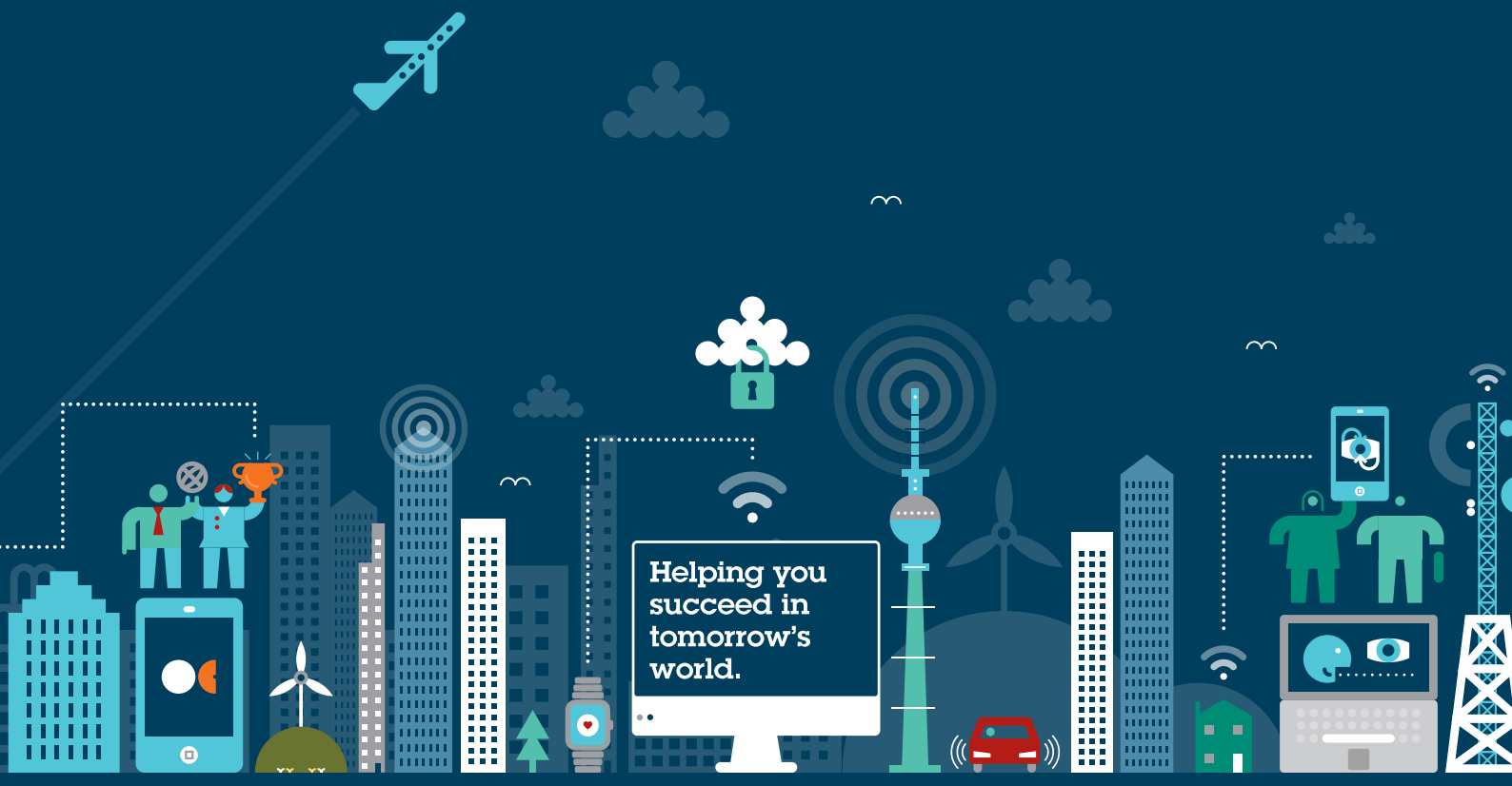
EU General Data Protection Regulation

A UK perspective on its key aspects

August 2016



After many years of debate, the European General Data Protection Regulation (GDPR) has finally been agreed and passed and the date has been set for its implementation: 25 May 2018.

While the impact of Brexit is currently uncertain, it is highly likely that the UK will continue to implement the GDPR in the short term and would need to maintain a law similar to the GDPR in the longer term. Statements from the UK Information Commissioner's Office (ICO) before and after the referendum have supported that view. Therefore, irrespective of whether or not your organisation has operations in other EU Member States (so that GDPR compliance would be required in any event), we recommend continuing with GDPR compliance projects as planned.

On the assumption that the GDPR (or something very similar) will apply in the UK, in this note we discuss the key areas of reform in the GDPR and what it means for businesses from a UK law perspective. We have prepared a separate, more detailed note on the implications of Brexit in relation to data protection and privacy.

The GDPR is an evolution of existing UK data protection law rather than a revolution. However, there are some significant changes that have the potential to have a profound impact on many organisations that collect and use information about individuals. This is especially likely if a company's approach to compliance with current data protection law requirements is patchy or inconsistent.

The importance of preparing and ensuring compliance with the new law cannot be understated, not least because of the huge fines of up to €20m or 4% of worldwide turnover that could be levied for breaches. There are other business benefits for those organisations that use the changes as an opportunity to adopt a fresh approach to thinking about data privacy and protection – not just as a hurdle to business or additional burden, but also as a way to build and enhance trust with their customers and employees.

Overall scope and territorial application

The GDPR will replace the UK's Data Protection Act 1998 (DPA) (and other laws enacted across all Member States to implement the EU Data Protection Directive 1995). Other laws covering data and privacy issues will continue in force, although work has started separately to assess if and how the e-Privacy Directive, which has been implemented in the UK as the Privacy and Electronic Communications Regulations covering data and marketing, will be updated.

The GDPR has a greater territorial reach than existing laws and so will apply to many more organisations around the world. EU organisations processing personal data in the context of their activities will be covered, regardless of whether the processing takes place in the EU. In addition, the GDPR will also apply to organisations with no establishment in the EU who process personal data of EU based individuals where the processing relates to:

- the offering of goods or services to those individuals, whether or not payment is required; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.

The GDPR applies to controllers of data – those who, alone or jointly with others, determine the purposes and means of the processing of personal data. For the first time, processors who process personal data on behalf of the controller will also have their own obligations and responsibilities under the GDPR (see below).

Types of data and processing activities covered

The GDPR covers very similar categories of data and activities as the DPA. Broadly it covers information relating to an identified or identifiable natural person. The new definition of personal data potentially broadens the scope of data covered and also specifically refers to identifiers such as an identification number, location data, an online identifier or to one or more factors specific to someone's physical, physiological, genetic, mental, economic, cultural or social identity. This also means that a name is not necessarily required for information to be caught by the GDPR – any means of unique identification is likely to be sufficient.

Specific obligations apply to the use of:

- **sensitive personal data** – information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, along with genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation – this is now referred to as "special categories of personal data";

- **profiling** – automated processing to evaluate, analyse and predict personal aspects, such as work performance, economic situation, health, behaviour, location; and

- **psuedonymisation** – processing data in a way such that it can no longer be attributed to a specific person without the use of additional information which is kept separately from it. (This is different to anonymisation, which in theory should not be reversible.)

The use of privacy notices

Transparency is a key theme of the GDPR and so the format, positioning, provision and content of privacy notices takes on new significance, especially where consent from data subjects is required before data processing can begin.

Privacy notices must be concise, transparent, intelligible and in an easily accessible form. They must also be drafted using clear and plain language.

The GDPR includes a list of information that must be provided to data subjects when data is collected. This includes: the controller's identity and contact details; the purposes and legal basis of processing; details on other recipients and cross-border transfers; the period for which data will be stored (or relevant criteria for determining this); the existence of data subjects' rights (see below) and the existence of any automated decision making.

These requirements must also be met if an organisation does not obtain information directly from a data subject. This leads to potential challenges for organisations that rely heavily on information gathered by third parties.

Legal basis for processing and consent

Controllers must ensure that they have a legal basis to process the information, and not process data beyond the purposes for which it has been obtained. In most cases, controllers will be able to easily satisfy this requirement where data is required to perform a contract (e.g. a home address required to deliver goods ordered online) or to meet a legal requirement (e.g. obtaining the national insurance number of employees).

It will also be possible to use data where an individual has specifically agreed to this. However, the requirements for consent are set to be more difficult for the following reasons:

- requests for consent must be clearly distinguishable from other matters in an intelligible and easily accessible form and use clear and plain language;

- data subjects must be able to withdraw consent as easily as it was given and must be told upfront that this is possible;

- where contract performance is conditional on consent to processing personal data that is not necessary for performance of that contract, such consent is unlikely to be "freely given"; and

- controllers must keep clear evidence of consents obtained.

Controllers may also hold and use personal data if the processing of that data is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Legitimate interests could include processing to prevent fraud, for direct marketing purposes, internal administrative purposes within a group, and ensuring network and information security.

However, this does not give organisations carte blanche to use data for any purpose whatsoever. Controllers cannot rely on this provision where the interests or fundamental rights and freedoms of the data subject override their own. Therefore, controllers will need to make a careful assessment in each case, including by taking account of the reasonable expectations of the data subject. It will be particularly difficult to rely on the legitimate interest condition where the data subject is a child.

Accountability, data protection by design and by default and record keeping

While the requirement to make an annual notification to the ICO falls away, there are plenty of other requirements to take its place as controllers become responsible for, and must be able to demonstrate, compliance with all of the principles relating to data processing. The principles in GDPR are broadly similar but stricter than the existing eight principles in the DPA. They are:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation; and
- integrity and confidentiality.

Security and international data transfers are dealt with separately (see below).

Accountability

Controllers will be expected to implement appropriate technical and organisational measures to ensure and demonstrate compliance with GDPR. It will no longer be enough for an organisation to be generally acting in a compliant way; they will also need to take steps to show that they are compliant. In practice, this will mean using a combination of software tools, training, staff awareness and data protection policies.

Data protection by design and by default

The GDPR emphasises the concept that data protection should not be an afterthought or an issue casually considered at the end of a project or bolted on to procedures; it must be central to the way that organisations plan and operate. Systems and processes must be designed with data protection compliance in mind and must by default ensure that only data necessary for each specific purpose is processed and that it is not accessible to an indefinite number of individuals.

There is also an emphasis on using measures (such as pseudonymisation and data minimisation) designed to implement data protection principles and a requirement to think about appropriate organisational and technical measures, not just at the outset but throughout the period that the data is processed.

Privacy impact assessments

For some time the ICO has been recommending that privacy impact assessments are carried out in certain circumstances, but now this concept is specifically included in the GDPR. Such assessments will be required before processing activities commence, especially if they involve "new technologies", are likely to result in high risk to rights and freedoms such as automated processing (including profiling), or include large scale processing of "special categories" of data.

Any impact assessment will need to involve an organisation's data protection officer (if there is one – see below) and consider the nature, scope, context and purposes of the processing and involve a systematic and extensive evaluation of the processing operations, the purposes of them, their necessity and proportionality in relation to the purposes, an assessment of risks and rights of the data subjects involved and the measures envisaged to ensure protection of personal data.

Controllers will be expected to seek the views of data subjects or their representatives and in certain circumstances consult with the ICO (or other relevant data protection authority). Given the likely timescales involved in consulting with the ICO (up to eight weeks with a possible extension of six weeks or more if further information is required from a controller), controllers should approach any high risk processing with caution and ensure that substantial measures are in place to mitigate any risks so that no consultation with the ICO is needed. We also await further guidance on the meaning of "high risk", which will be helpful in assessing when consultation may be required.

Data protection authorities, including the ICO, are required to issue "white lists" and "black lists" of processing for which an impact assessment is or is not required. These should help controllers to decide whether to carry out impact assessments and whether to consult or not.

Record keeping

Controllers will in future also be required to maintain written records of their processing activities, except in certain limited circumstances, and must make these available to supervisory authorities on request.

The records should include: the name and contact details of processors, each controller and (where applicable) representative and data protection officer; purposes and categories of processing; categories of data subjects; categories of recipients of personal data including overseas; details of transfers outside the EEA, including documentation of appropriate safeguards; data retention periods; and a general description of technical and organisational security measures.

Data Protection Officers

A Data Protection Officer (DPO) will need to be appointed if an organisation's core activities consist of either:

- processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- processing of special categories of data **and** personal data relating to criminal convictions and offences in specific circumstances on a large scale.

We are expecting further guidance on the application of these terms and the meaning of "large scale". In other cases, a DPO is optional unless required by EU or local law.

Even if not strictly required, many organisations may decide that there are benefits in having a DPO, such as centralising compliance, having a main point of contact and giving clarity around the responsibility for overall compliance within an organisation. In all cases, organisations need to ensure that they provide their DPO with necessary resources, and access to data and relevant business operations.

It will be possible for a group of undertakings to appoint a single DPO but they must be easily accessible from each company. So, for companies with multiple offices across different time zones and/or locations, more than one DPO may be needed.

The DPO is expected to have expert knowledge of data protection law and practice and could be an employee or an external contractor, such as a consultant or law firm. Their role is to be involved in all data protection issues in a timely manner and to monitor compliance as well as be a source of advice internally, and act as a single point of contact externally.

The DPO plays an important and in many ways unique role in acting as an independent observer and monitor of data protection compliance. Whilst they may perform other duties in their day-to-day activities, there cannot be any conflict of interest. They cannot be instructed in their role and, from an organisational perspective, will be expected to report to the highest level of management. Finally, they may not be dismissed or penalised for performing their tasks.

Enhanced security obligations and notification

Security is already a high priority in the face of significant and evolving risks. In many ways, GDPR highlights the growing importance of ensuring that personal data is kept secure by introducing new obligations and a requirement to notify security breaches to the ICO and individuals in some circumstances.

Security obligations

In general, organisations are expected to fully assess and then implement measures to ensure a level of security which is tailored and appropriate to the risk. For the first time, there are security measures specifically covered in the GDPR, such as:

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

Breach notification to regulators

Controllers must report "personal data breaches" to the ICO (or other relevant data protection authority) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in risk for the rights and freedoms of individuals.

A personal data breach is defined quite widely to include: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". A number of different types of incident could therefore trigger a requirement to notify.

The notification itself must include various information, such as, a description of the nature of the breach, the categories of data and number of people involved and approximate number of records. Both the effect and remedial action taken by the controller must be provided. Whilst this information may be provided in phases, it nonetheless highlights the importance of good incident management policies and processes, not least so that controllers can make an informed decision about whether to notify and how this should be managed effectively.

Breach notification to data subjects

The GDPR also introduces a new requirement to notify affected individuals without undue delay if their rights and freedoms are put at high risk. The notification must describe the nature of the breach in clear and plain language and also include details of the DPO (or other contact point), the likely consequences, and the measures being taken to address the breach.

There is an important exception to the requirement to notify if one of certain conditions has been met:

- the controller has implemented measures to protect the data, including those that render the data unintelligible, for example, encryption;
- the controller has taken measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or
- notifying data subjects would involve disproportionate effort, although in such circumstances a public communication is then envisaged.

The ICO (or other supervisory authority) may also require a controller to notify data subjects even if the controller had previously decided not to notify them.

The GDPR emphasises the concept that data protection should not be an afterthought or an issue casually considered at the end of a project or bolted on to procedures; it must be central to the way that organisations plan and operate.

Using data processors

Controllers using data processors to carry out data processing on their behalf will need to bear in mind much stricter requirements as the controller/processor relationship becomes more heavily regulated. The requirements apply regardless of the volume or sensitivity of processing.

Before appointing a data processor, controllers will be expected to assess whether a processor has provided sufficient guarantees to ensure that the GDPR requirements will be met and the rights of data subjects will be protected. This will require careful due diligence and review, including by taking into account any approved codes of conduct with which a processor complies.

Instead of merely a requirement to have a written contract covering security related obligations as now, the GDPR sets out much more prescriptive requirements for a binding contract between the controller and processor, which must include:

- the subject matter and duration of processing;
- the nature and purpose of processing; type of personal data;
- the categories of data subjects; and
- the obligations and rights of the controller.

The contract itself must also include specific provisions, which could in due course be covered by standard contractual clauses (similar to those used for data transfers) laid down by the European Commission. The contract must specify that the processor:

- follows the controller's instructions (including regarding data transfers outside the EEA);
- imposes confidentiality obligations on persons handling data;
- ensures the security of processing (as described above);
- notifies the controller of any personal data breaches;
- does not engage sub-processors without the controller's consent and a written contract flowing down the same obligations;
- assists the controller in responding to requests from data subjects;
- assists with consultations with supervisory authorities;
- allows the controller to decide whether data should be deleted or returned on termination of the contract;
- supports the controller by providing evidence of compliance and audits; and
- notifies the controller if any of their instructions breach the GDPR or UK data protection law provisions.

If the processor starts to determine the purposes and means of processing, then it will be considered a data controller and will itself be responsible for compliance with the more detailed and stricter requirements imposed on data controllers.

New processor obligations

For the first time processors will be directly responsible for compliance with data protection law, which is a significant change for those organisations acting as processors who up until now have only faced the obligations contractually flowed down to them by their customers who are controllers.

The key new areas for processors to consider and implement include a specific requirement:

- not to sub-contract their processing activities without controller consent;
- to maintain records of processing carried out on behalf of controllers, which must include: the name and contact details of processors, each controller and (where applicable) representative and DPO for each; categories of processing for each controller; transfers of data outside the EEA, including identification of the country; documentation of appropriate safeguards; a general description of technical and organisational security measures;
- to implement appropriate data security measures and notify controllers of security breaches;
- to appoint a DPO (where applicable); and
- to ensure that transfers of personal data out of the EEA are compliant.

A failure to comply with these requirements may result in enforcement action by the ICO (or other relevant regulator) but a processor will only be liable where they do not follow the processor-specific obligations set out in the GDPR or the controller's lawful instructions.

Additional data subject rights and enforcement

The GDPR builds on existing data subject rights and adds some new rights that organisations processing personal data will need to consider so they can respond promptly and to the relevant individual's satisfaction.

Data subjects will have the right to be told whether data about them is being processed and to be provided with various details about that processing activity, which broadly mirrors what they should be told when their data is collected (see above). They are also entitled to be told the source of the information, where it was not collected directly from them, and be provided with a copy.

Individuals will be able to request that any inaccuracies about their information are rectified without undue delay and to be able to restrict a controller's processing activities, especially where the accuracy of the data is contested or the grounds for processing are considered unlawful. They could also object to processing which a controller was carrying out based on the controller's legitimate interests, such as direct marketing or profiling, or where decisions were being made based solely on automated processing including profiling.

However, there are two new rights that particularly stand out as being new and giving data subjects significant controls over their information.

- Firstly, the right to erasure of personal data, the so-called "right to be forgotten". This will enable a data subject to request that their information is deleted where it is no longer necessary in relation to purposes for which it was collected, or they withdraw consent (and no other ground for processing applies), or the processing is unlawful. If data has been made public by a controller, then they must delete it as far as possible taking into account available technology and costs. Requests must be satisfied without undue delay. There are, however, some potentially useful derogations that may apply, such as where a controller would need to retain information to comply with legal obligations, such as employee tax records.
- Secondly, there is a new right to data portability, which will mean that data subjects will have the right to request that their data is moved to another controller in a structured, commonly used and machine-readable format if technically feasible.

International data transfers

The existing cross-border transfer rules and derogations remain largely unchanged, in that in order to transfer data outside of the EEA, one of a number of solutions must be in place. These include: data subject consent; a finding of adequacy in respect of the recipient country; standard/model contractual clauses; binding corporate rules; or that the transfer is required for the performance of a contract.

However, the position as regards transfers looks set to be less certain going forwards because future European Commission decisions on adequacy will be subject to periodic review at least every 4 years.

If a controller wants to use non-standard contractual clauses, they will need to obtain approval from the ICO or another appropriate data protection authority. In addition, if data subject consent is relied upon, it must be explicit and the individual must have been informed of the risks – again this emphasises the focus on transparency.

There is a potentially useful new "derogation" where other standard derogations cannot be used, if the transfer is: not repetitive, concerns only a limited number of individuals, is necessary for the purposes of compelling legitimate interests of the controller and where this is not overridden by the interests, rights or freedoms of the data subjects involved. The controller must also have assessed all the circumstances, adduced suitable safeguards, informed its data protection authority and notified the data subjects of the transfer and the "compelling legitimate interest" of the controller.

Supervision by regulators

Generally speaking, the current position is that controllers are supervised by the national data protection authorities in those countries in which they operate and are established. There is some limited co-ordination but local differences exist, not least because there are different local laws and the approach taken by data protection authorities differs considerably.

The aim of the GDPR is to harmonise the approach to supervision, enable controllers and processors to deal with one main regulator, and also provide individuals with easier access to a supervisory body for complaints purposes.

To address these aims, the GDPR enables controllers and processors with establishments in more than one EU member state to deal primarily with their lead supervisory authority. The lead supervisory authority will be located in the country where the controller or processor has their "main establishment" – meaning where their "central administration" and decision making power is based. For processors without any central administration in the EU, then their main establishment will be the member state where the main processing activities are carried out.

However, regardless of which data protection authority is the lead supervisory authority, any data protection authority will be able to deal with complaints lodged by data subjects where the complaint in effect relates only to their country. So, for example, even if a controller chooses the Spanish data protection authority as its lead supervisory authority, if an individual in France has a complaint solely affecting data subjects in France, then the French data protection authority, the CNIL, will have competency to deal with it.

As well as having the power to issue fines (see below), supervisory authorities will have wide powers to investigate potential breaches, including ordering controllers and processors to provide information, to carry out data protection audits, and to obtain access to premises and equipment. They will be able to issue warnings, order specific compliance measures to be taken and suspend cross-border data flows. They will also have an advisory role and can authorise various measures, such as non-standard contractual clauses or certain types of processing activities, as mentioned above.

Fines and enforcement

The sanctions being introduced by the GDPR will significantly change the enforcement landscape. In the UK, the maximum current fine is £500,000. Under the GDPR, the ICO and all other data protection authorities will have the power to issue fines of up to the higher of 4% of worldwide turnover or €20,000,000. The fines could be levied against data controllers and/or processors.

The types of breaches that could lead to fines of the highest level include: breaches relating to consent, rights exercised by data subjects and transfers outside the EEA. There is also a lower tier of fine for other breaches, of the higher of 2% of worldwide turnover or €10,000,000.

There are also rights to compensation for data subjects which together with a new concept of the "representation of data subjects", could create a significant new class action threat.

For the first time processors will be directly responsible for compliance with data protection law.

What do you need to do to prepare for the GDPR?

Many organisations will need to start taking steps towards compliance now to ensure they are ready for 2018. Some organisations are already contracting on the basis that the new rules apply. For many, the key challenges will be working out where to focus efforts, getting budget, allocating responsibility and deciding how to get started. The following six steps may help to guide that process.

1. **Lay the foundations:** by raising awareness, reviewing GDPR guidance and prioritising the tasks ahead;
2. **Gather information:** to get a clear picture of what personal data you currently process, how you use it and what compliance measures you currently have in place;
3. **Review and assess:** by performing a gap analysis of your current compliance measures against the more stringent requirements of the GDPR;
4. **Implement change:** by putting in place the necessary policies and procedures, rolling out training to staff, making any technical changes to your online platforms, re-negotiating contracts (where necessary) and refreshing consents (again, where necessary);
5. **Complete the finishing touches:** the remedial steps which you have identified as lower risk or easier to implement; and
6. **Follow up with on-going monitoring and maintenance:** to identify any areas that are not working perfectly and adjust accordingly, and adapt to changes in your business or GDPR guidance.

We have produced a more detailed note on what steps to take to prepare for the GDPR and how to manage compliance. If you would like a copy, please get in touch.

If you would like to discuss how the GDPR impacts on your organisation in more detail, for example, to plan your roadmap to compliance, consider what you should be doing now, and decide which are the key areas of risk, please do not hesitate to get in touch with one of our data protection team.

Osborne Clarke in numbers

215+
expert partners

600+
talented lawyers

20
well-connected offices

14
languages

7
key sectors

1
client-centred approach

Key contacts

Mark Taylor
UK
T +44 20 7105 7640
mark.taylor@osborneclarke.com

Emily Jones
US
T +1 650 714 6386
emily.jones@osborneclarke.com

Will Robertson
UK
T +44 117 917 3660
will.robertson@osborneclarke.com

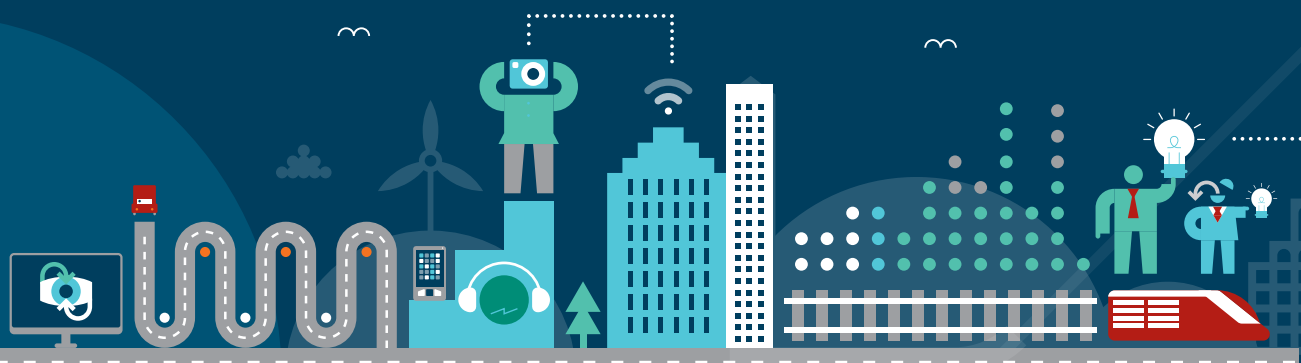
Ashley Hurst
UK
T +44 20 7105 7302
ashley.hurst@osborneclarke.com

Where we work

Belgium: Brussels
France: Paris
Germany: Berlin, Cologne, Hamburg, Munich
Hong Kong
India: Mumbai*
Italy: Milan, Brescia, Padua, Rome
Singapore
Spain: Barcelona, Madrid
The Netherlands: Amsterdam
UK: London, Bristol, Thames Valley
USA: Silicon Valley, New York, San Francisco

Osborne Clarke is the business name for an international legal practice and its associated businesses. Full details here: osborneclarke.com/definitions
*Relationship firm

osborneclarke.com



August 2016
Publication number
30420341