Hogan Lovells

Future-proofing privacy

A guide to preparing for the EU Data Protection Regulation

Topics

The time has come

Eduardo Ustaran

It's been a long way and the task is not over yet. However, there is light at the end of the EU data protection reform tunnel. The modernisation of European privacy laws has reached a critical milestone and we can now safely assume that this process will culminate in a radical new framework in a matter of months.

Influenced by overwhelming technological advances and the Snowden revelations, the resulting EU Data Protection Regulation is set to introduce new accountability obligations, stronger rights and ongoing restrictions on international data flows. Overall, the new framework will be 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 forthcoming 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 Information Management 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.

Eduardo Ustaran
Partner, London
T +44 20 7296 5249
eduardo.ustaran@hoganlovells.com

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.

We are now at the stage where three parties need to reach agreement on the draft Regulation before it can become law: the Commission, the Parliament, and the Council. This is done through a negotiation process known as the trialogue. During the trialogue the draft of the Regulation approved by the Parliament (the "**Parliament draft**") and the one agreed within the Council (the "**Council draft**") will be thoroughly debated and following a degree of compromise by all involved, a final version of the Regulation will eventually emerge.

Once the Regulation is formally adopted by the Parliament and the Council, there will be a two year transition period before it becomes enforceable by data protection authorities ("**DPAs**"), but given the number of potential stakeholders in large organisations, and the lead times on IT projects, this may come to seem like not long at all. One thing is certain: all parties involved are committed to creating a robust framework that 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

Nils Rauer and Victoria Hordern

Quick read

- If an organisation is established in the EU, whether as a controller or processor, the Regulation will definitely apply.
- Non-EU controllers that offer goods or services to EU residents or monitor the behaviour of EU residents 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 EU residents.

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) Residence of the individuals

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 residing in the EU. If a non-EU organisation is processing the personal data of individuals residing in the EU for activities relating to:

- Offering goods or services to such individuals
- 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.
This new rule is not without its complexities. For instance, it is not immediately clear how to determine whether someone is a resident of the EU or not. Does an individual need to possess residency status as awarded under the local law of the Member State? Likewise, there are online offerings of goods and services or monitoring activities that are not obviously directed at EU residents. What factors will the EU regulators use to determine whether the processing activities of a non-EU organisation are related to offering goods or services to EU residents? Will the language of the website be determinative as indicating that particular individuals are being targeted? Given that the English language is the prevailing language on the Internet, will all those English language websites be considered to be offering goods or services to UK and Irish residents? There is an indication that it will come down to whether

it is apparent that the controller is envisaging doing business with individuals residing in a Member State but this will need to be assessed in a consistent manner.

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 with 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 EU residents.

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 application of the law rule 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.

Following the CJEU's Google Spain decision in May 2014 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 assess whether their online presence will fall within the rules of offering goods or services to EU residents or monitoring EU residents. Where this is the case, they should assume that the Regulation will apply.
- Global businesses without a clearly identified EU-based controller should position an entity in one EU Member State as the entity through which they conduct all data processing subject to EU rules. 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

Marco Berliri, Massimiliano Masnada, César Ortiz-Úrculo and Giulia Mariuz

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 is likely to give greater flexibility to organisations involved in the processing of personal data for scientific research and public health purposes.
- Genetic data is classified as data concerning health, and included among the special categories of data.
- Biometric data is also defined but is not considered to be sensitive data. Its processing may require a data protection impact assessment in certain scenarios.

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. In exchange for the lower level of privacy intrusion, the applicable 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.
- **Anonymous 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**. Such a definition did not appear in the Commission draft, but is included in the Parliament draft and the Council draft. 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 regime affecting pseudonymous data is less stringent. For example, profiling based exclusively on the processing of pseudonymous data is presumed not to significantly affect individuals. In addition, Member States are likely to be given the option to specify exceptions to the consent requirement with respect to the processing of health data, provided that such data is anonymous or, if anonymisation is not possible, pseudonymous in accordance with the most advanced technical standards.

New types of regulated data

Whilst the definition of data concerning health is not likely to differ greatly from how it is currently interpreted under the Data Protection Directive, there are provisions in both the Parliament's and Council's drafts that facilitate the processing of health data for scientific (i.e. research) purposes. Indeed, examining registries to obtain new knowledge is acknowledged to be beneficial for medical research, carrying out further processing for scientific purposes is not considered incompatible with the initial purpose, and health data may be stored beyond the normal retention period when being used for these purposes. Health data may also be processed for public interest reasons in the area of public health without consent, especially when linked to a quality or cost-effectiveness benefit, provided that it does not end up in the hands of third parties, such as employers, banks or insurance companies.

Although a data protection impact assessment must be carried out in most profiling instances, such impact assessment is not required if the processing is protected by professional secrecy, and managed, for example, by a healthcare professional. Following a similar rationale, health data processed for healthcare purposes (e.g. preventive or occupational medicine, medical diagnosis, employer assessments of the working capacity of employees, provision of health or social care or treatment or management of health or social care, or under a contract with a health professional) should be processed by or under the responsibility of a healthcare professional (or other person subject to an obligation of secrecy).

Genetic data is defined as personal data relating to the genetic characteristics of an individual that have been inherited or acquired resulting in particular from an analysis of a biological sample from the individual in question. Genetic data is regarded as personal data concerning health, and is included among the special categories of data. It will be left to Member States to allow this to be processed without consent for healthcare and medical purposes when carried out by or under the responsibility of a healthcare professional (or other person subject to an obligation of secrecy).

Biometric data, which is 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, is not included among the special categories of data, but when processed for taking decisions regarding specific individuals on a large scale, a data protection impact assessment will be required.

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?

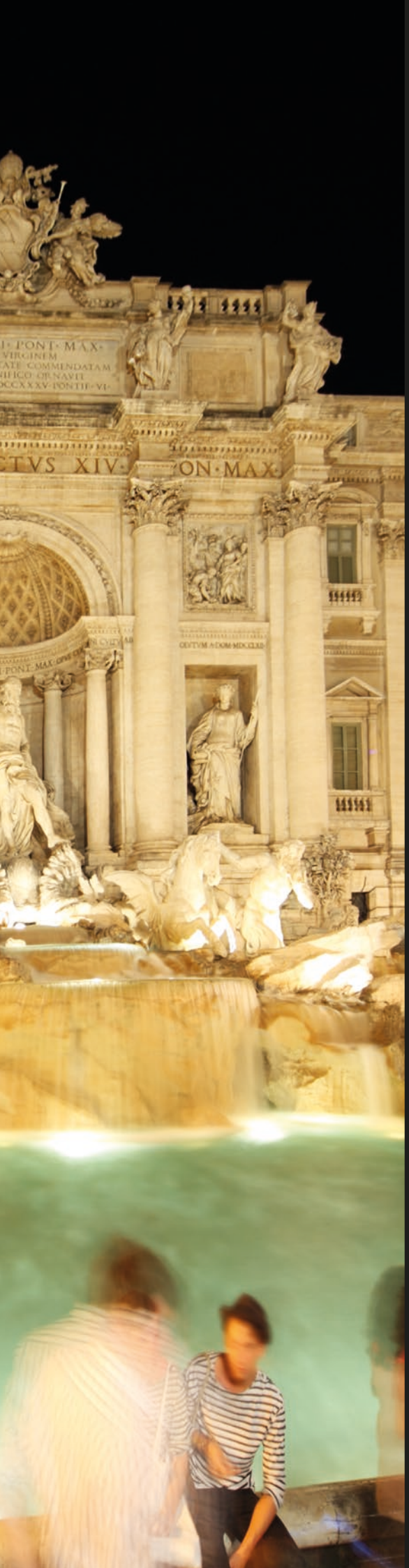
At the moment the standards according to which data is considered as anonymous or pseudonymous are established by the DPAs at a national level. Once the Regulation comes into force, the requirements and the applicable regime will become more uniform and this will provide greater legal certainty.

The latest proposals on processing of data for scientific research and public health are reassuring, but the degree to which the companies involved in those fields will face greater flexibility is still uncertain.

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).


PERFECIT
BENEDIC



Justifying data uses – from consent to legitimate interests

Gonzalo Gallego and Ewa Kacperek

Quick read

- Each instance of personal data processing requires a valid ground for processing.
- The main grounds for processing include consent, performance of a contract, fulfilment of a legal requirement and the legitimate interests of the controller.
- The bar for showing the existence of certain grounds for processing will be set higher, particularly in relation to consent.
- The processing of sensitive personal data is subject to a special, even more stringent regime.

Grounds for processing

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 remains unchanged under the draft Regulation. However, the bar for showing the existence of certain grounds for processing will be set higher, particularly in relation to consent.

Stringent and uncertain consent rules

For starters, under the draft Regulation, if the data subject's consent is given in a written document, and that document also concerns other matters (e.g. terms of service), the consent must be presented in a form that is distinguishable from the remaining contents of that document. This will result in the need to review existing contracts, general terms and conditions and other existing documents, in order to differentiate the consent language from the remaining subject matter.

The draft Regulation does not clarify whether implied consent (i.e. consent inferred from the conduct of the individual) will be valid or not. The reference to "**clear affirmative action**" in the definition of consent in the draft Regulation points towards the rejection of implied consent. However, the deletion of the words "**explicit**" from such definition in the Council draft and the fact that the same draft distinguishes between "**explicit consent**" for special categories of personal data and just "consent" for other type of personal data, open the window to a potential acceptance of implied consent in the final draft of the Regulation.

Consent not freely-given and significant imbalance of positions

To be valid, consent must be freely given. This means that the individual must have a free choice to accept (or not accept) the proposed uses of personal data. In the Commission draft one of the cases where consent may not be regarded as free is where there is a "significant imbalance" between the positions of the data subject and the controller. This may prove a significant hurdle in contexts where the respective positions of the parties are mostly inherently unequal, such as the employee-employer relationship.

Protection of children

Any consent given by a child under 13 in an online context will only be valid, according to the Commission draft, if that consent is either given or authorised by that child's legal guardian. The other drafts extend that requirement beyond the online context, to cover situations where any goods or services are offered directly to a child under 13.

Processing not based on consent

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 processing operations is where the data processing activities are 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 the pre-contractual activities are undertaken.

A further basis for processing, which is significant from a practical point of view, is where the processing is undertaken in order to comply with an obligation imposed on the controller by applicable law.

Crucially, both the Data Processing Directive and the draft Regulation contain a provision under which the legitimate interests pursued by a controller can justify the data processing. When relying on this ground, those legitimate interests should be weighed against the fundamental rights or freedoms of the individual. Only when such rights do not override the legitimate interests of the controller are such legitimate interests a valid ground for processing. This balancing test between the controller's legitimate interests and the rights of individuals must be carefully assessed in practice in order to be confident that it provides a solid ground for ongoing data processing activities.

Sensitive personal data

Under the Regulation, a special category of personal data – so-called sensitive personal data – will continue to enjoy a higher level of protection. The types of information that are regarded as sensitive personal data are expressly enumerated and include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life. The draft Regulation adds certain new categories to the existing list under Data Protection Directive, including genetic data and data about criminal convictions or related security measures.

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 data 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. A new processing ground is proposed in the Parliament draft: the processing of sensitive data should be justified if it is necessary to perform a contract concluded with the data subject or prior to entering into a contract – if the data subject requested that the pre-contractual activities are undertaken. 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 draft Regulation provides additional safeguards in connection with the processing of health-related data as well as the processing of personal data for historical, statistical and scientific research purposes.

Cessation of processing

The processing of personal data must cease if the basis for processing that provided the justification for the processing activities is no longer applicable, unless there is another justification for data processing that is still valid.

What to do now

- Businesses will need to review existing templates and procedures to ensure any consents are clearly distinguished.
- Businesses processing personal data of minors under 13 on the basis of consents will need to prepare strategies for obtaining guardian consents or authorisations.
- Employers and other controllers in positions of significant imbalance of powers will need to minimise the need for obtaining employee or other similarly positioned data subjects' consent.

New and stronger rights

Marco Berliri, Massimiliano Masnada, Sian Rudgard and Giulia Mariuz

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 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'.

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 of the processing including the key contractual terms if the processing is based on a contract between the controller and the individual, or whether the processing is based on legitimate interests
- The period for which the personal data will be stored
- The nature of the rights of available under the law, including the contact details of 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
- Sources 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 or voluntary, as well as the possible consequences of failing to provide such data.

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 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 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
- a court order rules that the data must be erased
- 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 as the Council draft proposes a number of limits.

The right to data portability

The Commission Draft 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 Council draft proposes the right shall apply only to data that was provided by the data subject to the data controller.

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. In general such profiling will require explicit consent from the individual, although there are some exemptions.

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

Joke Bodewits and Patrice Navarro

Quick read

- Profiling is a discrete data processing activity that will be strictly regulated.
- Profiling activities will only be permitted in narrowly specified cases.
- 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.

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 draft Regulation includes various restrictions on profiling, which is not defined in the Commission draft, but includes analysing personal preferences or behaviour. As a general rule, under the Regulation individuals should not be subject to decision-making measures based solely on profiling, when such measures produce 'legal effects' on them (e.g. a bank decides not to grant a mortgage on the basis of profiling information), or significantly affect them.

Profiling activities will only be permitted: (i) with the data subject's explicit consent, (ii) if expressly authorised by EU or Member State law, or (iii) carried out in the course of entering into a contract or performing a contract between the data subject and the data controller. In addition, there will be a blanket prohibition on profiling based on sensitive personal data and an express obligation to inform upfront about profiling activities.

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 wishes by the data subject, either by a statement of 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 process continues its course and the framework is finalised, it is crucial to understand that practical implications for businesses and the digital economy as a whole. It is quite likely that the Regulation will regard profiling as a high risk activity that will be 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 legitimising those activities. Given the perceived risks of profiling, this simply 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.
- To the extent that consent is likely to be required, identify the most appropriate mechanism and how to deploy it in practice.

The new accountability regime

Mac Macmillan and Sarah Taieb

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.

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?

Article 22.1 of the current version of the Regulation relating to the Obligations of the controller provides that:

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

The three drafts of the Regulation currently in circulation differ in how prescriptive they are about what is required in practice by Article 22 and the principle of accountability. They variously include the following elements:

- Adoption of a privacy policy and implementation of measures to ensure that an organisation's processing of personal data complies with 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). Although his prescribed tasks vary between the three drafts, the role of the DPO is critical for accountability. He 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.

How can businesses start to prepare?

Whatever the final text of the Regulation, 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. 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
- 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.


5 4

Data processors' new obligations

Christian Tinnefeld and Katie McMullan

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.

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
- There are significant penalties which can be imposed on processors for failure to comply with their increased responsibilities
- 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
- If processors act outside the authority given to them by controllers, they may be deemed a joint controller and therefore held to an even higher standard of accountability.

The new rules are considered in further detail below and will be triggered where:

- the processor is established in the EU
- EU law applies to the activities of the controller.

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:

- Maintain documentation. Most processors will be required to maintain documentation about the processing operations under their responsibility, such as the name and contact information of the controller/s the processor is acting on behalf of, the purposes of the processing, any legitimate interests pursued by the controller (where relevant) and information about retention periods. The main difficulty with this provision is that much of the information that is required will be information about the controller, but the obligation to maintain it lies with both parties which, in practice, means that controllers and processors will be required to document their relationship and the processing activities in much more detail. 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 and must also alert and inform a controller immediately after the establishment of a personal data breach
- Carry out data protection impact assessments. The Regulation requires impact assessments to be carried out when processing operations present certain specified risks, either by the controller or the processor acting on their behalf
- Obtain prior authorisation or undertake prior consultation. The processor will be required to consult or obtain prior authorisation from the relevant supervisory authority prior to certain processing activities being undertaken
- Appoint a data protection officer. Many processors will be required to appoint a data protection officer if certain thresholds are met
- Comply with the international data transfer requirements
- Co-operate with a supervisory authority if requested to do so, for example by submitting documentation to demonstrate compliance with the above responsibilities.

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 specific requirements which must be placed on processors are as follows:

- Only to act on the instructions from the controller, in particular where the transfer of personal data is prohibited
- Ensure that the processor's staff are committed to confidentiality
- Take all security measures as required by the Regulation

- Sub-contract only with the prior permission of the controller (so deals being negotiated currently should ideally be future-proofed by obtaining this consent now)
- Agree with the controller the necessary technical and organisational requirements for fulfilment of data subjects' rights in accordance with the Regulation
- Assist the controller with complying with the breach notification, data protection impact assessment and prior authorisation obligations contained in the Regulation
- Hand over results at the end of the processing and not process data otherwise
- Make information available to the controller and supervisory authority in certain circumstances.

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.

Joint controllers

According to the draft Regulation, where a processor processes personal information other than as instructed by the controller, it will be considered a controller in respect of that processing and subject to the prescribed rules regarding joint controllers. These include an obligation on the joint controllers to define their respective responsibilities and agree on who will conduct the necessary procedures for subject access requests. It is unclear how this provision will work in practice, but it will likely require controllers and processors to document the processor's tasks in more detail. It may also have significant impact on the way that cloud service providers manage their services in Europe, which could impact the costs of such services going forward. However, the Council has deleted this provision from its latest text.

Sanctions for non-compliance

The Regulation proposes penalties of up to 2% 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. In particular, it is a significant change from the current Directive that processors will be directly liable for certain fines when there has been a breach which will very likely impact on negotiations with service providers, 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. The Regulation also encourages the drawing up of codes of conduct and certification mechanisms by data protection authorities, 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 and those who do so will have a competitive advantage.

What to do now

- 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

Martin Pflueger, Rik Zagers and Hannah Jackson

Quick read

- The existing restrictions affecting international data transfers are set to continue under the Regulation.
- Existing adequacy findings and Safe Harbor will in principle continue to be valid.
- The Regulation seeks to extend 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 expected to be simplified.

What's the deal?

The Data Protection Directive and the Regulation both impose restrictions on the transfer of personal data by EU based businesses 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:

- 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 a dozen countries, along with the US Department of Commerce's U.S.-EU Safe Harbor Framework 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 standard contractual clauses approved by the Commission ("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, BCRs or the U.S.-EU Safe Harbor Framework. This approach is essentially set to continue with some variations.

Adequacy

The Regulation allows for the designation of not only third countries but also specific territories, sectors and states within such countries 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 the ability of the Commission to decide that a third country no longer ensures an adequate level of protection.

Existing adequacy decisions made by the Commission under the Data Protection Directive will continue to remain in force. The Parliament draft proposes a limitation for those existing decisions, meaning that they will remain valid for only five years after the Regulation comes into force. However, this is strongly disputed and reflected in neither the Commission draft nor in the Council draft.

Despite recent discussion, and unless otherwise repealed or amended, the U.S.-EU Safe Harbor Framework will continue to be recognised under the Regulation as providing for an adequate level of data protection for transfers of personal data from the EU to the U.S.

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 Draft Regulation explicitly provides that this will no longer be the case.

In addition, the Regulation seeks to further extend the options and procedures available to data controllers to legitimise international transfers (such as standard and ad hoc contractual clauses and codes of conduct adopted or authorised by DPAs). The exact mechanisms, however, are still being debated and the draft texts of the Commission, the Parliament and the Council differ significantly.

The Parliament draft proposes that international transfers should be permitted where both the data exporter and the data importer hold a valid "European Data Protection Seal" in accordance with the requirements set out in the Regulation. This is, however, not reflected in the same way by the other draft texts and it remains to be seen whether it will find its way to the final version of the Regulation. Further, the Parliament draft envisages the limitation of the validity of existing Commission decisions on the adequacy provided by the use of EU Model Clauses to five years after entry into force of the

Regulation. However, this is strongly disputed and not reflected in the Commission draft or in the Council draft.

Importantly, although BCRs for processors are not explicitly mentioned in all drafts of the Regulation, given the clear recognition by the data protection authorities, they are likely to remain an innovative mechanism under which data processors can assist data controller clients to meet their obligations in relation to the international transfer of personal data.

Derogations

The derogations set out in the Data Protection Directive will continue to apply under the Regulation. In addition, the Commission and Council drafts provide that transfers which are not frequent and/or massive (or, respectively, "large scale" as stipulated by the Council draft) could be allowed if the transfer is necessary for 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. The data controller is also subject to a documentation obligation which requires a full record of the transfer and the further processing operations to be kept.

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 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 Contracts 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 Draft Regulation formally recognises BCRs as a valid transfer mechanism and sets out uniform rules for their adoption. The Regulation is expected to simplify the BCR approval process and further strengthen 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.

Derogations

Since the Regulation provides that transfers are also allowed on the basis of legitimate interests of the controller, we may see an increase in data transfers based on this derogation. This will particularly be the case 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

Marcus Schreibauer, Jan Spittka and Lilly Taranto

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 a damage is suffered.
- Heavier fines against data controllers and data processors of up to €1 million or 2% of annual worldwide turnover whichever is higher.

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 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 business, but could potentially make it difficult for individuals to pursue complaints.

Some DPAs also raised concerns that it could lead to forum shopping. The three drafts in circulation provide different solutions to the issue and it is likely that this will be one of the most hotly debated provisions during the trialogue stage.

In the Council draft this model applies:

- to data controllers with establishments in several Member States
- 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, 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 DPAs of the other affected Member States have to coordinate with the lead DPA to reach a consensus regarding the enforcement measures. If the involved DPAs are not able to reach a consensus, the European Data Protection Board will decide by simple majority.

A new European Data Protection Board will be established, with 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.

There is an 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 it 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 damage suffered as a result of processing carried out in breach of the Regulation (discussions are on-going as to whether this should include non-pecuniary damages). Where more than one data controller and data processor is 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 currently being considered include:

- a written warning in case of first and non-intentional breaches to individuals and organisations with less than 250 employees whose main business is not the processing of personal data
- Fines of up to €250,000 or up to 0.5% of the organisation's annual worldwide turnover for failure to deal properly with individual's rights
- Fines of up to €500,000 or up to 1% of annual worldwide turnover for failure to respond to subject access requests in line with the Regulation
- Fines up to €1 million or up to 2% of annual worldwide turnover for other compliance failures such as failure to comply with the requirements regarding profiling, failure to notify data breaches, transferring data internationally without adequate safeguards or failure to appoint a data protection officer.

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, its ultimate form and viability is still unclear, and there remains a risk that the trialogue process will result in an unwieldy mechanism that leaves us with the same or even greater uncertainty as to which regulator is the competent one.

What to do now

- 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 to 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.
- Closely monitor the enforcement actions and announcements of your competent DPA.

Data Protection in the workplace

Tim Wybitul

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.

Relevance of employee data protection for enterprises

Data privacy in an employment context remains an important 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 legitimate expectation of privacy – including at their workplace. This inherent conflict of interests has created a considerable volume of case law regarding employee monitoring in several member states, relating to the permissibility of 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 many jurisdictions. 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, and it is expected that 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 will considerably change 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, the new right of data portability means there will be a right to portability of data from one employer to another, and data privacy impact assessments may be required in many aspects of work life. 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.

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 draft Regulation will be particularly relevant in an employment context, since 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.

However, Article 82 of the Parliament draft also contains extensive additional provisions aimed at protecting the rights and freedom of employees. In accordance with the provisions of the Regulation and the principle of proportionality, member states may adopt specific rules regulating the processing of personal data in an employment context. Among other things, profiling or the use of employee data for secondary purposes as well as the processing of employee data without their knowledge will be prohibited.

It remains to be seen to what extent these employee-friendly provisions will actually make it into the final version of the Regulation. In any case, 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, member states may allow the processing of personal data to 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 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 and the Regulation does not resolve this issue. Therefore, it is unlikely that employee consent will ever be the most robust basis for the use of that data, and this needs to be factored in when justifying such uses.

What to do now

- 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.
- Align HR and data protection functions in order to ensure compliance with the new requirements.
- Analyse whether your business' personnel and data protection structures provide the level of transparency required by the new data protection rules.
- 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.

Our global Privacy and Information Management practice

Our global Privacy and Information Management 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 Information Management 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 Information Management 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 Information Management for over 25 years. Today Hogan Lovells has one of the largest and most experienced Privacy and Information Management 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).

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

Chambers Global, 2015

“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

Rankings and Awards

2015

Our global Privacy and Information Management 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*)
- BAND 2 for Europe-wide Privacy and Data Protection (*Chambers Europe*)
- Band 2 for UK-wide Privacy and Data Protection (*Chambers UK*)
- TIER 1 for Technology: Data Protection and Privacy (*Legal 500* US)

Our Privacy and Information Management 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 operating out of more than 45 offices in the United States, Latin America, Europe, the Middle East, Africa, and Asia.

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 reach

North America


R. Cashdan
Los Angeles


D. Hansell
Los Angeles


M. Maddigan
Los Angeles


R. Samuel
Los Angeles


V. Brennan
Northern Virginia


M. Larner
Northern Virginia


J.Talotta
Northern Virginia


C. James
Denver


S. Altman
Washington


K. Armstrong
Washington


B. Bennett
Washington


M. Bianchi
Washington


J. Bomberg
Washington


M. Brennan
Washington


B. Cohen
Washington


J. Denvil
Washington


M. Gitomer
Washington


S. Gold
Washington


D. Kaplan
Washington


M. Kisloff
Washington


M. Levine
Washington


J. Lolley
Washington


S.Loughlin
Washington


P. Otto
Washington


H. Pearson
Washington


M. Sneed
Washington


S. Spagnolo
Washington


T. Tobin
Washington


M. Wilder
Washington


C. Wolf
Washington


J. Cyr
New York


D. Hanswirth
New York


M. Yanez V.
Monterrey


F. de Noriega Olea
Mexico City


L. Gonzalez Cossio
Mexico City

Europe


Q. Archer
London


V. Hordern
London


H. Jackson
London


M. Macmillan
London


K. McMullan
London

S. Rudgard
London

L. Taranto
London

E. Ustaran
London

G. Gallego
Madrid

C. Ortiz-Urculo
Madrid

L. Badin
Madrid

J. Bodewits
Amsterdam

A. de Jong
Amsterdam

R. Zagers
Amsterdam

W. Maxwell
Paris

D. Taylor
Paris

P. Navarro
Paris

P. Le Bousse
Paris

M. Berliri
Rome

M. Masnada
Rome

G. Mariuz
Rome

M. Colonna
Rome

E. Wright
Brussels

N. Pourbaix
Brussels

N. Gulyaeva
Moscow

M. Sedykh
Moscow

M. Schreibauer
Düsseldorf

J. Spittka
Düsseldorf

B. Balas-Noszczyk
Warsaw

J. Baczuk
Warsaw

E. Kacperek
Warsaw

N. Rauer
Frankfurt

T. Wybitul
Frankfurt

D. Ettig
Frankfurt

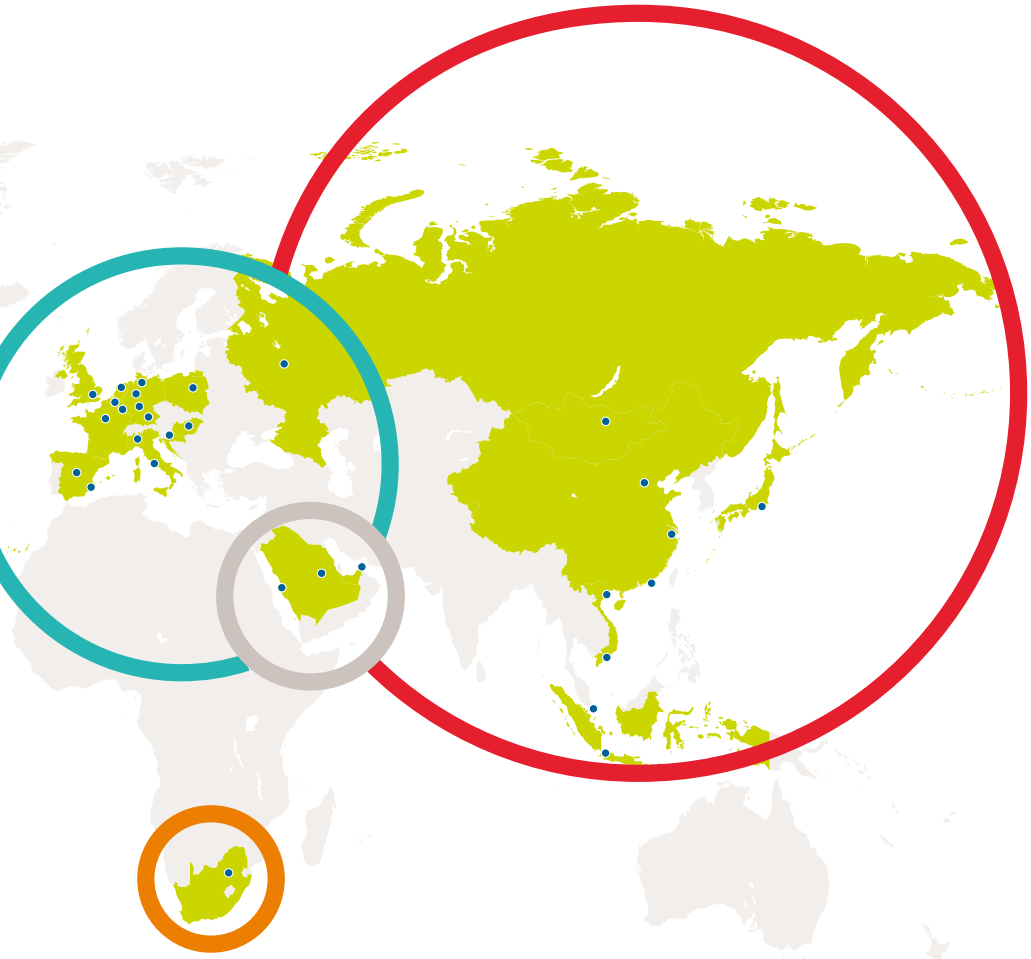
S. Schuppert
Munich

M. Pflueger
Munich

M. Fischer
Munich

C. Tinnefeld
Hamburg

C. Noblet
Budapest



Asia

J. Wei
Beijing

R. Zou
Beijing

M. Parsons
Hong Kong

P. Colegate
Hong Kong

H. Leung
Hong Kong

B. Lui
Hong Kong

South Africa

S. Monty
Johannesburg

L. Pillay
Johannesburg

Notes

www.hoganlovells.com

Hogan Lovells has offices in:

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
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Philadelphia
Rio de Janeiro
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Tokyo
Ulaanbaatar
Warsaw
Washington, DC
Zagreb*

* Associated offices