the Data Protection Directive applied to the data processing the individual complained about.

Similarly the Belgian Privacy Commissioner (in May 2015) issued a recommendation that clarified that Belgian law applied to Facebook's activities in Belgium regardless of the arguments Facebook made that the data controller of its processing in the EU was established in Ireland and therefore its processing was subject to Irish data protection law.

In October 2015, the CJEU ruled in *Weltimmo* that the concept of 'establishment' under the current Data Protection Directive should be interpreted broadly. In the CJEU's view even minimal activities in a Member State can trigger the application of the local law of that Member State. This decision therefore risks dislodging the long-standing country of origin principle under the Data Protection Directive, under which an organization established in one Member State only has to observe the data protection law of that Member State even when it processes personal data about individuals resident in other Member States.

Following the CJEU's Google Spain decision in May 2014, the CJEU's decision in *Weltimmo* in October 2015 and increasing regulator activism, all global businesses should take note of how they may be brought within the scope of the Regulation even if it appears that a non-EU based part of their business is involved in different services from EU operations.

What to do now

- Identify any processor entities established in the EU and initiate a plan to ensure that such entities comply with their applicable obligations under the Regulation.
- Non-EU organisations should consider whether they could be considered to be 'established' in the EU even if they are only engaged in minimal activities in a Member State.
- Non-EU organisations should assess whether their online presence will fall within the rules of offering goods or services to, or monitoring of, individuals in the EU. Where this is the case, they should assume that the Regulation will apply.
- While global businesses without a clearly identified EU-based controller have in the past positioned an entity in one EU Member State as the entity through which they conduct all data processing subject to EU rules, this strategy will be under much greater scrutiny following the *Weltimmo* decision. For some controllers it will be additionally important to facilitate an ongoing dialogue with the data protection regulator of that Member State to explain its position.

The concept of personal data revisited

Quick read

- The Regulation confirms that location data, online identifiers or other factors relating to an individual are personal data.
- In between personal data and anonymous data, the Regulation introduces a third category: pseudonymous data.
- Pseudonymous data is subject to the Regulation, but the applicable requirements are less stringent.
- The Regulation encourages organisations to apply pseudonymisation, which facilitates the processing of personal data for scientific, historical and statistical purposes or for secondary purposes.
- Genetic data and biometric data are both defined for the first time, and included among the special categories of data where they are being processed in order to uniquely identify a person.

The concept of personal data revisited

Massimiliano Masnada, Mac Macmillan and Giulia Mariuz

What's the deal?

Pseudonymisation enters the stage

Along with the concept of personal data, as opposed to anonymous data, the Regulation introduces a third category, that of pseudonymous data. Pseudonymous data is information that no longer allows the identification of an individual without additional information and is kept separate from it. Pseudonymisation, while granting higher data security, also enhances data utility. In exchange for the lower level of privacy intrusion, and in order to encourage data controllers to resort to pseudoanonymisation, certain requirements are less stringent.

As a result, the complexities surrounding the concept of personal data are likely to increase given the three possible categories of information:

- The framework set forth by the Regulation applies to **personal data**, defined as any information relating to a natural person who can be identified, directly or indirectly, by reference to an identifier. The Regulation expressly considers as identifiers a name, an identification number, location data, online identifier or other factors related with the physical, physiological, genetic, mental, economic, cultural or social identity of a person. In this respect, the Regulation is crystal clear about the fact that technology-based identifiers such as MAC addresses qualify as personal data.
- A**nonymous data**, which is information not related to an identified or identifiable natural person, or data that does not allow identification of an individual, is therefore excluded from the scope of the Regulation.
- In between personal and anonymous data there is a third category, so-called **pseudonymous data**. Pseudonymous data does not directly disclose a data subject's identity, but it may still identify an individual by way of association with additional information. Under the Regulation, pseudonymous data is still regarded as personal information and therefore subject to data protection guarantees.

Crucially, the Regulation creates incentives for controllers applying pseudonymisation, as the regime affecting pseudonymous data is less stringent. For example, pseudonymisation is a measure for processing personal data for scientific, historical and statistical purposes. In addition, data controllers might be facilitated to process pseudonymous data beyond their original collection purposes. Accordingly, in the context of the privacy by design, pseudonymisation will play a great role, representing a good practice that should be implemented, together with other guarantees, in order to ensure safe data processing.

New types of regulated data

The Regulation introduces a number of new definitions of special categories of data.

Genetic data is defined as personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question. Biometric data is defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data. Both these new categories of data are included among the special categories of data, but only where they are being processed in order to uniquely identify a person.

The Regulation also contains a definition of "data concerning health": personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status. Member States are given the right to introduce further conditions, including limitations, relating to processing in relation to all three of these categories of special data.

There are new grounds for processing special categories of data that facilitate the processing of health data for scientific (i.e. research) purposes. Health data may also be processed for public interest reasons in the area of public health, such as protecting against serious cross-border threats or ensuring high standards of quality and safety of health care on the basis of Union law or Member State law which provide for suitable protections, in particular professional secrecy. There is also a new ground of processing where necessary for the purposes of preventive or occupational medicine, and for the assessment of the working capacity of the employee which will be useful for employers.

In some of the drafts of the Regulation data protection impact assessments were mandatory for certain processing of special categories of data. These are no longer expressly mentioned. Instead the requirement for a data protection impact assessment is linked to processing "likely to result in a high risk for the rights and freedoms of individuals". DPAs may publish a list of the kind of processing operations which fall within this requirements, and it is likely that at least some processing of health data will require privacy impact assessments.

Likely practical impact

A key takeaway from this myriad of concepts is that those using pseudonymous data in the context of their activities (e.g. for R&D purposes, or in the health sector for clinical studies) will have to assess the anonymisation and pseudonymisation techniques being used, in order to establish whether the processed data is subject to data protection principles or not.

However in general terms and looking at the glass half full, we are heading for greater flexibility for organisations involved in the processing of personal data for scientific research and public health purposes, as long as certain privacy enhancing measures are in place.

What will happen next?

At the moment the standards according to which data is considered as anonymous or pseudonymous are established by the DPAs at a national level. Once the Regulation comes into force, the requirements and the applicable regime will become more uniform and this will provide greater legal certainty.

What to do now

- Assess the different types of information handled by the organisation in line with the new categories in the Regulation.
- Determine whether it will be possible to benefit from the greater flexibility afforded to pseudonymous data.
- Plan and develop processes for carrying out data protection impact assessments (for example for profiling or use of biometric data).

Justifying data uses – from consent to legitimate interests

Quick read

- Each instance of personal data processing requires a valid ground for processing.
- The main grounds for data processing include consent, performance of a contract, compliance with a legal obligation, and the legitimate interests of the controller.
- With the Regulation, the bar for showing the existence of certain grounds for processing will be set higher – for example with strict new requirements for obtaining consent.
- The processing of sensitive personal data is subject to a special, even more stringent regime.

Justifying data uses – from consent to legitimate interests

Gonzalo Gallego, Ewa Kacperek and Lanah Kammourieh

Grounds for processing

Currently, under the Data Protection Directive, each instance of data processing requires a legal justification – a "ground for processing". This fundamental feature of EU data protection law will remain unchanged under the Regulation. However, the bar for showing the existence of certain grounds for processing will be set higher. This is especially true with regards to consent.

Stringent new consent rules

The Regulation lays out strict new conditions for obtaining valid consent from the data subject.

For starters, if consent is given in a written document, and that document also concerns other matters (e.g. terms of service), then the request for consent must be presented in a form that is distinguishable from the rest of the document. It must also be formulated in clear and plain language. For many companies, this will require reviewing existing contracts, general terms and conditions, and other documents to clearly distinguish the consent portion and ensure it is written in layman's terms. In addition, the Regulation requires that it be "as easy to withdraw consent as to give it" at any time the data subject wishes.

Consent must also be given freely. The Regulation flags up the common practice of making consent to data processing a condition for performance of a contract (like the provision of a service), even when such data processing is not necessary to performance. While the Regulation does not clearly outlaw this practice, it warns that "the utmost account" will be taken of such facts in determining whether consent was truly freely given. This may prove a significant hurdle for many companies. This provision will also, in all likelihood, cover situations of power imbalance, such as an employer-employee relationship, where the employee might feel that consent to data processing is not truly optional.

One grey area remains: the Regulation does not state clearly whether implied consent (i.e. consent inferred from the conduct of the individual) will be valid or not. The text defines consent as a specific, informed, and unambiguous indication of the subject's wishes – and adds that it can be given "by a statement or by a clear affirmative action". This suggests that consent may be construed from the subject's actions, but that it will be subject to a strict test: those actions will have to be a clear manifestation of intent. The negotiation process that led to the adoption of the Regulation also sheds light on this. The Council's draft initially required all consent to be "explicit", but the final text does not. Tellingly, "explicit consent" is required where sensitive categories of personal data are concerned; but all other types of personal data processing require only "consent". This suggests there will remain some place, however limited, for implied consent.

Protection of children

Children benefit from additional protection under the Regulation. Any consent given by a child (the cutoff age may vary from 13 to 16 depending on the Member State concerned) in an online context will only be valid if it is either given or authorised by the child's legal guardian. The data controller also has the responsibility to make reasonable efforts to verify that consent was in fact given by the child's legal guardian.

Other grounds for data processing

Contrary to popular belief, a data subject's consent is not the most frequent justification for the use of personal data. A valid ground for data processing is where it is necessary for the performance of a contract concluded with the data subject or, prior to entering into a contract, if the data subject has requested that pre-contractual activities be undertaken.

Another basis, which is significant from a practical point of view, is where the processing is undertaken by the data controller in order to comply with a legal obligation.

Crucially, both the Data Protection Directive and the Regulation also contain a provision under which a controller can justify data processing on the basis of pursuing his/her/the company's legitimate interests. When relying on this ground, those legitimate interests should be weighed against the fundamental rights and freedoms of the individual. Only when those rights do not override the legitimate interests of the controller are such legitimate interests a valid ground for processing. This balancing must be carefully assessed in practice in order for the controller to be confident that it provides a solid ground for on-going data processing activities.

Sensitive personal data

Under the Regulation, a special category of personal data – termed "sensitive personal data" – will continue to enjoy a higher level of protection. The types of information regarded as sensitive are expressly listed: they include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning a person's health or sex life. The GDPR also adds new categories to those already protected under the Data Protection Directive: genetic data and biometric data where they are processed in order to uniquely identify a person.

The peculiarity of sensitive personal data is that, as a rule, its processing is prohibited, unless certain specifically listed exceptions apply. These include the consent of the data subject or the fact that the data subject has made the information public. Another justification for processing of sensitive personal data is the need to use such data in the establishment, exercise, or defence of legal claims. Some new processing grounds are added in the Regulation: the processing of sensitive data can be justified for reasons of substantial public interest, for individual health purposes, public health reasons, or for archiving, scientific, historical, or statistical purposes linked to the public interest. One must remember, however, that any exception to the general rule prohibiting the processing of personal data will be interpreted narrowly.

Other special categories of data

The GDPR provides additional safeguards in connection with the processing of data relating to criminal convictions and offences, as well as processing for historical, statistical and scientific research purposes. Member States are also free to adopt further safeguards for the processing of genetic, biometric, and health data.

Cessation of processing

The processing of personal data is both "purpose-limited" and "storage-limited": it can be carried out only for a specific purpose, cannot be stored longer than necessary for that purpose, and cannot be further processed in a way incompatible with that purpose.

What to do now

- Businesses will need to review their existing templates and procedures to ensure any consents requested from data subjects are easy to understand and clearly distinguished from other terms and conditions.
- Businesses processing personal data of minors under 13 on the basis of consent will need to prepare strategies for obtaining guardian consents or authorisations.
- Controllers in positions of power over the data subject (such as employers), or controllers who condition the provision of services on user consent to data processing, will need to minimise reliance on such consent.

New and stronger rights

Quick read

- The Regulation retains existing rights such as subject access, rectification, erasure, and to object.
- It also introduces the new rights of data portability, the right to restriction of processing, the right to be forgotten, and certain rights in relation to profiling. Profiling is likely to require consent.
- The Regulation adds to the categories of information that must be provided to individuals. However organisations will now be able to have a single privacy notice where they have establishments in different Member States.
- The Regulation expands the level of information to be provided to individuals making subject access requests and removes the right to charge a fee unless the request is 'manifestly excessive'.

New and stronger rights

Massimiliano Masnada, Sian Rudgard and Giulia Mariuz

What's the deal?

The Regulation aims to strengthen the rights of individuals. It does so by retaining rights that already exist under the Data Protection Directive and introducing the new rights of data portability, the right to be forgotten, and certain rights in relation to profiling. In this chapter we look at each of these rights in turn and assess the likely practical impact that the changes brought about by the Regulation will have on organisations.

Clearer information provision

Consumer groups often complain that information notices are too long and difficult for consumers to understand. This issue has become more significant as personal data is now collected in a variety of different situations (for example through mobile devices and the internet of things), where the nature of data collection and processing is less obvious. The Regulation requires controllers to tell individuals how their information will be used in clear and plain language, adapted to the individual data subject. For example, if information is being collected from a child, the language of the notice must be such that a child can understand it.

The information notice must contain the following:

- The identity and contact details of the controller; any representative of the controller; the data protection officer; and any recipients, or categories of recipients of the personal data
- The purposes and legal bases of the processing (including, where the processing is based on the legitimate interests of the controller or a third party, a description of those legitimate interests)
- Where processing is based upon consent, reference to a right to withdraw such consent without affecting the legitimacy of prior processing
- If the processing involves automated decision-making, including profiling, information about the logic involved, including the consequences for the individual
- The period for which the personal data will be stored, or the criteria used to determine this
- The nature of the rights of available under the law, including the contact details of, and the right to complain to, the relevant supervisory authority
- Where applicable, if the personal data is to be transferred to a third country, the level of protection afforded by that third country by reference to an adequacy decision, or details of the safeguards adopted by controllers in the absence of an adequacy decision
- Where personal data is not collected directly from the individual, the sources and categories of the personal data
- Any further information to ensure that the processing of the personal data is fair

In addition, where information is collected directly from a data subject the controller must also tell the data subject whether the provision of personal data is obligatory (such as a statutory or contractual requirement) or voluntary, as well as the possible consequences of failing to provide such data.

If a controller intends to carry out processing that is not covered by the original information notice, the controller must provide additional information to a data subject prior to such processing to ensure that the processing is fair.

The right of subject access

The right of subject access permits individuals to request the personal data that is being processed by the controller. The Regulation makes some additions to the detailed information to be provided in response to a request, and also makes some procedural changes:

- Controllers must put in place a process for dealing with requests
- Where a request is made in electronic form, the information must be provided in electronic form, unless the data subject requests otherwise
- Controllers may no longer charge a fee unless the request is 'manifestly unfounded or excessive', for example where it is repetitive in character. The onus is on the controller to demonstrate the manifestly excessive character of the request
- The controller must provide the requested information within one month of receipt of the request. This is less time than allowed by some Member States at present. There is potential for an extension period, but it only applies in very limited circumstances.

The right to rectification

The Regulation retains the right to obtain from the controller rectification of personal data which are inaccurate and to obtain completion of incomplete personal data, including by way of supplementing a corrective statement with very little change.

The right to object

The Regulation broadens the current right to object to data processing. In particular, a data subject is always entitled to object to processing carried out on the basis of a legitimate interest of the controller or for the purposes of direct marketing without the need of indicating specific justifications.

The right to restriction of processing

The Regulation introduces the right to obtain restriction of the processing that can be exercised, for example, while complaints (for example, about accuracy) are pending, or if the processing is unlawful, but the data subject objects to erasure of the data.

If a controller intends to carry out processing that is not covered by the original information notice, the controller must provide additional information to a data subject prior to such processing to ensure that the processing is fair.

The right to be forgotten and to erasure

The Regulation gives data subjects the right to have their personal data erased, provided that certain conditions are met. In particular, the data must be erased when:

- it is no longer needed for its original purpose
- the data subject withdraws consent and there is no other legitimate basis for the processing
- the data subject objects to the processing
- the data must be erased in order to comply with a legal obligation to which the controller is subject
- the data has been collected in relation to the offering of information society services to children
- the processing is unlawful

This right to be forgotten was one of the most controversial aspects of the Regulation when it was first published, not least because the practical limits on a controller's obligation to delete data were unclear. Following the decision in Google v Costeja, the right to have data erased no longer represents such a dramatic change, but it remains to be seen what the extent of the obligation will be in practice, as the Regulation proposes a number of limits, such as, for instance, when the processing is necessary for exercising the right of freedom of expression and information.

The right to data portability

The Regulation gives individuals the right to have a copy of their personal data in a commonly used electronic and structured format that allows for further use, including by other data controllers. This right raises both practical and commercial issues for most controllers, and the Regulation proposes the right shall apply only to data that was provided by the data subject to the data controller. The Article 29 Working Party has indicated that issuing guidance on this new right is a priority for them.

Profiling

Profiling is discussed in more detail elsewhere in this publication. Briefly, under the Regulation the data subject will have the right not to be subject to a decision entailing the evaluation of personal aspects relating to him based solely on automated processing and having direct legal effects on (or affecting) him, save where the processing is on certain specified grounds.

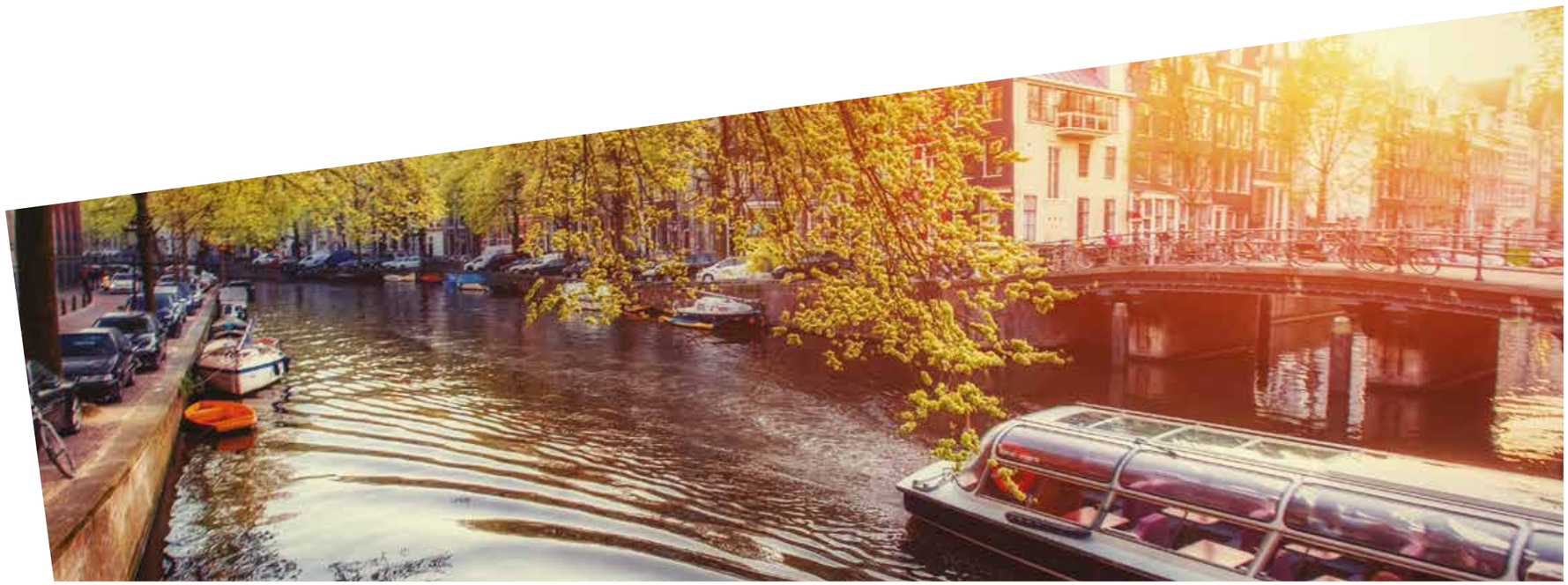
Likely practical impact

The accountability approach built into the Regulation means that organisations must be able to demonstrate that they have procedures in place for dealing with their obligations to data subjects. In addition to creating such processes, organisations will need to review their existing information notices to assess whether they contain all necessary information, and whether this information is easily understood. Some organisations may already be operating to a higher standard in some countries because of provisions under their local law. An advantage of the Regulation, therefore, is that controllers will be able to have identical notices across Member States.

The new rights to erasure and data portability will almost certainly require IT system changes. The detail of these changes is not settled yet, but given project lead times organisations may need to start alerting their IT teams to the forthcoming need for these changes.

What to do now

- Review current information notices to ensure that they are accurate, comprehensive, and up to date. Consider whether any additional information will be required under the Regulation, and whether the language is sufficiently clear for the target audience.
- Consider whether you need to create procedures for handling requests from data subjects to exercise their rights.
- Identify your current profiling activities and assess whether they meet the requirements or the Regulation.
- Consider how to implement appropriate consent request mechanisms for profiling.



Profiling restrictions v Big Data

Quick read

- Profiling is a discrete data processing activity that will be strictly regulated.
- Many restrictions apply to automated data processing such as profiling, including strict information obligations and duty to honour data subjects' right to object.
- Prior consent to profiling is likely to be required in many instances.
- Given the perceived risks of profiling, this simply must become a compliance priority.

Profiling restrictions v Big Data

Joke Bodewits and Patrice Navarro

A stricter regime for profiling

Profiling and big data analytics are set to play a pivotal role in the growth of the digital economy. From cookie-based tracking to people's interaction through social media, the size and the degree of granularity of our digital footprints have created unprecedented opportunities for business development and service delivery. The scale of data collection, data sharing and data analysis has not gone unnoticed to public policy makers and this has led to the inclusion of special rules addressing profiling in the Regulation. In fact, from the point of view of those businesses seeking to benefit from data analytics, the provisions dealing with profiling are likely to become the most crucial aspect of the entire Regulation.

When the Data Protection Directive was adopted, back in 1995, no one could imagine that people's relentless use of technology would become the main source of personal data and that in turn this would lead to the current explosion of Big Data analytics. The approach of the Data Protection Directive is to say that data subjects have a general right 'not to be subject to a decision which produces legal effect concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him.' This is set to change under the Regulation, due to concerns over the emergence of Big Data and the perceived privacy intrusions attached to it.

The Regulation includes various restrictions on profiling, including analysing personal preferences or behaviour, although they have been watered down from the stricter approach seen in early drafts of the Regulation. In practice the data subject's right to object to profiling will be of great importance.

The data subject may object to profiling, at any time, on grounds relating to his or her particular situation, where the basis of such processing is that it is necessary for the purposes of legitimate interests pursued by the data controller. In such cases, the data controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. When the profiling is related to direct marketing, the data subject has an absolute right to object. In this case, the processing must stop and the controller cannot continue under any circumstances.

The data subject will not be able to object to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, if the decision: (i) is based on the data subject's explicit consent, (ii) is expressly authorised by EU or Member State law, or (iii) is necessary for entering into, or performance of a contract between the data subject and a data controller.

Profiling-based decisions must not be based on special categories of personal data (e.g. racial, ethnic, or religious information) unless (i) the data subject has given explicit consent for one or more specified purposes, except where prohibited by European law or member state law; or (ii) processing is necessary for reasons of substantial public interest, on the basis of European or member state law.

It is of paramount importance to inform the data subject who is subject to a decision based solely on automated processing, including profiling, at the first communication of his or her right to object to profiling. It must be explicitly brought to his or her attention and must be presented clearly and separately from any other information. The controller must inform a data subject at the time data is collected not only of the fact that profiling will occur, but also of "the logic involved" and "the envisaged consequences of such processing".

Profiling in practice

In many situations, the only lawful basis for profiling will be the explicit consent of the data subject. As the Regulation requires explicit consent to be a 'freely given, specific and informed indication of his or her wishes by the data subject, either by a statement or by a clear affirmative action', engaging in lawful profiling could become much more cumbersome.

For example, data subjects will need to be informed about the profiling and the consequences of profiling and consent will need to meet very high regulatory expectations. This could mean that Big Data analytics involving personal data may require businesses to obtain explicit consent before the analyses can be conducted, for example in relation to customer tracking, behavioural targeting and advertising.

In summary, businesses that regularly engage in data analytics activities will need to consider how they can implement appropriate transparency and consent mechanisms in order to continue profiling activities under the Regulation.

The impact on the digital economy

The potential consequences of the forthcoming legal regime dealing with profiling should not be underestimated. As the legislative framework is now finalised, it is crucial to understand the practical implications for businesses and the digital economy as a whole. The Regulation regards profiling as a high risk activity and it is subject to strict conditions and rigorous oversight.

Therefore, compliance with this new regime should form part of all businesses' Big Data strategies. In many instances, this will involve setting up data collection processes that trigger an appropriate consent mechanism. This will often be determined by a preliminary assessment of the intended data activities that seeks to identify the impact on people's privacy and the most suitable approach to legitimizing those activities. Given the perceived risks of profiling, this must become a compliance priority.

What to do now

- Conduct an assessment of all data activities that may qualify as 'profiling' and determine the applicable legal basis: (i) consent, (ii) required for the entry into or performance of a contract or (iii) authorisation by law.
- Identify any decision which relates to sensitive data or children, in both case further scrutiny will have to be applied
- To the extent that consent is likely to be required, identify the most appropriate mechanism for obtaining this and how to deploy it in practice

The new accountability regime

Quick read

- The notion of accountability has been the subject of discussions since 1980.
- Accountability is about demonstrating compliance and being transparent about such compliance.
- The Data Protection Directive already includes a number of obligations/ recommendations for data controllers which echo the accountability principle, but new obligations in the Regulation formalise the requirement.
- Accountability may be a way of restoring trust given concerns about big data, evolution of technologies and the increase in cybercrime.
- Compliance with the accountability provisions of the Regulation will entail conducting audits, implementing internal and external policies and processes, privacy impact assessments and security measures and appointing a DPO.

The new accountability regime

Mac Macmillan and Sarah Taieb

Background of the notion of accountability

Accountability has been described by the Article 29 Working Party as a way of "showing how responsibility is exercised and making this verifiable".

Accountability is far from being a new concept. It was introduced back in 1980 in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

In 2010, the Article 29 Working Party issued an Opinion on the principle of accountability where it put forward a concrete proposal for adding a principle of accountability so data controllers *"put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with and to demonstrate so to supervisory authorities upon request"*. According to the Article 29 Working Party, the accountability principle *"should contribute to moving data protection from 'theory to practice' as well as helping data protection authorities in their supervision and enforcement tasks"*.

From a national standpoint, in January 2015, the French DPA, the CNIL, issued an accountability standard. The CNIL's accountability standard is divided into 25 requirements relating to the existence of both an internal privacy policy and an outward-facing privacy policy as well as the appointment of a data protection officer. Companies that demonstrate that they comply with the new standard will be able to obtain an "accountability seal" from the CNIL.

Accountability in the Data Protection Directive

Although the Data Protection Directive does not specifically refer to the term "accountability", a number of its provisions set a basis for accountability:

- Data controllers must ensure compliance with the main principles relating to data quality
- Notification obligations towards the DPAs
- Duty to implement "appropriate technical and organizational measures" to safeguard and protect data.

Need for specific provisions relating to accountability

Specifically referring to accountability in the Regulation will ensure in a more effective manner that data controllers comply with their obligations. As mentioned by the Article 29 Working Party, to ensure the effectiveness of the provisions of Directive 95/46/ EC, it would be necessary to fully integrate the data protection principles in the data controller's "shared values and practice".

In addition, the increased risks presented by big data, increased transfer and centralisation of data, and the rise in cybercrime mean accountability is more important for data controllers to show that they use privacy as a positive safeguard, helping them to regain the trust of their customers.

What does the Regulation require for accountability?

The notion of accountability is introduced by Article 5 as follows: *"the controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability")"*. The Paragraph 1 to which it refers lists six general principles relating to the processing of data, principles which are already familiar from the Data Protection Directive. Accountability, within the meaning of the Regulation, is a situation where a company is able to demonstrate that it acts in compliance with the principles of the Regulation.

Article 24.1 relating to the Responsibility of the controller expands on the concept introduced by Article 5, providing that:

"Taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. These measures shall be reviewed and updated where necessary".

More specific obligations which contribute to accountability are set out in other articles. They include the following elements:

- Implementation of appropriate data protection policies and measures to ensure that an organisation's processing of personal data complies with the Regulation
- Adherence to approved codes of conduct or an approved certification mechanism. These are not mandatory but are suggested as a way that controllers can demonstrate that they are complying with their obligations under the Regulation
- Adoption of measures, such as an internal or external audit process, to demonstrate that an organisation's processing of personal data complies with the Regulation
- Implementation of technical and organizational methods to protect data against unauthorized or unlawful processing
- Keeping records of the processing of personal data which the organization carries out. The level of detail required is not yet settled, but it is likely that it will be similar to that currently required for data protection registrations in many Member States at present, for example, the purposes of processing, the categories of data subjects and data, the recipients or categories of recipients of data and, if possible, the time limits for deletion of the different categories of data
- Carrying out data protection impact assessments for operations which present specific risks to individuals due to the nature or scope of the processing operation
- Appointment of an independent data protection officer (DPO). Appointing a DPO is only mandatory in certain cases, in particular where sensitive data are being processed. The role of the DPO is critical for accountability. The DPO should be selected for his or her expertise, and reports to the highest level of the company's management. The DPO is required to inform the controller of its obligations under the Regulation, and to monitor the implementation and application of the controller's policies in relation to personal data. DPOs must be involved in all issues raised by the protection of personal data within a company, in particular by organizing training and a network of persons aware of the data protection issues within the company. They also act as a point of contact for supervisory authorities and must cooperate with the latter.

How can businesses start to prepare?

It is likely that the DPAs will provide further details of what they expect in this area. Indeed, as mentioned above, the CNIL has already done so. Pending agreement on a common approach what can businesses be doing to prepare now?

The key concept to keep in mind is that this is about embedding privacy in the organization. Many organizations have internal privacy policies which set out the principles to which the organization will adhere, but implementation goes little further than posting the policy on the intranet. As the Article 29 Working Party memorably put it in its 2009 paper on "The Future of Privacy", the principles and obligations "should permeate the cultural fabric of organisations, at all levels, rather than being thought of as a series of legal requirements to be ticked off by the legal department." Companies need to be thinking not only about what compliance requires but how to communicate that throughout the organization.

Steps which you can take at this stage to help plan your approach to accountability include:

- Identify and review all your existing policies to see what your current state is. This may go far wider than privacy policies, to encompass IT and security policies, protection of information assets, use of electronic communications and monitoring
- An effective accountability programme needs support from senior levels of the organization. Start identifying key stakeholders who may be able and willing to provide this
- Appoint a DPO if you are required to have one
- Identify where data is processed within your organization from both a functional and a geographical perspective. Remember to include third party processors
- Do a gap analysis of what processes you have in place for handling new and existing data protection obligations. For example is there a clear process for handling requests for data subjects in relation to their data?
- Identify who the key actors are in relation to data processing so that you can involve them in developing processes
- Consider whether you have existing audit processes within the organization which you can leverage to monitor compliance in this area.

What to do now

- Identify your current state: review all relevant existing policies, and identify where data is processed within your organisation from both a functional and a geographical perspective.
- Do a gap analysis of what processes you have in place for handling new and existing data protection obligations.
- Identify key actors in relation to data processing so that you can involve them in developing new processes.
- Identify key senior stakeholders to support your accountability programme.

Data processors' new obligations

Quick read

- The Regulation will impose a number of compliance obligations and possible sanctions directly on service providers.
- This is a significant change as currently service providers do not have any direct obligations to comply with EU data protection law (their obligations derive from their contracts with controllers).
- Very detailed contractual arrangements will be required between organisations and their service providers.
- New deals being negotiated now should be future proofed.

Data processors' new obligations

Christian Tinnefeld and Katie McMullan

What's the deal?

The Regulation will have a significant impact on service providers/vendors (i.e. data "processors") and organisations that engage them because:

- The Regulation imposes a number of detailed obligations and restrictions directly on processors, unlike the current Directive that only applies to data controllers
- A processor will be fully liable for the actions of any sub-processor that it uses to provide its services and will be required to flow down its obligations under the Regulation to the sub-processor
- There are significant penalties which can be imposed on processors for failure to comply with their increased responsibilities and individuals have enhanced rights to seek compensation directly from service providers
- The new law is much more prescriptive about the contractual arrangements that must be in place between controllers and processors than under the current Directive
- The new rules are considered in further detail below and will be triggered where:
- The processor is established in the EU (even if the actual processing takes place outside the EU)
- Where the processor offers goods or services or monitors the behaviour of EU-based individuals (even if the processor is not established in the EU). In such circumstances the non-EU based processor must designate an EU representative, unless the data processing is occasional, does not involve sensitive data processing or is not high risk to the individual

Likely practical impact for processors

The Regulation goes beyond the position under the current Directive by imposing a number of obligations directly on processors. This means that service providers now run the risk of direct enforcement action by a supervisory authority in the event of non-compliance with their new obligations, which include the following:

- **Stricter requirements for sub-processing.** The Regulation contains a new restriction on processors engaging another processor (i.e. sub-processing) without the consent of the controller. A controller may provide a general consent to sub-processing but if it does, the processor is required to inform the controller of any new or replacement sub-processors and the controller has the right to object. Processors must impose the same data privacy obligations on the sub-processors (see below) and will remain fully liable for the sub-processor's performance.
- **Prescriptive terms for contracts with controllers** (explained in further detail below).
- **Maintain records of processing activities.** Most processors will be required to maintain documentation about its data processing activities (unless it employments fewer than 250 people and is not engaged in high risk or sensitive data processing) such as the name and contact information of each controller/s the processor is acting on behalf of, the categories of processing carried out on behalf of each controller and details of transfers to non-EU countries. The processor may also be required to submit the documentation to a supervisory authority if requested to do so.
- **Implement Security.** Processors will be directly responsible for implementing appropriate security measures. This includes a positive obligation to consider pseudonymisation and encryption, ensure on-going confidentiality, integrity, availability and resilience of systems and services, restore access to data and operate a process to regularly test, assess and evaluate the effectiveness of security measures. The processor must also notify a controller without 'undue delay' after becoming aware of a personal data breach
- **Appoint a data protection officer.** Processors will be required to appoint a data protection officer ('DPO') where their core processing activities involve on a large scale (i) regular and systematic monitoring of individuals or (ii) processing of sensitive or criminal data
- **Comply with the international data transfer requirements.** Processors alongside controllers are responsible for compliance with the data transfer rules. Notably if a processor receives a request from a non-EU court, tribunal or administrative authority to disclosure data held in the EU (and therefore make a data transfer) and it cannot rely on another ground for transfers, this request is only recognised under the Regulation if based on an international agreement (such as a mutual legal assistance treating) in force between the non-EU country and the EU or Member State
- **Co-operate with a supervisory authority if requested to do so.** Processors will therefore need to consider how they will comply with this obligation in a way that does not amount to a breach of contract with a controller.

Likely practical impact for data processing agreements

For businesses that use processors to provide services on their behalf, one of the most significant changes in relation to data processors' new obligations is that the Regulation prescribes the terms that must be contained in a written agreement between the controller and processor. The contract must contain more detail than is required under the Directive about the processing the processor is engaged in and in particular must set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. This is a significant change for some processors, for example cloud service providers, who currently may know nothing about the data they host.

The processor must also:

- Process the personal data only on 'documented instructions' from the controller, including in relation to international data transfers
- Ensure that the processor's staff are committed to confidentiality
- Take all appropriate security measures as required by the Regulation
- Sub-contract only with the prior specific or general written consent of the controller, flow down its obligations and remain liable for the actions of any sub-processors, as noted above (so deals being negotiated currently should ideally be future-proofed by obtaining this consent now)
- Help the controller respond to requests from individuals
- Assist the controller with data security, data breaches, data protection impact assessments and when consulting with the DPA

– Delete or return all data to the controller at the end of the provision of data processing services and delete existing copies unless required to retain them by law

– Make information available to the controller to demonstrate the processor's compliance and allow for and contribute to audits

These changes will likely lead to service providers pushing for detailed allocation of risks in their contractual arrangements.

In addition, the Regulation does not specifically address the position in relation to existing contracts or put in place transitional arrangements which means that many service agreements between controllers and processors may need to be renegotiated.

Sanctions for non-compliance

The Regulation proposes penalties of up to 4% of worldwide turnover or €100 million for the most serious data protection breaches which significantly increases the risk to both controllers and processors of data if they fail to discharge their regulatory obligations. DPAs also have extensive supervisory powers, including powers to obtain access to all the personal data a processor holds, access processor premises, issue warnings, order compliance and ban processing. Another significant change is that individuals will also have the right to seek a judicial remedy and claim compensation directly against a processor for infringing their rights as a result of the processor's non-compliance with the Regulation. Additionally where an individual's rights are violated, the individual may claim in full against the processor, leaving the processor to bring a claim against the controller to recover its share of the liability.

The heightened risks and direct obligations for data processors under the Regulation will therefore very likely impact on negotiations with service providers going forward, particularly in respect of security standards, risk allocation and pricing.

New codes of conduct and certification mechanisms

Controllers are expressly required by the Regulation to appoint only processors that are able to provide sufficient guarantees to the effect that they can provide their services in compliance with requirements of the law and ensure the protection of the rights of individuals. The Regulation also encourages the drawing up of codes of conduct and certification mechanisms by data protection authorities, the European Data Protection Board, the Commission, associations and industry bodies. It is therefore likely that sophisticated processors will seize upon the opportunity to demonstrate sufficient guarantees by adherence to these new codes of conduct and certification mechanisms although adherence to a code or scheme brings with it greater scrutiny, and if there is a failure, the prospect of being publicly suspended or excluded from the code or scheme.

What to do now

– Controllers should identify all current contracts with data processors and their renewal dates, in order to develop a plan for bringing them into compliance with the Regulation.

– Future proof deals being negotiated now. Controllers and processors should carefully document the responsibilities of the parties and specifically take into account the forthcoming changes when deciding on providing consent for sub-processors, pricing, security standards and risk allocation.

– Processors should identify any aspects that have significant impact on their business operations and start preparing for their increased obligations.

– Consider appropriate outreach actions, for example to contribute to new codes of conduct and certification mechanisms in conjunction with relevant industry bodies and associations.

International data transfers 2.0

Quick read

- The existing restrictions affecting international data transfers are set to continue under the Regulation.
- Existing adequacy findings and standard contractual clauses approved by the Commission ("EU Model Clauses") will in principle continue to be valid.
- The Regulation extends the options available to legitimise international transfers (such as standard and "ad hoc" contractual clauses and codes of conduct adopted or authorised by DPAs).
- BCRs are officially recognised and the approval process is set out in the Regulation.

International data transfers 2.0

Martin Pflueger, Rik Zagers and Hannah Jackson

What's the deal?

The Data Protection Directive and the Regulation both impose restrictions on the transfer of personal data by EU based businesses (whether those businesses are data controllers or data processors) to destinations outside the EEA.

Recap on current framework

Transfers of personal data to a third country outside the EEA are allowed under the current Data Protection Directive only if one of the following requirements has been met:

- the Commission has established that the third country ensures an adequate level of data protection by reason of its domestic law or as a result of the international commitments it has entered into. The Commission has so far recognised eleven countries as providing adequate protection
- adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights have been adduced, such as:
  - where the transfer is based on the EU Model Clauses
  - where other transfer mechanisms recognised by European DPAs under the Data Protection Directive (such as Binding Corporate Rules ("BCRs")) are in place
- one of the derogations under the Data Protection Directive applies, such as where the data subject has consented to the transfer.

These restrictions, however, have not been uniformly implemented by EU Member States. In some Member States additional requirements apply, such as prior notification to or approval by the local DPA, particularly where companies wish to rely on EU Model Clauses or BCRs. This approach is essentially set to continue with some variations.

Adequacy

The Regulation allows for the designation not only of third countries but also specific territories, sectors and states within such countries, as well as international organisations, as providing an adequate level of protection for personal data transferred from the EU. In addition, the Regulation sets out in more detail the procedure and criteria for the Commission's adequacy decisions, including a requirement for a decision to be reviewed at least every 4 years and a mechanism under which the Commission can decide that a third country no longer ensures an adequate level of protection.

Although existing adequacy decisions made by the Commission under the Data Protection Directive will continue to remain in force, the Commission will be under an on-going obligation to monitor developments in third countries which could affect the adequacy decisions awarded under the Data Protection Directive.

Appropriate safeguards

The Regulation recognises and preserves the existing transfer mechanisms under the Data Protection Directive for transfers of personal data to third countries which do not provide an adequate level of data protection.

However, while under the current Data Protection Directive, several Member States require that a transfer to third countries outside the EU/EEA must be notified to or authorised by local DPAs, in particular where based on EU Model Clauses or BCRs, the Regulation explicitly provides that this will no longer be the case.

In addition to this improvement, the Regulation further extends the options and procedures available to data controllers (and to data processors) to legitimise international transfers, with the options now including:

- **BCRs:** BCRs (including BCRs for processors) are given specific recognition in the Regulation, which also sets out in detail the content they must include and the procedure under which they will be approved;
- **standard contractual clauses:** adopted by the Commission (including the existing EU Model Clauses, which will remain valid under the Regulation unless they are specifically amended or repealed by the Commission);
- **standard contractual clauses adopted by a DPA and approved by the Commission;**
- **an approved code of conduct:** groups of data controllers represented by an association will be able to prepare codes of conduct which set out how they comply with the Regulation. These codes will be approved by the competent DPA (or the DPA and the European Data Protection Board) and may then be adopted (by way of 'binding enforceable commitments') by entities which are not subject to the Regulation to provide appropriate safeguards for personal data transferred to them;
- **an approved certification mechanism, seal or mark:** the Regulation creates a mechanism under which data protection certifications, seals and marks can be established. Entities which are not subject to the Regulation will be able to obtain these certifications, seals and marks and make 'binding enforceable commitments' to comply with them to demonstrate that they offer appropriate safeguards for personal data transferred; and
- **other contractual clauses authorised by a data protection authority in accordance with the so-called 'consistency mechanism'** (so-called "ad hoc" contractual clauses).

Derogations

The derogations set out in the Data Protection Directive will continue to apply under the Regulation. In addition, the Regulation provides that, where none of the other derogations for a specific situation is applicable, transfers which are not repetitive and involve only a limited number of data subjects could be allowed if the transfer is necessary for the 'compelling' legitimate interests of the data controller. If the data controller wishes to rely on this derogation, it must have assessed all the circumstances surrounding the transfer, and must have adduced appropriate safeguards based on that assessment. In addition, the data controller must:

- inform both the DPA and the data subject of the transfer, and tell the data subject what the 'compelling legitimate interest' on which it is relying is; and
- keep a full record of the transfer, the assessment conducted and the 'appropriate safeguards' implemented.

Transfers required by the law of a non-EU country

As anticipated, the Regulation specifically addresses transfers of personal data required by a non-EU court, tribunal or administrative authority. If a controller or processor receives a request from one of these bodies and it cannot rely on another basis for a transfer to it, the request will only be recognised under the Regulation if it is based on an international agreement (such as an mutual legal assistance treaty) in force between the non-EU country and the European Union or Member State. The UK government has already indicated that it intends to opt out of this provision.

Likely practical impact

Adequacy

Under the Regulation specific territories within a country (e.g. single U.S. States) may qualify as providing for an adequate level of data protection. The Commission may also decide that specific industry sectors or international organisations are adequate in terms of data protection. Initially such standards are likely to be found in sectors in which high privacy standards already exist (e.g. the banking and/or insurance sectors).

Appropriate safeguards

The Regulation prevents local DPAs from requiring any specific authorisation for cross-border transfers outside the EEA if the requirements of the Regulation are otherwise met. For multinational companies relying on EU Model Clauses or BCRs to legitimise their transfers, this will drastically reduce the administrative burden – the days of local administrative differences or further notification or approval requirements will be over.

The Regulation formally recognises BCRs as a valid transfer mechanism and sets out uniform rules for their adoption, further strengthening the role of BCRs as a mechanism to enable cross-border transfers. The likely practical impact is that we will see an increasing number of companies implementing BCRs.

It remains to be seen how the new transfer mechanisms, such as approved codes of conduct or certification mechanisms, will be implemented in practice. However, these mechanisms may be interesting solutions also for controllers and processors not established in the EU in order to provide appropriate safeguards for international data transfers from the EU.

Derogations

Since the Regulation provides that transfers are also allowed on the basis of the compelling legitimate interests of the controller, we may see an increase in data transfers based on this derogation. This will be of interest for companies where transfers only take place occasionally and not on a large scale, and no other derogations are reasonably available.

What to do now

- Identify the key international data flows carried out in the context of an organisation's core operations.
- Assess what mechanisms are currently in place to legitimise international data transfers and assess their validity under the Regulation.
- For intra-group data transfers, consider carrying out a BCR Gap Analysis to determine the practical viability of BCR.
- For transfers of data to third party suppliers (e.g. cloud service providers), deploy a flexible contractual mechanism that also covers sub-contracting.

Enforcement and the risk of non-compliance

Quick read

- Independent and better equipped DPAs.
- Broad range of investigative and corrective powers.
- “One Stop Shop” to ensure a comprehensive enforcement of data protection law.
- Stronger judicial remedies at the individuals’ disposal including a right to compensation where damage is suffered.
- Heavy fines against data controllers and data processors of up to €20 million or 4% of annual worldwide turnover whichever is higher.

Enforcement and the risk of non-compliance

Marcus Schreibauer and Lilly Taranto

One of the major purposes of the Regulation is to ensure a consistent application of data protection law throughout the EU, not only to provide a high level of data protection but also to guarantee legal certainty for businesses when handling personal data. This has presented legislators with one of their biggest challenges: how to maintain the existing network of independent national DPAs, whilst ensuring that they promote a consistent interpretation of the Regulation and minimising the number of different DPAs which a controller has to deal with. It remains to be seen whether they have devised a workable solution.

Status and powers of the DPAs

Under the Regulation, each Member State is required to establish one or more independent DPAs responsible for monitoring compliance, and to ensure they are adequately resourced. If a Member State establishes more than one DPA, it must designate one DPA to represent the other DPAs in the European Data Protection Board and has to implement proceedings to ensure that all DPAs comply with the cooperation and consistency mechanism created by the Regulation.

DPAs are provided with a broad range of enforcement powers, including:

- to notify data controllers or data processors of an alleged breach of data protection law
- to order data controllers and data processors to provide or to allow access to any information relevant for the performance of its duties
- to carry out investigations in the form of on-site audits
- to order controllers or processors to bring processing operations into compliance with the Regulation
- to order the rectification, erasure or destruction of personal data
- to impose a temporary or definitive ban on processing
- to impose administrative fines.

The cooperation and consistency mechanism and One Stop Shop

A key innovation of the Regulation is that where a controller is established in more than one Member State, the DPA of the country of the main establishment of the controller will be competent to regulate all its data processing activities throughout the EU. This provides an attractive solution for businesses, but could potentially make it difficult for individuals to pursue complaints. However the final draft of the Regulation makes clear that individuals are entitled to lodge complaints with the DPA of their home Member State, even if this is not the data controller's lead authority.

The One Stop Shop applies:

- to data controllers or data processors with establishments in several Member States or
- where the processing of personal data takes place in the context of the activities of a single establishment and is likely to substantially affect data subjects in more than one Member State.

In these cases, generally only one lead DPA can bring enforcement actions against the data controller, namely the DPA in the country of the main establishment of the controller. The lead DPA co-ordinates input from the DPAs of the other affected Member States in order to reach a consensus regarding the enforcement measures. Any local DPA which has informed the lead DPA about an infringement is competent to provide a draft suggestion for enforcement actions to the lead DPA. If the involved DPAs are not able to reach a consensus, a new body, the European Data Protection Board, will decide by simple majority.

This new body will have responsibility for approving measures by DPAs which are intended to have legal effects, such as adopting a code of conduct, authorizing contractual clauses for data transfers abroad or approving BCRs. This is intended to promote a consistent approach to enforcement by the different DPAs.

However, there are exceptions to the One Stop Shop and the consistency mechanism.

Each local DPA is still competent to deal with complaints or possible infringements of the Regulation, if the issue relates only to an establishment in its Member State or substantially affects data subjects only in its Member State. In these cases, the local DPA has to notify the lead DPA which then has three weeks to decide whether or not to deal with the infringement. If the lead DPA decides not to handle the case, the local DPA becomes competent for enforcement actions, but has to observe the rules regarding mutual assistance and joint operations of the DPAs.

There is another exception to the consistency mechanism by way of an urgency procedure where the competent DPA considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects. In such cases the competent DPA may adopt provisional measures with a specified period of validity. DPAs may also conduct joint operations, including joint investigations and joint enforcement actions.

Stronger judicial remedies and heavier sanctions

The Regulation provides individuals with judicial remedies against:

- Decisions of a DPA which concern them
- A DPA, obliging it to act on a complaint
- Data controllers and data processors who breach their rights by failing to comply with the Regulation.

These rights can be exercised by consumer bodies on behalf of data subjects. It will be interesting to see to what extent such organisations bring a different focus to enforcement of rights.

Individuals will also have a right to compensation from both data controllers and data processors for material and immaterial damage suffered as a result of processing carried out in breach of the Regulation. Where more than one data controller and data processor are involved in the processing the Regulation provides that they will be jointly and severally liable unless they can prove that they were not responsible for the event that caused the damage.

A significant change is that sanctions will now apply not only to data controllers, but also to data processors that have breached their data protection obligations. There is also a significant increase in the potential severity of sanctions, acknowledging the fact that current fines are insignificant for certain organisations. Sanctions include:

- Fines of up to €10 million, or in case of an undertaking, up to 2% of annual worldwide turnover for non-compliance with obligations of data controllers and data processors under the Regulation, e.g. such as the obligations to enter into a written data processing agreement, implement sufficient IT security measures or provid a comprehensive and transparent privacy policy.
- Fines up to €20million, or in case of an undertaking, up to 4% of annual worldwide turnover for other compliance failures with respect to infringements of the rights of the data subjects and the general principles for data processing, e.g. failure to respond to data subject access requests in line with the Regulation or any inadmissible data processing.
- Fines up to €20 million, or in case of an undertaking, up to 4% of annual worldwide turnover for failures to comply with orders of the competent DPA.

The level of sanctions will be fixed having regard to factors such as the nature, gravity and duration of the breach and whether this was intentional or negligent, history of previous breaches, the data protection compliance structure that was in place and the level of co-operation with the DPAs to try and remedy the breach.

Likely practical impact

The One Stop Shop mechanism has the potential to be a substantial improvement on the fragmented regulatory activities under the Data Protection Directive, as it may enable businesses which operate across the EU to deal with only one DPA. However, it remains to be seen how this will work in practice. Due to the various exceptions, data controllers and data processors may still have to deal with several local DPAs which may interpret the Regulations in different ways.

What to do

- Organisations operating in a number of Member States will benefit from a strategic analysis of the distribution of their data processing activities to assess whether there is a clear country of main establishment, and if not whether it would be beneficial to have one.
- Develop a workable DPA cooperation strategy and procedure.
- Organisations which traditionally act as data processors should conduct a risk assessment of their operations which takes into account the changes in liability.
- Develop guidelines for information requests and inspections by a DPA and train your staff on what to do during an inspection.
- Implement a data protection specific compliance management system to avoid violations of the Regulation which may result in fines of millions of Euros.
- Closely monitor the enforcement actions and announcements of the competent DPA.

Data protection in the workplace

Quick read

- The general principles of the Regulation also apply to employers processing employees' personal data.
- Member States may provide for more specific rules regarding employee data protection so this area of data privacy is expected to remain less harmonised than others.
- The conditions under which personal data in an employment context may be processed on the basis of employees' consent may be determined by Member States.
- Collective agreements may govern the processing of employees' personal data in an employment context.

Data protection in the workplace

Tim Wybitul

Relevance of employee data protection for enterprises

Data privacy in an employment context remains a challenge for companies. On the one hand, employers have a strong interest in monitoring personnel conduct or performance. Few controllers are likely to have collected more personal data about an individual than their employer. On the other hand, employees have a reasonable expectation of privacy – including in their workplace. This inherent conflict of interests has created a considerable volume of case law regarding employee monitoring in several Member States, e. g. relating to the permissibility of monitoring internal investigations and compliance controls.

Modern technology offers advanced technical options to monitor employee performance and conduct. Even standard IT applications may be used to control or record personnel behaviour in the workplace. Where previously the degree of employee supervision was limited by what the technology could do, rapid technological advancements mean that data protection laws are now the principal limitation in the EU. The Regulation is due to play a major role in this respect. As a consequence, employee data privacy has been one of the most hotly debated aspects of the Regulation. This area of data privacy will remain less harmonised than other fields of data protection.

Likely practical impact of the Regulation on employee data protection

For most Member States, the Regulation considerably changes the landscape. Even for employers in Member States with relatively strict employee data protection requirements, the upcoming data protection regime will create additional challenges.

As a general rule, all of the principles and restrictions of the Regulation also apply in the workplace. For instance, monitoring employee performance or conduct may call for prior data protection impact assessments. The new right of data portability means companies could be required to transfer employee data of a leaving employee to a new employer. Moreover, the severe maximum penalties which can be imposed under the new data protection framework are a strong encouragement for employers to ensure effective data protection for their employees.

Quite a number of provisions in the Regulation were obviously drafted in the light of internet commerce, social media or other contemporary forms of business or communication. Some of these mechanisms simply do not match well with an employment context, e.g. data portability. Employers should closely analyse where the Regulation necessitates changes to current employee data being processed.

Few controllers are likely to have collected more personal data about an individual than their employer.

Processing employees' personal data for the performance of the employment contract

Personal data must be processed in a manner which is adequate, relevant and not excessive in relation to the purposes of the employment relationship for which they are processed. Current Article 6 (1)(b) of the Regulation will be particularly relevant in an employment context. It permits the use of personal data to the extent that processing is necessary for the performance of the employment contract between data subject and controller. Employers are well-advised to take particular care to comply with the strict requirements regarding transparency and documentation in order to avoid fines, employee damage claims and possibly exclusion of evidence presented to labor courts, e.g. in dismissal lawsuits.

Article 82 of the Regulation also contains additional provisions aimed at protecting the rights and freedom of employees. Member States may adopt specific rules regulating the processing of personal data in an employment context.

It is likely that Member States that traditionally have a high degree of employee data privacy will adopt employee-specific data protection rules. As a consequence, there may be considerable variations in employee data protection and, consequently, a lesser degree of harmonisation between the individual Member States.

Processing employees' personal data for other legitimate purposes

The processing of employee data may be legitimised by the general provisions of the Regulation. For example, Article 6 (1)(b) permits processing where this is necessary for the purposes of legitimate interests pursued by the employer or by a third party. However, this must be balanced against the interests or fundamental rights and freedoms of the data subject, i.e. the employee. Outside an employment context, this provision may permit the collection and other processing of employee data.

Processing employees' personal data on the basis of collective agreements

Under Article 82 of the Regulation, the processing of personal data may be governed by collective agreements, for example by collective bargaining agreements or works council agreements, which may be entered into between employers and employees' representatives.

In some countries with strong employee representative rights, like for instance Germany, works council agreements are already a reliable and safe way to govern the use of data in the work place. In Member States permitting the use of employee data on the basis of collective agreements, it can be expected that domestic courts will quickly establish rules and standards for permissible collective provisions. However, this would then result in even less EU-wide harmonisation regarding data protection in the work place.

Processing personal data on the basis of employee consent

Article 6 (1)(a) of the Regulation provides that processing of personal data for one or more specific purposes may be lawful if the data subject has given unambiguous consent to it. Not surprisingly, such consent must be freely given. In some Member States, the question whether and under what circumstances employees can consent to the processing of their personal data has been an ongoing debate for years. The Regulation does not resolve this issue. Rather, Recital 34 states that consent should not provide a valid legal ground for the processing of personal data in a specific case, where there is a clear imbalance between the data subject and the controller, Therefore, it is unlikely that employee consent will ever be a robust basis for the use of that data, and this needs to be factored in when justifying such uses.

Rather, employers should establish a high degree of transparency regarding data protection at the workplace as well as a robust and effective data protection management system

What to do

- Employers should closely analyse where the Regulation necessitates changes to current employee data being processed.
- Analyse whether your business' personnel and data protection structures provide the level of transparency and documentation required by the new data protection rules.
- Align HR and data protection functions in order to ensure compliance with the new requirements.
- Keep in mind that specific employee data protection rules may be passed by individual Member States, which would prevent a high degree of harmonisation in this area. Closely monitor whether Member States relevant to your business/ workforce implement specific employee data rules.
- If collective agreements (including works council agreements or collective bargaining agreements) apply to your business: closely analyse any existing agreements and negotiate necessary changes in a timely manner.

Security is a critical piece of the data protection jigsaw

Quick read

- All businesses processing personal data, both controllers and processors, will be subject to the obligation to have appropriate security in place.
- Adherence to officially approved Codes of Conduct may help companies demonstrate they have met the required standard.
- The Regulation will make notification of personal data breaches to data protection authorities mandatory for all businesses for the first time.
- Businesses will also have to notify data subjects of data breaches, unless they can demonstrate that data was rendered unintelligible by technological protections such as encryption.

Security is a critical piece of the data protection jigsaw

Mac Macmillan

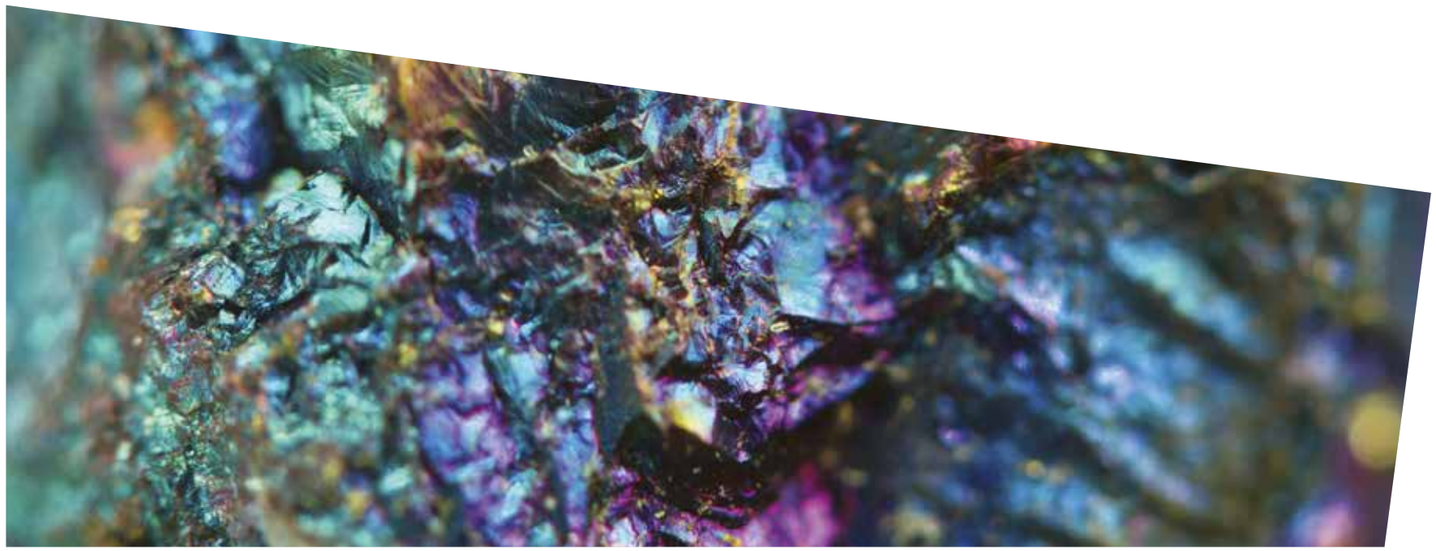
What's the deal?

Security is a critical piece of the data protection jigsaw. Clear comprehensive privacy notices, rights to access and port data, and the protections offered by the principle of purpose limitation and restrictions on data transfers have little value to consumers if their data is not secure. Lack of consumer confidence has been identified as a key risk for the development of the digital single market, and a series of high profile breaches has exacerbated the situation. So it was inevitable that data protection reform would need to demonstrate that regulators were serious about data security and the Regulation does this by introducing three critical changes:

- Obligations to have appropriate security in place will apply directly to data processors for the first time.
- There will be mandatory reporting of data breaches to data protection authorities.
- There will also be mandatory reporting of data breaches to data subjects in certain situations.

The obligation to have appropriate security

At the moment data controllers are under an obligation to have in place appropriate technical and organisational measures to protect the personal data which they process, and to impose the same obligation in their contracts with service providers. Under the Regulation this obligation is extended to processors. This is sensible in a world where service providers may have complex sub-contracting arrangements in place already, particularly in the cloud services environment, and tell customers that it is not practical for them to seek to amend contracts relating to long-standing arrangements. Under the Regulation any service provider wanting to do business with European customers is going to have to ensure that all its arrangements meet European standards because it will be legally obliged to do so. However this may be challenging. The security measures must take into account the nature of the personal data to be protected, the state of the art and the costs of their implementation. Many hosting providers have no visibility of the data which they host so they will be unable to assess the nature of the risk. This means they may have to place obligations on their customers to assess, at a minimum, the level of security which they require.



Another change the Regulation makes is that it is more prescriptive about what areas security measures should cover, saying that where appropriate they should include:

- Pseudonymisation and encryption of personal data
- The ability to ensure on-going confidentiality, integrity, availability and resilience of systems and services processing personal data
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Companies should note the second and third bullet points - they mean that "security" as it is understood by the Regulation is not just about external threats, but also encompasses business continuity issues.

Notification of breaches to DPAs

As was widely expected, the Regulation introduces mandatory reporting of data breaches to the relevant DPA, but fortunately not within the 24 hour time period originally proposed by the Commission. Instead controllers must report breaches without undue delay and where feasible within 72 hours of having become aware of it. If the notification is not made within 72 hours, the notification must be accompanied by a reasoned justification. Processors are required to notify the data controller of breaches.

Another aspect of the original notification proposal which caused significant concern was that there was no materiality threshold, meaning that DPAs were likely to be overwhelmed with fairly insignificant reports. The final version says that it is not necessary to report a breach if it is "unlikely to result in a risk for the rights and freedoms of individuals". This is an improvement, but very few breaches will represent no risk at all to individuals, so we will need to wait for guidance on how DPAs intend to interpret this threshold.

Where a notification is required, it should include:

a) A description of the nature of the breach, including the categories and number of data subjects concerned and the categories and number of data records concerned

b) The identity of the data protection officer or other contact for more information

c) A description of the likely consequences of the breach

d) A description of the measures taken or proposed to be taken by the controller to address the breach including, where appropriate to mitigate its possible adverse effects.

All personal data breaches must be documented by data controllers to enable DPAs to verify compliance. The documentation should include the facts surrounding the breach, its effect, and the remedial action taken.

Many organisations already have data breach handling processes in place, but it is likely that these will need review to ensure they meet the new requirements of the Regulation. Where companies are already considering how to manage their cybersecurity risk more generally, it may be advisable to combine the two workstreams to avoid confusing overlapping of processes.

Notification of breaches to data subjects

After notifying the DPA, the controller is also required to notify the data subject, where the breach is likely to "result in a high risk to the rights and freedoms of individuals". The notice must be in clear and plain language. It should describe the nature of the breach, its likely consequences and what the controller is doing to address the breach and mitigate its adverse effects. It should also include contact details of the data protection officer or other contact point where more information can be obtained.

Data subject notification will not be necessary if the controller has applied appropriate protection measures to the affected data, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption, or if it has subsequently taken measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise. If individual notifications would be a disproportionate effort, the controller can use some form of public communication instead provided that this will be equally effective in informing individuals. Importantly, DPAs have the power to overrule controllers and order them to issue a notice to data subjects if they disagree with a controller's assessment of the risk.

What to do now

- Consider whether you as an organisation understand the relative sensitivity of the different data sets which you process
- Develop a plan for reviewing your security measures for appropriateness
- Review contracts with service providers to ensure they contain appropriate provisions.
- If you are a processor, consider whether you have visibility of the sensitivity of the data which you process or whether you need to amend customer contracts to address this.
- Review training provided to employees on data security.
- Develop a breach management procedure which includes clear reporting lines within the organisation to ensure there are no reporting delays

Our global Privacy and Cybersecurity practice

Our global Privacy and Cybersecurity practice

Realizing the true value of data

Finding the right balance between the most fruitful use of data and the protection of privacy is one of the greatest challenges of our time. Personal information is an extremely valuable asset and its responsible exploitation is crucial for the world's prosperity. For that reason, our approach is to look at privacy compliance and information governance as part of our clients' strategic vision for success.

Embracing privacy, data protection, and cybersecurity can be crucial in order to gain competitive advantage, because it will promote employee and customer loyalty, encourage consistency and efficiency, and facilitate international expansion. In addition, we believe that privacy is not only compatible with innovation, but can make a valuable contribution to it.

With its depth of knowledge and global presence, Hogan Lovells' Privacy and Cybersecurity team is uniquely placed to help clients realize this potential. We have extensive experience of assisting clients with multi-jurisdictional projects and understand the complexities involved in dealing with laws
and regulators across the world. We offer:

- A true specialist practice focused on privacy, cybersecurity, data protection, and information management
- Thought leadership and close involvement in the development and interpretation of the law
- Seamless global coverage through our well established and continuously developing team
- Advice which goes beyond achieving compliance and adds value to the information held by organizations
- A one stop shop for all of your data privacy needs around the globe.

Our focus and experience

The Hogan Lovells Privacy and Cybersecurity practice spans the globe and all aspects of privacy, data protection, cybersecurity, and information management.

- No other team in the world has our track record of BCR approvals. We have advised on and successfully secured approvals of BCRs for nine applicant companies and are currently working on several BCR projects.
- We have worked with numerous multi-nationals on other data transfer solutions, including adoption of model clauses, intra-group agreements and Safe Harbor.
- We have advised numerous global companies with respect to complying with their notification obligations across the EU.
- We have drafted and advised on many global data processing contractual arrangements to ensure practical and effective compliance with security-related obligations.
- We have liaised with policy makers throughout the world and contributed to the legislative process in the EU and other jurisdictions.
- We have assisted clients in devising and implementing regulator cooperation strategies, including liaising closely with EU data protection authorities.
- We have surveyed in detail the laws and regulations impacting employee monitoring practices in over 60 countries, including important markets in Europe, the Americas, Asia, the Middle East and Africa.
- We advised a number of global companies on data privacy questions arising from their migration of HR and customer data of their European subsidiaries to cloud service providers.
- We have advised many multi-nationals on localising website privacy policies.
- We have assisted leading global companies to adopt and implement a pan-European strategy in respect of the EU cookie consent requirements for their website and mobile application offerings.
- We provided strategic advice to a number of clients on data breach notification requirements throughout the world.
- We have advised on complex matters ranging from the use of biometrics to the collection of mobile device data, including making submissions to multiple data protection authorities to facilitate the deployment of new data-driven technologies.

How we can help

We have had a team specializing in Privacy and Cybersecurity for over 25 years. Today Hogan Lovells has one of the largest and most experienced Privacy and Cybersecurity practices in the world, spanning the United States, Europe, and Asia. We assist clients with all of their compliance and risk management challenges, drafting policies and providing advice on legal issues, risk management strategies, and strategic governance. With our global reach, we are able to provide a 24-hour global privacy hotline to respond to data emergencies. We play an important role in the development of public policy regarding the future regulation of privacy. Additionally, we provide the latest privacy and data protection legal developments and trends to our clients via our blog, *Chronicle of Data Protection* (http://www.hldataprotection.com).

"The firm has a first-class collection of people when it comes to new technologies. They have been sage on these issues and have helped us to shape emerging areas of law."

Chambers Europe, 2015

"A premier data protection practice – they provide global perspectives and a practical approach, and have a real breadth of experience."

Chambers Global, 2015

Rankings and Awards

2016

Band 1 for UK-wide Data Protection and Information Law *(Chambers UK)*

Band 1 for Europe-wide Data Protection *(Chambers Europe)*

Maintained out top ranked positions in *Chambers Global* and *Chambers USA*

2015

Our global Privacy and Cybersecurity practice has once again been ranked BAND 1 for Privacy and Data Protection by *Chambers Global* for 2015.

2014

Band 1 for Global Privacy and Data Protection practice *(Chambers Global)*

Band 1 for Nationwide Privacy and Data Security *(Chambers USA)*

BAND 1 for Nationwide Healthcare Privacy and Data Security *(Chambers USA)*

TIER 1 for Technology: Data Protection and Privacy *(Legal 500 US)*

Our Privacy and Cybersecurity lawyers are also recognized by leading industry publications:

Star Individual Eduardo Ustaran by *Chambers UK*

Star individual Christopher Wolf by *Chambers USA*

BAND 1 Marcy Wilder by *Chambers USA*

BAND 2 Quentin Archer by *Chambers UK*

LEADING LAWYERS Marcy Wilder and Christopher Wolf by *Legal 500* US

SUPER LAWYERS Eduardo Ustaran, Marcy Wilder, and Christopher Wolf

WHO'S WHO LEGAL Quentin Archer, Marco Berliri, Winston Maxwell, Stefan Schuppert, Eduardo Ustaran, Conor Ward, and Christopher Wolf

About Hogan Lovells

Hogan Lovells is a global law firm that helps corporations, financial institutions, and governmental entities across the spectrum of their critical business and legal issues globally and locally. We have over 2,500 lawyers across more than 45 offices in Africa, Asia, Australia, Europe, Latin America, the Middle East, and North America.

Hogan Lovells offers:

- a unique, high quality transatlantic capability, with extensive reach into the world's commercial and financial centers;
- particular and distinctive strengths in the areas of government regulatory, litigation and arbitration, corporate, finance, and intellectual property; and
- access to a significant depth of knowledge and resource in many major industry sectors including consumer, insurance, hotels and leisure, telecommunications, media and technology, energy and natural resources, infrastructure, financial services, life sciences and healthcare, and real estate.

Our practice breadth, geographical reach, and industry knowledge provide us with insights into the issues that affect our clients most deeply and enable us to provide high quality business-oriented legal advice to assist them in achieving their commercial goals.

A distinctive culture

Hogan Lovells is distinguished by a highly collaborative culture which values the contribution of our diverse team both within the firm and in the wider community. Our style is open, service focused, and friendly. We believe that our commitment to client service, commerciality, and teamwork provides benefits to our clients and enhances effective business relationships.

Our Global Privacy and Cybersecurity Team

North America

R. Cashdan Los Angeles
D. Hansell Los Angeles
M. Maddigan Los Angeles
R. Samuel Los Angeles
S. Yonekura Los Angeles
V. Brennan Northern Virginia
M. Larner Northern Virginia

J.Talotta Northern Virginia
C. James Denver
A. Bender Washington, D.C.
B. Bennett Washington, D.C.
M. Bianchi Washington, D.C.
J. Bomberg Washington, D.C.
M. Brennan Washington, D.C.

J. Brill Washington, D.C.
B. Cohen Washington, D.C.
A. Cooke Washington, D.C.
J. Denvil Washington, D.C.
K. Gasztonyi Washington, D.C.
M. Gitomer Washington, D.C.
S. Gold Washington, D.C.

L. Hardy Washington, D.C.
D. Kaplan Washington, D.C.
M. Kisloff Washington, D.C.
M. Levine Washington, D.C.
J. Lolley Washington, D.C.
S. Loughlin Washington, D.C.
M. Mason Washington, D.C.

P. Otto Washington, D.C.
H. Pearson Washington, D.C.
M. Sneed Washington, D.C.
S. Spagnolo Washington, D.C.
T. Tobin Washington, D.C.
M. Wilder Washington, D.C.
C. Wolf Washington, D.C.

S. Gosnell Handler New York
D. Hanswirth New York
T. House New York

F. de Noriega Olea Mexico City
M. Yanez V. Monterrey

South America

R. Loureiro Brazil
G. Rodriguez Caracas
J. Pondal Caracas

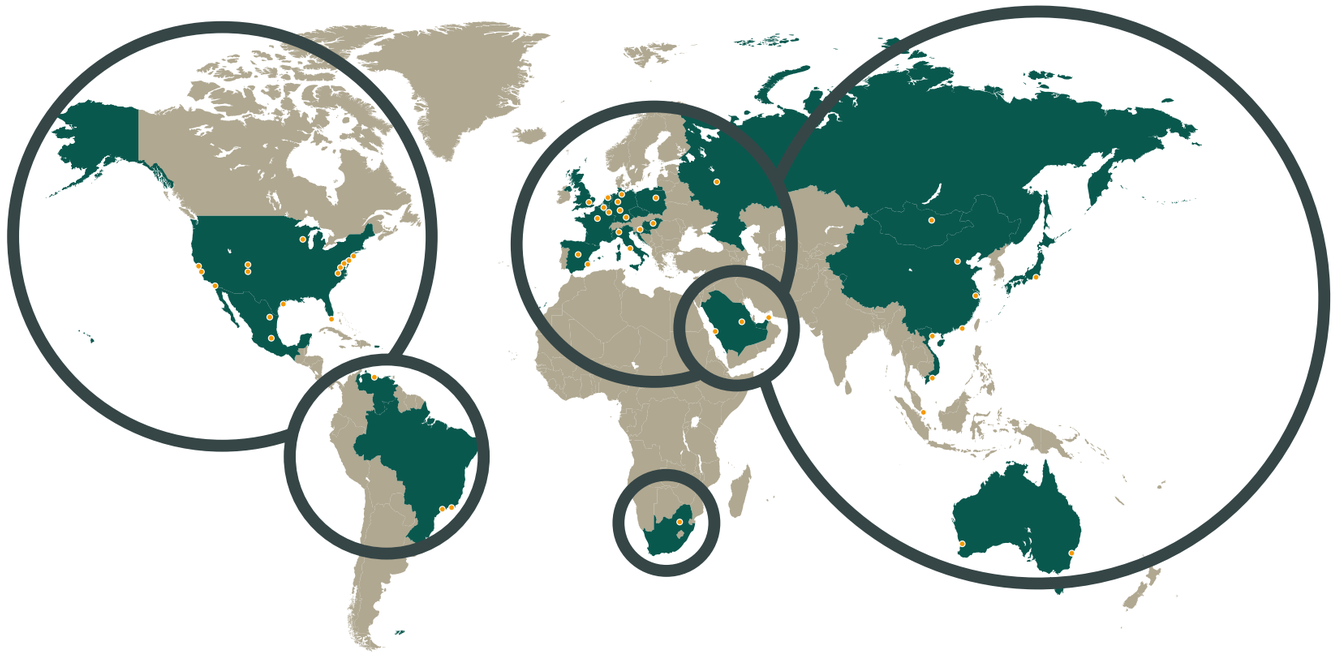
Europe

Q. Archer London
V. Hordern London
H. Jackson London
L. Kammourieh London

M. Macmillan London
K. McMullan London
S. Rudgard London
L. Taranto London

E. Ustaran London
N. Westbrook London

G. Gallego Madrid
L. Badin Madrid
M. Schreibauer Düsseldorf



V. Denoyelle Paris
M. Gérot Paris
W. Maxwell Paris

P. Navarro Paris
D. Taylor Paris
S. Taieb Paris

M. Berliri Rome
M. Colonna Rome
M. Masnada Rome

E. Wright Brussels
N. Pourbaix Brussels

F. Roy Brussels
M. Miglietti Brussels

N. Gulyaeva Moscow
M. Sedykh Moscow

C. Tinnefeld Hamburg
H. Hanssen Hamburg

B. Balas-Noszczyk Warsaw
J. Baczuk Warsaw
E. Kacperek Warsaw
W. Wołosiuk Warsaw

W. Böhm Frankfurt
D. Ettig Frankfurt
S. Gäbeler Frankfurt

N. Rauer Frankfurt
M. Telöken Frankfurt
T. Wybitul Frankfurt

S. Schuppert Munich
M. Pflueger Munich
M. Fischer Munich

J. Bodewits Amsterdam
C. van Dam Amsterdam
R. Zagers Amsterdam

Asia

S. Gong Beijing
J. Wei Beijing
R. Zou Beijing

M. Parsons Hong Kong
P. Colegate Hong Kong
H. Leung Hong Kong
B. Lui Hong Kong

H. Imai Tokyo
S. Keen Singapore
J. Olson Ho Chi Minh City

South Africa

L. Pillay Johannesburg

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Jeddah
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices