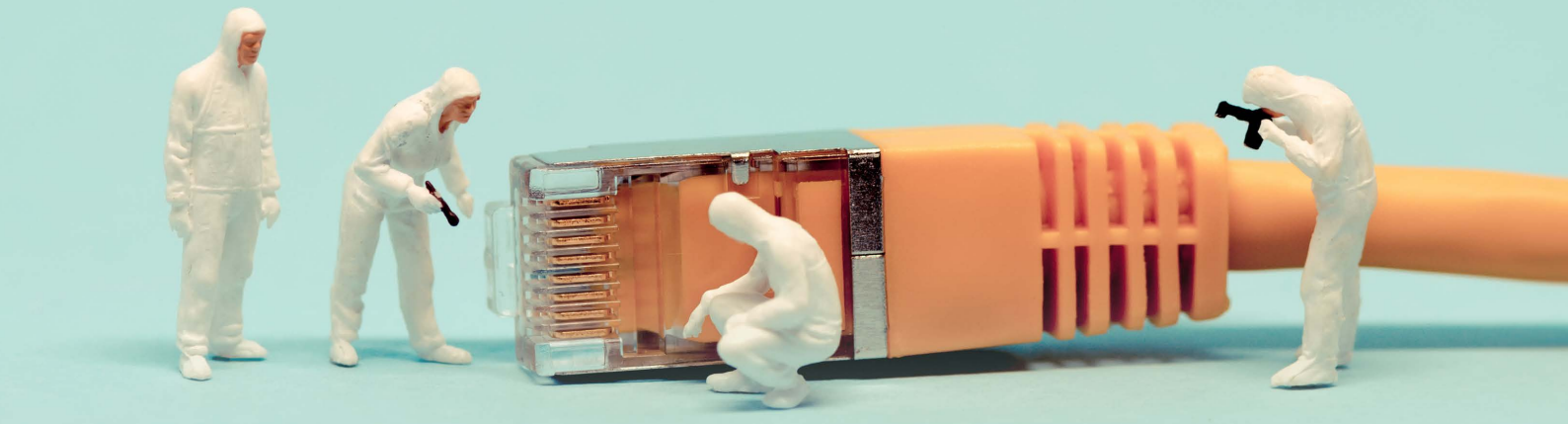
Your World First

C/M/S/
Law.Tax

The EU General Data Protection Regulation



2016

Contents

Introduction

The EU data protection landscape, having remained largely unchanged since 1995, is now on the brink of a radical transformation. After extensive negotiations, the GDPR was formally adopted on 4 May 2016 and is set to replace most EU data protection legislation, including the DPA in the UK.

Unlike the current Directive, the GDPR will be directly applicable in all EU Member States without the need for national legislation. It will apply from **25 May 2018**.

The GDPR brings new concepts into the regulatory spotlight, including profiling and the right to be forgotten. It imposes extensive new obligations on businesses and transforms the role of the Data Processor. Rights for individuals are significantly strengthened and maximum fines in respect of breaches are increased exponentially from £500,000 under the DPA, to up to €20,000,000 or 4% of annual worldwide turnover under the GDPR.

This Brochure aims to explain the main differences between the Directive/DPA and the GDPR. We have used weather themed icons for categorising the changes, so that at a glance, you can see how this may affect your business.

Please see our Glossary on page 21 for an explanation of the defined terms and abbreviations that we have used in this Brochure.

If you would like more information on the GDPR or the DPA, please contact one of us.

Alan Nelson
Partner, Technology
T: +44 141 304 6006
E: alan.nelson@cms-cmck.com

Duncan Turner
Senior Associate, Technology
T: +44 131 200 7669
E: duncan.turner@cms-cmck.com

Jennifer Barr
Associate, Technology
T: +44 141 304 6233
E: jennifer.barr@cms-cmck.com

General Data Protection Regulation timeline

7 December 2011
Draft of the proposed General Data Protection Regulation leaked and published online.

25 January 2012
European Commission formally publishes draft of the proposed Regulation (the 'Commission Draft').

30-31 May 2012
European Parliament Committee on Civil Liberties, Justice and Home Affairs (the 'LIBE Committee') commences discussions on the Commission Draft.

July – October 2012
LIBE Committee publishes three European Parliament working documents on the Commission Draft.

October – November 2012
European Parliament leads an inter-parliamentary hearing with national parliaments.

10 January 2013
LIBE Committee publishes a draft report on the Commission Draft including proposed amendments to it.

31 May 2013
European Council publishes key issues document on Chapters I to IV of the Commission Draft.

21 October 2013
LIBE Committee votes on a compromise text of the proposed Regulation.

12 March 2014
European Parliament holds a plenary vote in first reading of the proposed Regulation and adopts the LIBE Committee's compromise text (the 'Parliament Draft').

European Commission publications

European Parliament publications

European Council publications

May 2014 – March 2015

European Council agrees a partial general approach on Chapters II, IV, V, VI and VII of the proposed Regulation.

15 June 2015

European Council adopts a general approach on the proposed Regulation (the 'Council Draft').

24 June 2015

First trilogue meeting held between the Commission, Parliament and Council to agree an overall roadmap for trilogue negotiations.

July – December 2015

Further trilogue meetings held to negotiate the Commission Draft, Council Draft and Parliament Draft with the aim of agreeing the final text of the Regulation.

15 December 2015

The Commission, Parliament and Council reach agreement on a compromise text of the Regulation after months of trilogue negotiations.

12 February 2016

European Council confirms agreement on the terms of the Regulation by adopting a political agreement on its text.

8 April 2016

European Council formally adopts the Regulation.

4 May 2016

The General Data Protection Regulation published in the Official Journal of the European Union.

25 May 2016

The Regulation comes into force.

25 May 2018

The Regulation comes into effect at the end of the two year implementation period.


The Hague
London
Brussels
English Channel
Paris
FRANCE
Geneva (Genève)
Lyon
Bordeaux
Nantes
Brest
Le Havre
Strasbourg
Munich
Bay of
Biscay

Jurisdictional scope

Data Controllers that are established within the UK and Process Personal Data in the context of that establishment are currently subject to the DPA. These persons/businesses will also be subject to the GDPR when it takes effect, but the GDPR casts the net wider in terms of its jurisdictional scope. The GDPR will also apply to Data Processors whereas the DPA does not.

For Data Controllers established outside of the UK (and EU) the criteria for determining if they must comply with the GDPR, is significantly altered, as compared to that set out in the DPA/Directive.

Under current law, Data Controllers are subject to the DPA if they are established outside of the European Economic Area but they use equipment in the UK for Processing Personal Data (except for the purposes of transit).

In comparison, the jurisdictional scope of the GDPR is wider. Data Controllers and Data Processors based outside of the EU will be required to comply with the GDPR, if their Processing activities are related to:

— the offering of goods or services (free of charge or paid for) to individuals in the EU; or

— the monitoring of the behaviour of individuals in the EU.

The recitals to the GDPR indicate that websites which use a language or a currency that is generally used in an EU Member State and offer individuals the option of ordering goods or services in that language/currency, or which specifically mention EU-based customers/users, may fall within this definition.

In terms of monitoring within the EU, the recitals to the GDPR say that it will be necessary to consider if individuals are tracked online or subjected to profiling, particularly in order to take decisions about the individual or for the purposes of analysing or predicting personal preferences, behaviours and attitudes.

Data Controllers and Data Processors that are established outside of the EU, but which target individuals in the EU, may fall within the scope of the GDPR. If this is the case, they should carry out an analysis of the obligations contained within this legislation to ensure that they are able to comply. Most businesses which fall into this category will also need to appoint an EU-based representative.

Preparation for implementation: Non-EU established Data Controllers and Data Processors should check these new rules as soon as possible. If their Processing activities do fall under the criteria above, they must comply with the GDPR and should start preparing to do so well in advance. Consider if you need to appoint an EU based representative.

Fines/Enforcement

Under current laws in EU Member States, fines that may be levied for breaches of data protection law vary significantly. In the UK, the DPA provides for a maximum fine of £500,000 for a serious breach by a Data Controller. Under the GDPR, the level of fines may be significantly higher and can apply to Data Processors as well as Data Controllers.

The GDPR establishes a two-tiered system of administrative fines, which is applicable to both Data Controllers and Data Processors (although the question of whether or not such fines should be levied against public authorities is delegated to national lawmakers). Some infringements (for example of provisions relating to keeping records of Processing) are subject to fines of up to €10,000,000, or for an '*undertaking*', up to 2% of worldwide annual turnover in the previous financial year, whichever is higher. Others (such as breaches of the basic principles for Processing/conditions for obtaining consent) are punishable by higher fines of up to €20,000,000, or for undertakings, up to 4% of worldwide annual turnover in the previous financial year, whichever is higher.

Please see the Appendix at page 22 for tables setting out which breaches of the GDPR attract which level of fine and the factors that may be taken into account in determining the amount of the fine.

In terms of other types of enforcement by data protection authorities, this is also something that currently varies considerably between EU Member States under current data protection laws. In the UK, the ICO has powers to issue information notices and enforcement notices (although in practice the ICO often seeks undertakings committing an organisation to a particular course of action). It can also conduct audits and bring prosecutions for breaches of the DPA. Enforcement powers will, in general, be harmonised under the GDPR (although criminal enforcement is delegated to EU Member States). In the UK, these enforcement powers will be more wide-ranging than under the DPA. They include powers to issue warnings, reprimands and orders to Data Controllers and Data Processors; to impose temporary and definitive bans on Processing; to suspend overseas data flows; and to order the rectification or erasure of Personal Data.

The remedies available to individuals are also strengthened under the GDPR. These include rights: (i) to claim compensation from Data Controllers *and* Data Processors for damage caused by a breach of the GDPR; (ii) to an effective judicial remedy against Data Controllers *and* Data Processors in respect of the non-compliant Processing of Personal Data; (iii) to make a complaint to a Supervisory Authority; and (iv) to an effective judicial remedy against a Supervisory Authority that has not correctly handled a complaint.

Preparation for implementation: Organisations could prepare for the introduction of these provisions by identifying and addressing any current gaps in their data protection compliance, which may be considered low-risk now, but which could result in much higher exposure once the GDPR applies. It would also be advisable to identify the new obligations imposed by the GDPR and develop a plan for achieving practical compliance with these prior to 25 May 2018.


BCE ECB EZB EKT

Privacy notices

Under the GDPR, Data Controllers must take appropriate measures to provide information regarding the Processing of Personal Data to individuals in a concise, transparent, intelligible and easily accessible form, using clear and plain language (in particular, if the notice is addressed specifically to children).

Although organisations currently have an obligation under the Directive to provide notice of their Processing to Data Subjects (often facilitated through the use of privacy policies), the GDPR sets a higher standard of notice than the Directive by adding a significant number of prescribed new fields of information which must be provided. Such new fields of information include the period for which the data will be stored, the existence of various Data Subject rights, the source of the data in the event that it is not collected directly from the Data Subject, as well as details of the legal basis for the Processing and if the Processing is based on the Data Controller's legitimate interests.

Where data is collected from the Data Subject, notice does not need to be provided if the Data Subject already has the relevant information or if an exemption applies. Where data is not obtained directly from the Data Subject, notice is also not required if the provision of the information would be impossible or would involve disproportionate effort, the Processing is required by law or where the data must remain confidential subject to an obligation of professional secrecy.

The GDPR also provides for the future use of standardised icons to inform consumers about data Processing practices in a simplified format.

Preparation for implementation: Although the GDPR introduces much more extensive requirements for information notices, the advantage to organisations is that the GDPR is intended to lead to a standardised approach, such that a single notice is more likely to be sufficient across all Member States. Before the GDPR applies, organisations should be reviewing and updating their existing privacy policies to take into account the additional notice requirements introduced by the GDPR.

Consent

The GDPR amends the definition of consent under the Directive such that consent of a Data Subject to the Processing of their Personal Data must now be '*freely given, specific, informed and unambiguous*' and be given either '***by a statement or by a clear affirmative action***'.

Where '*special categories of personal data*' (which is in general terms '*sensitive personal data*' under the DPA, minus data in relation to offences and criminal convictions, plus the new categories of genetic and biometric data) is Processed, consent must be *'explicit'*. Where Processing is based on consent the burden of proof for demonstrating that consent has been given by the Data Subject lies with the Data Controller. Data Subjects also have the right to withdraw consent at any time and must be informed of this right prior to the giving of consent.

Although consent can be achieved though ticking a box when visiting a website, choosing certain technical settings or by any other statement or conduct that clearly indicates acceptance of the proposed data Processing, silence, pre-ticked boxes or inactivity are insufficient.

Consent will also not be regarded as freely-given if the Data Subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment. For example, consent will be not be deemed freely given where entering into a contract, or receiving a service is 'tied' to the Data Subject giving consent to the Processing of their data which is not necessary for the performance of the contract.

Where online services (e.g. email accounts and social media accounts) are offered directly to children, parental consent is required for the Processing of Personal Data relating to such services where the child is below 16 years of age, unless individual Member States legislate for a lower age limit, which may not be below 13 years of age. The position is therefore that children over 16 are always able to give consent to data Processing for online services themselves, whereas children under 13 can never give such consent, and for ages in between, Member States have discretion to decide.

Preparation for implementation: The new provisions on consent will mean that, in practice, consent is much more difficult to obtain. With the introduction of the new requirement for consent to be '*unambiguous*', organisations which currently rely on implied consent for data Processing activities should review and adapt their existing practices as it is now clear that mere acquiescence (for example failing to un-tick a ticked box) does not constitute valid consent.

Data subject rights

Data Subjects have various rights under the DPA that have essentially been retained under the GDPR. Further rights have been introduced by the GDPR.

Under the DPA individuals have rights to:

— receive certain information (see Privacy Notices/ Consent sections on pages 10-11);

— access Personal Data (known as a '*Subject Access Request*');

— prevent Processing likely to cause damage or distress;

— prevent Processing for the purposes of direct marketing;

— object to automated decision-taking;

— obtain compensation for damage/distress; and

— obtain a court order for the rectification, blocking, erasure and/or destruction of inaccurate Personal Data.

In general terms, all of these rights have been translated across to the GDPR, but many are also enhanced by the new law, for example:

— there is a standalone '*right to erasure*' which applies in a wider range of circumstances and without the need for the individual to obtain a court order;

— individuals have broader rights to restrict the Processing of their Personal Data; and

— individuals are entitled to receive more information via a Subject Access Request without having to pay a fee, unless the request is '*manifestly unfounded or excessive*'.

The GDPR also sets out a new '*right to data portability*', which in limited circumstances gives the individual a right to receive from the Data Controller his/her Personal Data, in a '*structured, commonly used and machine-readable format*' and '*where technically feasible*' he or she may require that it be transferred to another Data Controller.

Preparation for implementation: As the GDPR will build on existing rights that individuals already have under the DPA, in order to prepare for the changes that will take place, organisations should first check their existing procedures to ensure that they are adequate to address all current rights. The next steps should be to consider the enhancements to these rights that will come into effect under the GDPR and look at formats in which Personal Data should be provided to individuals, in order to comply with the new right to data portability.

Data breach reporting

Under the Directive there is no mandatory obligation on Data Controllers to report data breaches to their national data protection authority or to inform Data Subjects affected by the breach, although specific notification requirements do exist in some sectors. The GDPR introduces a system of mandatory notification for data breaches.

In the absence of a mandatory notification requirement, under the Directive, Member States have developed their own practices and in the UK the view of the ICO is that 'serious' data breaches should be brought to its attention.

The GDPR introduces a system of mandatory notification for data breaches, and Data Controllers will be required to notify Personal Data breaches to Supervisory Authorities without undue delay and, where feasible, no later than 72 hours of becoming aware of the breach. Set categories of information must be provided in the notification. However, there will be a materiality threshold whereby notification to Supervisory Authorities is not required where the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Data Controllers must also communicate data breaches to Data Subjects without undue delay, although, this is only required where the breach is likely to result in a high risk to the rights and freedoms of individuals. However, no such communication is required where measures have been taken to render the data unintelligible, or subsequent measures have been taken by the Data Controller to ensure that the risk to the rights and freedoms of the Data Subjects is no longer likely to materialise. A public communication may be used if notification to individual Data Subjects would involve disproportionate effort.

Preparation for implementation: Organisations will need to develop, test and implement data breach and crisis response plans which take these new notification requirements into account. They should have a clear view of privacy governance, with defined lines of responsibility, and ensure that they have agile processes in place to guarantee compliance.

Data protection officers

Compared with the DPA, the GDPR introduces new requirements in relation to data protection officers ('**DPOs**'). The DPA does not require any organisation to appoint a DPO. However, some Data Controllers, and some Data Processors too, will need to appoint one under the GDPR.

This requirement applies to:

- public authorities or bodies (except courts acting in their judicial capacity);
- those required to appoint a DPO under national law; and
- other Data Controllers and Data Processors with core activities involving either:
  - the regular, systematic and large scale monitoring of individuals (e.g. through CCTV recording, employee email access, or use of vehicle telemetry devices); or
  - the large scale processing of '*special categories of data*' and/or '*personal data relating to criminal convictions and offences*' (which is in general terms '*sensitive personal data*' under the DPA, plus the new categories of genetic and biometric data).

A DPO's tasks will include advising colleagues and monitoring their organisation's data protection compliance, providing training, running audits, advising on privacy impact assessments and dealing with Supervisory Authorities.

Preparation for implementation: In order for any organisations that will be affected by this change to prepare for its implementation, they could appoint a DPO now, and provide this person with training and support to ensure that they will be able to fulfil their role effectively when the GDPR comes into effect.

International transfers of personal data

Under the DPA, Personal Data should not be transferred to a country outside the European Economic Area (EEA) unless there is an '*adequate level of protection*' or an exemption applies. The onus for compliance rests on the Data Controller. Under the GDPR the same transfer restriction applies, not only to Data Controllers, but also to Data Processors.

Existing methods of ensuring an adequate level of protection and the exemptions are broadly unchanged under the GDPR.

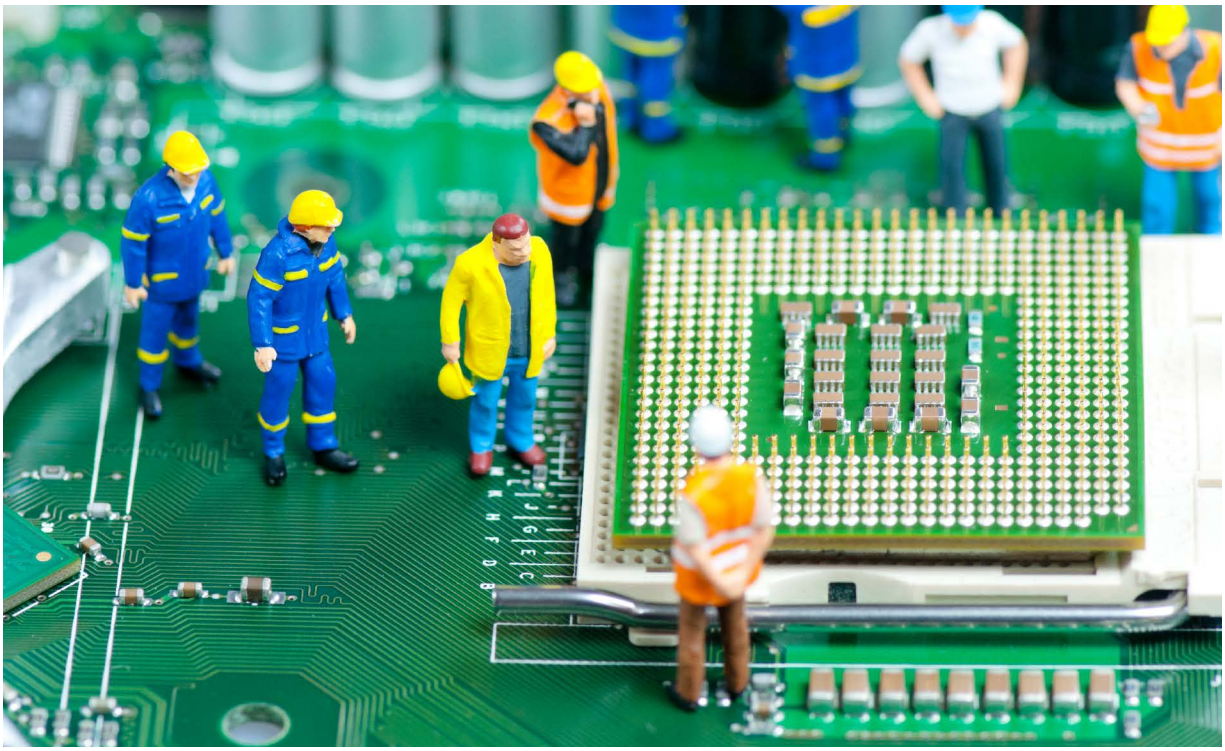
BCRs are expressly provided for in the GDPR, unlike under the Directive and the DPA. Their use is extended beyond transfers between group members to also include groups of *'enterprises engaged in a joint economic activity'*. The relevant Supervisory Authority in each EU Member State from which Personal Data is to be transferred will still need to approve the BCRs under the GDPR, but this will be subject to the *'consistency mechanism'* set out in the GDPR, which is designed to contribute to the consistent application of the GDPR. As a result it should be easier to obtain approvals from the relevant Supervisory Authorities. If the relevant requirements as set out in the GDPR are met, the approval should be granted. Additional requirements, that currently apply in certain Member States, should not continue following the application of the GDPR.

Self-assessment by the Data Controller as to whether a transfer ensures an adequate level of protection is currently a possibility in the UK. That will no longer be the case under the GDPR except in limited circumstances.

The GDPR introduces the possibility of transfers being made where there is an approved code of conduct or certification mechanism (these are provided for in the GDPR for the purpose of demonstrating compliance with the GDPR), together with binding and enforceable commitments of the Data Controller or the Data Processor that is outside the EEA to apply appropriate safeguards.

Preparation for implementation: Organisations should identify the international transfers of Personal Data that they make and ensure that the transfers will be lawful under the GDPR. Given the greater ease in which it should be possible to put in place BCRs, organisations that have until now been hesitant as to putting these in place may wish to look further into this as a mechanism for compliance in relation to intra-group transfers.

Data protection by design and default, impact assessments, anonymisation and pseudonymisation



The GDPR introduces a number of measures into law that are currently recognised as recommended approaches.

Data Protection by Design and Default
The GDPR requires Data Controllers to implement appropriate technical and organisational measures that are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into Processing in order to meet the requirements of the GDPR. In determining what would be '*appropriate*', the Data Controller should take into account, amongst other things, the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, and the risks posed by the Processing in question.

In addition, Data Controllers must implement measures to ensure that, by default, only Personal Data that are necessary for the specific purpose of the Processing are indeed Processed. This involves the restriction of Personal Data collected, the period of storage of the Personal Data and their access.

The appropriate measures to be implemented may be decided upon following the performance of an impact assessment and may involve the anonymisation or pseudonymisation of Personal Data.

Impact Assessments
The GDPR places an obligation on Data Controllers to perform an impact assessment where, taking into account the nature, scope, context and purposes of the Processing, is likely a high risk to the rights and freedoms of individuals. The impact assessment should be performed prior to such Processing and contain, as a minimum, a description of the envisaged Processing operations and the purposes of the Processing, an assessment of the necessity and proportionality of the Processing operations in relation to the purposes, an assessment of the risks and the measures envisaged to address the risks.

The GDPR sets out particular circumstances when impact assessments should be used and that each Supervisory Authority should publish a list of the kind of Processing that would require the production of an impact assessment.

Anonymisation and Pseudonymisation
Anonymous data (i.e. data that does not relate to an identified or identifiable person) does not fall within the scope of the GDPR. The GDPR contains the concept of 'pseudonymisation', which involves the Processing of Personal Data in such a way that the Personal Data can no longer be attributed to a specific person without the use of some other information that is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable person. Pseudonymisation of data is given in the GDPR as an example of a measure that may help to satisfy the requirement for appropriate technical and organisational security measures to be in place.

Preparation for implementation: Organisations should identify whether the Processing that they undertake is of the sort that would necessitate an impact assessment being performed. They should keep an eye on communications from the Supervisory Authority for the list setting out the kinds of Processing that would require the production of an impact assessment. Organisations should consider ways in which anonymisation and pseudonymisation of Personal Data could be utilised in their businesses to reduce the level of risk in their Processing activities. Where an organisation plans to undertake some new Processing, for example on the installation of new technology, it should build in data protection compliance measures as part of its planning around that Processing.

Accountability

The GDPR introduces several new accountability requirements, which are not included in the DPA or the Directive. These are designed to ensure that organisations comply with the GDPR in practice and that they are able to demonstrate their compliance when required.

Under current data protection law, Data Controllers in all EU Member States must, subject to some limited exemptions, notify the relevant national data protection authority of their Processing activities. In the UK, most Data Controllers are required to submit a notification to the ICO, which must be renewed on an annual basis. The GDPR abolishes current notification requirements, but instead both Data Controllers and Data Processors will be required to keep relatively detailed records of their Processing activities and make these available to Supervisory Authorities on request. There is an exemption for enterprises or organisations that employ fewer than 250 persons unless the Processing is high risk, not occasional, or includes *'special categories of data'* and/or Personal Data relating to criminal convictions and offences (which is, in general terms, the equivalent of sensitive personal data under the DPA plus the new categories of genetic and biometric data).

There is also a new general requirement under the GDPR for Data Controllers to be able to demonstrate that their Processing activities are performed in accordance with the requirements of the GDPR. Where proportionate, this shall include the implementation of appropriate policies. Adherence to published codes of conduct/approved certification mechanisms are also referenced as ways of demonstrating compliance.

In addition, accountability under the GDPR is reinforced by requirements in relation to the appointment of Data Protection Officers (see page 14), as well as obligations relating to privacy by design (see page 16) and the conduct of impact assessments (see page 17).

Preparation for implementation: In order to prepare for new accountability measures in the GDPR, organisations can start now to develop a system for documenting Processing activities as they arise and for updating these records when the Processing changes. They can also take note of any codes of conduct that may be published by the ICO or any relevant overseas data protection authority.

Data Processor responsibilities

The Directive and the DPA place direct obligations on Data Controllers, but not on Data Processors. The GDPR will bring about significant changes as Data Processors will have direct legal responsibilities under the new law.

Under the DPA, in the event of a breach, it is generally the Data Controller that is subject to enforcement action (Data Processors may be exposed under the contractual arrangements with the Data Controllers). Under the GDPR, Data Processors may have direct legal responsibilities and they will also be exposed to enforcement action, including substantial administrative fines (see Fines/ Enforcement section at page 8) in the event of a breach.

For example, under the GDPR (subject to some exceptions) Data Processors will, for the first time, be directly required to:

- keep records of Processing activities;
- appoint a Data Protection Officer;
- obtain consent from the Data Controller before engaging a sub-contractor for Processing;
- tell the Data Controller if there is a data breach;
- put in place appropriate technical and organisational measures;
- cooperate with the relevant Supervisory Authority;
- comply with the GDPR's rules on overseas data transfers; and
- carry out data privacy impact assessments.

The GDPR also imposes more detailed requirements in relation to the contractual obligations that Data Controllers must impose on Data Processors. For example, under the GDPR, the Processing agreement between Data Controller and Data Processor must contain requirements for the Data Processor to: (a) ensure ensure that persons Processing Personal Data are subject to confidentially obligations; (b) return to the Data Controller or delete Personal Data once services have ended; and (c) allow for audits and inspections by or on behalf of, the Data Controller.

Preparation for implementation: In preparation for these changes, Data Controllers and Data Processors will need to re-visit and re-negotiate any current data Processing agreements. Organisations may also want to consider updating any existing template data Processing agreements which they have in place. Furthermore, Data Processors will need to familiarise themselves with the new obligations imposed by the GDPR and look at practical ways in which they can achieve compliance with these rules.

Regulators

Under the current Directive each EU Member State is required to have one or more supervisory authority/(ies), responsible within its territory, for monitoring the laws adopted pursuant to the Directive. The GDPR similarly requires that each Member State shall have one or more 'Supervisory Authority/ies' responsible for exercising powers given to it in the GDPR.

In the UK, there is one regulator dedicated to enforcing the DPA: the ICO (although the Financial Conduct Authority also has jurisdiction to set rules and fine the firms that it regulates for breaches of data security, and other sector-specific regulators may also set rules relating to the handling of personal information).

The GDPR similarly requires that each Member State shall have one or more 'Supervisory Authority/ies' responsible for exercising powers given to it in the GDPR.

Unlike the current Directive, the GDPR also makes provision for what is known as a 'one-stop shop' mechanism. Multinational organisations (both Data Controllers and Data Processors), which are established in more than one Member State, will be primarily regulated by a 'lead authority' in the Member State where they have their 'main establishment'. The lead authority will generally have jurisdiction over the multinational's cross-border Processing activities. However, the GDPR also contains a procedure for cooperation between the lead authority and other Supervisory Authorities where Processing takes place outside of the lead authority's territory only, or 'substantially affects' data subjects only in another Member State. Supervisory Authorities are also able to work together to conduct joint investigations and impose joint enforcement measures.

In addition, the GDPR also provides for the establishment of a 'European Data Protection Board' to include the head of one Supervisory Authority from each Member State. Under the GDPR any Supervisory Authority can ask the European Data Protection Board for an opinion on a matter concerning more than one Member State. The European Data Protection Board also has dispute resolution powers and may, in the case of a '*relevant and reasoned objection*' from a Supervisory Authority, make a binding decision overriding the opinion of the lead authority.

Preparation for implementation: At this stage, multinational organisations can give some thought as to where they have their main establishment so that they can keep up to date with publications released by the relevant data protection regulator in that place which is in 2018 likely to become their lead authority.

Glossary

BCRs: means binding corporate rules, being Personal Data protection policies which are adhered to by a Data Controller or Data Processor established in a Member State for transfers or a set of transfers of Personal Data to a Data Controller or Data Processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Data Controller: means the natural or legal person who alone, or jointly with others, determines the purposes and means of the processing of Personal Data.

Data Processor: means the natural or legal person who Processes Personal Data on behalf of the Data Controller.

Data Subject: means an identified or identifiable natural person.

Directive: means the Data Protection Directive *(95/46/EC)*.

DPA: means the Data Protection Act 1998.

GDPR: means the General Data Protection Regulation.

ICO: means the Information Commissioner's Office.

Personal Data: means any information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of the Data Subject.

Processing: means any operation/set of operations which is performed on Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and '**Process**' and '**Processed**' shall be construed accordingly.

Supervisory Authority: means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR to be, amongst other things, responsible for monitoring the application of the GDPR.

Appendix: administrative fines

Factors to be taken into account when deciding upon the amount of the fine *(Article 83(2))*

Factors	Action points
The nature, gravity and duration of the infringement (taking into account the nature, scope or purpose of the Processing concerned as well as the number of Data Subjects affected and the level of damage suffered by them).	— Conduct regular audits to identify potential risk areas and implement effective solutions — Be proactive – remember, prevention is always better than damage control
The intentional or negligent character of the infringement.	— Develop and implement clear internal policies on data privacy, and follow up with training and compliance checks — Define privacy governance processes and allocate responsibility for compliance to relevant stakeholders – ensure that privacy is on the agenda in the boardroom
Any action taken by the Data Controller or Data Processor to mitigate the damage suffered by Data Subjects.	— Act fast to contain actual infringements and to prevent potential infringements
The degree of responsibility of the Data Controller or Data Processor, taking into account the technical and organisational measures implemented by them pursuant to privacy by design and by default *(Articles 25)* and security of Processing *(Article 32)*.	— Ensure Processing contracts clearly allocate areas of responsibility and liability as between the Data Controller and Data Processor
Any relevant previous infringements by the Data Controller or Data Processor.	— Take steps to ensure that that any infringements are swiftly dealt with and do not become a recurring theme
The degree of cooperation with the Supervisory Authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement.	— Be cooperative and responsive when dealing the Supervisory Authority – do not delay in addressing infringements and mitigating their effects — Come prepared with suggested solutions regarding infringements – the interests of the Data Subject should be front and centre in these — Employ a 'front foot' approach to the organisation's relationship with the Supervisory Authority
The categories of Personal Data affected by the infringement.	— Ensure that additional protections are in place for special categories of data/ higher risk processing
The manner in which the infringement became known to the Supervisory Authority and whether the Data Controller or Data Processor notified the Supervisory Authority of the infringement.	— Notify data breaches to the Supervisory Authority as early as possible – and provide updates as further information comes to hand
Compliance with prior enforcement action brought by a Supervisory Authority *(Article 58(2))* concerned with the same subject-matter.	— Take steps to address all concerns raised by the Supervisory Authority in any previous enforcement action and ensure that it does not happen again – be able to demonstrate that significant efforts have been made to comply
Adherence to approved codes of conduct *(Article 40)* or approved certification mechanisms *(Article 42)*.	— Keep an eye out for approved codes and certification mechanisms from the Supervisory Authority
Any other aggravating or mitigating factor applicable to the circumstances of the case, e.g. financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	— Carefully weigh up the risks of non-compliance — Ensure that the technical and organisational measures you have in place are as robust, yet agile, as they can be

Tier 1 Breaches **Up to €20 million or 4% of the total worldwide annual turnover (whichever is greater)*†**
Failure to comply with the principles relating to Processing of Personal Data; lawfulness; conditions for consent; and Processing special categories of Personal Data *(Articles 5, 6, 7 and 9)*
Failure to give effect to certain rights of Data Subjects *(Articles 12-22)*
Transfer of Personal Data to third countries or international organisations without ensuring an adequate level of protection or applying an exemption *(Articles 44-49)*
Failure to comply with Member State laws adopted for specific Processing situations (including freedom of expression; in the context of employment; public access to official documents; archiving purposes in the public interest, scientific or historical research or statistical purposes; and obligations of secrecy) *(Chapter IX)*
Non-compliance with Supervisory Authority corrective and/or investigative powers *(Article 58(2) and Article 58(1))*

Tier 2 Breaches **Up to €10 million or up to 2% of the total worldwide annual turnover (whichever is greater)*†**
Failures in relation to consent for the Processing of children's Personal Data (*Article 8*)
Failure to give effect to certain of a Data Subject's rights where the Data Controller is able to identify the Data Subject (having been given the additional information to identify the same) *(Article 11)*
Failure to implement technical and organisational measures to ensure data protection by design and default *(Article 25)*
Failure by joint Data Controllers in being transparent in relation to their respective compliance obligations *(Article 26)*
Failure by non EU Data Controllers and Data Processors to designate appropriate representatives in the EU *(Article 27)*
Failure by Data Controllers to only use Data Processors who provide sufficient guarantees to implement appropriate technical and organisational measures to ensure compliance with the GDPR; and/or other requirements on Data Controllers in relation to their engagement of Data Processors *(Article 28)* Subcontracting of Processing by Data Processors without the prior written consent of the Data Controller (*Article 28*)
Failure of Data Processors to only Process Personal Data on the instructions of the Data Controller *(Article 29)*
Failures by Data Controllers and Data Processors in relation to obligations of Processing record keeping *(Article 30)*
Failure by Data Controllers and Data Processors to cooperate with the Supervisory Authority *(Article 31)*
Failure by Data Controllers and Data Processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk *(Article 32)*
Failures in relation to the notification of a Personal Data breach to the Supervisory Authority *(Article 33)*
Failures by a Data Controller in relation to the communication of a Personal Data breach to Data Subjects *(Article 34)*
Failures by a Data Controller in relation to data protection impact assessments or, where necessary, to consult with the Supervisory Authority prior to Processing *(Articles 35-36)*
Failure by a Data Controller or Data Processor to appropriately appoint a data protection officer where required *(Articles 37-39)*
Where a Data Controller or Data Processor relies on certification for compliance but fails to comply with the relevant obligations *(Article 42)*
Failure by a certification body to carry out its required duties *(Article 43)*
A body accredited to monitor compliance with a code of conduct fails to take appropriate action in cases of infringement of such code by a Data Controller or Data Processor *(Article 41(4))*

* Member States may impose rules on criminal sanctions for infringements of the GDPR too and may also allow for the deprivation of the profits gained from non-compliance with the GDPR. However, this action would be instead of, not in addition to, any administrative fine or other penalty *(Recital 149)*

† Where administrative fines are imposed on persons that are not an undertaking (i.e. an organisation not engaged in economic activity such as a public authority), the Supervisory Authority should take into account the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. Member States will determine whether and to what extent public authorities should be subject to administrative fines *(Recital 150)*

Contacts

ALBANIA

Marco Lacaita
E marco.lacaita@cms-aacs.com
T +355 4 430 2123

ALGERIA

Amine Sator
E amine.sator@cms-bfl.com
T +213 (7)21 69 3234

ARGENTINA

Ted Rhodes
E ted.rhodes@cms-cmck.com
T +55 21 3722 9831

AUSTRIA

Dr. Johannes Juranek
E johannes.juranek@cms-rrh.com
T +43 1 40 443 2450

BELGIUM

Tom De Cordier
E tom.decordier@cms-db.com
T +32 2 743 6913

BOSNIA AND HERZEGOVINA

Nedžida Salihović-Whalen
E nedzida.salihovic-whalen@cms-rrh.com
T +387 33 296 408

BRAZIL

Ted Rhodes
E ted.rhodes@cms-cmck.com
T +55 21 3722 9831

BULGARIA

Nevena Radlova
E nevena.radlova@cms-cmck.com
T +359 2 923 4866

CHINA

Nick Beckett
E nick.beckett@cms-cmck.com
T +86 10 8527 0287

CROATIA

Dr. Gregor Famira
E gregor.famira@cms-rrh.com
T +385 1 482 5602

CZECH REPUBLIC

Tomas Matejovsky
E tomas.matejovsky@cms-cmck.com
T +420 296 798 852

FRANCE

Anne-Laure Villedieu
E anne-laure.villedieu@cms-bfl.com
T +33 1 4738 4019

GERMANY

Christian Runte
E christian.runte@cms-hs.com
T +49 89 2380 7163

Michael Kamps
E michael.kamps@cms-hs.com
T +49 221 771 6270

Reemt Matthiesen
E reemt.matthiesen@cms-hs.com
T +49 89 23807 248

HUNGARY

Dora Petranyi
E dora.petranyi@cms-cmck.com
T +36 (06) 1 483 4820

ITALY

Fabrizio Spagnolo
E fabrizio.spagnolo@cms-aacs.com
T +39 06 478 151

LUXEMBOURG

Julien Leclere
E julien.leclere@cms-dblux.com
T +352 26 27 531

MEXICO

Derek Woodhouse
E dwoodhouse@wll.com.mx
T +52 (55) 2623.0552

MONTENEGRO

Radivoje Petrikić
E radivoje.petrikic@cms-rrh.com
T +381 11 320 8900

MOROCCO

Marc Veuillot
E marc.veuillot@cms-bfl.com
T +212 6 6108 9182

NETHERLANDS

Hendrik Struick
E hendrik.struik@cms-dsb.com
T +31 30 212 1726

OMAN

Ben Ewing
E benjamin.ewing@cms-cmck.com
T +938 2204 1199

POLAND

Tomasz Koryzma
E tomasz.koryzma@cms-cmck.com
T +48 22 520 8479

Marcin Lewoszewski
E marcin.lewoszewski@cms-cmck.com
T +48 22 520 5525

PORTUGAL

José Luís Arnaut
E joseluis.arnaut@cms-rpa.com
T +351 21 095 8133

ROMANIA

Marius Petroiu
E marius.petroiu@cms-cmck.com
T +40 21 407 3889

RUSSIA

Maxim Boulba
E maxim.boulba@cmslegal.ru
T +7 495 786 4023

SERBIA

Radivoje Petrikic
E radivoje.petrikic@cms-rrh.com
T +381 11 320 8900

SLOVAKIA

Hana Supeková
E hana.supekova@rc-cms.sk
T +421 2 3233 3444

Ian Parker
E ian.parker@cms-cmck.com
T +421 2 3233 3498

SLOVENIA

Luka Fabiani
E luka.fabiani@cms-rrh.com
T +396 1 620 5210

SPAIN

Blanca Cortes Fernandes
E blanca.cortes@cms-asl.com
T +34 91 451 9300

SWITZERLAND

Dr Robert G. Briner
E robert.briner@cms-veh.com
T +41 44 285 1111

TURKEY

John Fitzpatrick
E john.fitzpatrick@cms-cmck.com
T +44 7515 787 228

UKRAINE

Olexander Martinenko
E olexander.martinenko@cms-cmck.com
T +380 44 391 3704

Olga Belyakova
E olga.belyakova@cms-cmck.com
T +380 44 391 3377

UK

John Armstrong
E john.armstrong@cms-cmck.com
T +44 20 7367 2701

Emma Burnett
E emma.burnett@cms-cmck.com
T +44 20 7367 3565

Alan Nelson
E alan.nelson@cms-cmck.com
T +44 141 304 6006

Tom Scourfield
E tom.scourfield@cms-cmck.com
T +44 20 7367 2707

Ian Stevens
E ian.stevens@cms-cmck.com
T +44 20 7367 2597

Duncan Turner
E duncan.turner@cms-cmck.com
T +44 131 200 7669

Jennifer Barr
E jennifer.barr@cms-cmck.com
T +44 141 304 6233

UNITED ARAB EMIRATES

Matthew Culver
E matthew.culver@cms-cmck.com
T +971 4 350 7099


Aberdeen
Glasgow
Edinburgh
Mexico City
Hamburg
Amsterdam
Berlin
London
Utrecht
Duesseldorf
Leipzig
Bristol
Antwerp
Cologne
Brussels
Frankfurt
Luxembourg
Paris
Stuttgart
Strasbourg
Munich
Zurich
Geneva
Ljubljana
Lyon
Milan
Rome
Barcelona
Madrid
Lisbon
Seville
Algiers
Rio de Janeiro
Casablanca


Moscow
Warsaw
Kyiv
Bratislava
Budapest
Zagreb
Belgrade
Bucharest
Sarajevo
Sofia
Podgorica
Tirana
Istanbul
Beijing
Shanghai
Hong Kong
Tehran
Dubai
Muscat

1605-0211-23 (Scot)