



**GDPR Team**  
01244 354 815  
alison.brennan@dtmlegal.com

---


Alison Brennan  
Partner



Edward Barnes  
Head of Corporate and  
Commercial



Alison Brennan  
Partner



Fredrica Reid  
Solicitor

### **What organisations will be affected?**

The GDPR expands the territorial reach of the current Directive. It applies to any organisation established in the EU that processes personal data, even if the processing itself takes place outside the EU. Organisations without an establishment in the EU will also be caught by the GDPR if they process personal data of EU data subjects relating to goods or services offered to EU data subjects, or the monitoring of their behaviour.

A significant change introduced by the GDPR is its application to “data processors”. A data processor is any person, public authority, agency or other body who processes the data on behalf of the data controller. Data processors will, for the first time, have a direct obligation to data subjects at EU wide level. This means that data subjects will be able to enforce their rights directly against data processors under enforcement regimes. This exposes the non-compliant data processor to sanctions, including potentially hefty fines from supervisory authorities, which in the UK is the Information Commissioner’s Office (“ICO”). This change is particularly significant for organisations engaged in cloud computing services that currently have few direct responsibilities to data subjects.

### **Changes to the definition of personal data**

#### **Personal Data**

Under the current Directive, the definition of personal data covers any information relating to an identified or identifiable natural person. The GDPR has widened this definition to include name,

location data, online identifiers and factors specific to a person's genetic identity. The inclusion of online identifiers is a key change and will result in information such as IP addresses and cookies falling within the scope of the GDPR.

### **Sensitive Data**

The scope of "sensitive data" is expanded under the GDPR to the processing of information revealing ethnic origin, political opinions, trade union membership, genetic or biometric data or information which concerns a person's health or sexuality. Organisations that process sensitive data have heightened obligations under the GDPR and explicit consent must be obtained. It is worth noting that there are some exceptions under the regulations such as there being a substantial public interest and processing in the course of legal proceedings.

### **Data Protection Principles**

The "data protection principles" underpin the current Directive and govern how personal data may be processed. The principles contained in the GDPR are similar to those contained in the Directive, albeit with some notable additions:

- **Accountability** – the GDPR introduces a new concept of accountability which requires data controllers to be able to demonstrate how they have complied with the data protection principles. This requirement shifts the burden of proof on to the data controller in the event of a compliance investigation. Organisations should ensure that they have adequate record keeping and procedures in place. Accountability is reinforced by the increased sanctions introduced by the GDPR, including fines up to the greater of 4% of a company's annual revenue or €20 million, whichever is higher.
- **Lawfulness, fairness and transparency** - the inclusion of the principle of *transparency* is a new provision in the GDPR. Businesses should ensure that their privacy notices are sufficiently detailed so data subjects can provide informed consent.
- **Purpose Limitation** – Personal data must be collected for "specified, explicit and legitimate purposes". This is similar to the controls placed on data controllers under the current Directive. However, it also permits further processing for public interest or scientific purposes, widening the scope for further processing.
- **Data Minimisation** – the data collected must be adequate and relevant. Whilst this principle appears in both the Directive and the GDPR, it is more stringent in the latter. In particular, collection of personal data should be limited to "*what is necessary*". Organisations should review practices to determine whether any of the processing is unnecessary for the purpose they are trying to achieve.
- **Accuracy** - Under the current Directive data held should be accurate and, where necessary, kept up to date. The GDPR extends this so that organisations must take "reasonable steps" to ensure that inaccurate data is erased or rectified without delay. To deal with this, organisations should consider how frequently they review and update the data they hold.
- **Integrity and Confidentiality** – the GDPR requires organisations processing personal data to ensure appropriate security measures are implemented and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

- **Storage Limitation** – GDPR introduces specific exceptions to the principle that data should not be kept longer than is necessary. In particular, data may be stored for longer periods if it relates to scientific or historical research or statistical purposes, or archiving purposes in the public interest, provided appropriate technical and organisational measures are implemented.

**Consent of data subjects will be harder to obtain**

Organisations must be able to demonstrate that the data subject gave their consent to the processing and will bear the burden of proof that consent was validly obtained. The GDPR requires a very high standard of consent, which must be given by a clear affirmative action establishing a *freely given, specific, informed and unambiguous indication* of the individual's agreement to their personal data being processed.

**Freely Given** – data subjects must not be unable to refuse or withdraw consent without detriment.

**Specific** - when the processing has multiple purposes, the data subject should give their consent to each of the processing purposes.

**Informed** – the identity of the data controller and the purpose of the processing for which the data is intended must be clear and transparent.

**Unambiguous** - clear action which indicates affirmative agreement, for example, ticking a blank box. Mere acquiescence, such as failing to un-tick a pre-ticked box, does not constitute valid consent under the GDPR.

Organisations and in particular e-commerce services, will need to carefully review their existing practices and privacy notices. Policies should be sufficiently detailed so that informed consent is achieved and individuals must be notified of their right to withdraw their consent at any time.

**Use of Children’s data**

The GDPR introduces for the first time a number of specific requirements relating to the processing of children’s personal data.

Where services are offered directly to children under the age of 16, such as online services and apps, parental consent must be obtained. Member states have the option to specify a limit below 16 years provided that the age restriction does not fall below 13. Data controllers must be able to demonstrate that reasonable efforts have been made to verify that consent has been given by a parent or guardian. This, in practice, may be difficult to achieve and specific verification measures should be used.

The GDPR introduces additional rights for data subjects and strengthens the existing concepts of rectification, erasure and restriction of processing that exist under the current Directive.	
<b>Rectification</b>	data subjects are entitled to have inaccurate personal data rectified without undue delay. Organisations should ensure that data is stored in an accessible and editable format so that such requests can be dealt with swiftly.
<b>Right to be</b>	under the current Directive data subjects have a right to erasure where data is

<b>forgotten</b>	<p>processed in breach of the data protection principles. The GDPR extends this right to when data is no longer necessary for the purpose for which it was obtained, consent has been withdrawn, there are no legitimate grounds for processing or where data is unlawfully processed.</p> <p>Organisations will be in breach of the GDPR (and liable to sanction) for failing to comply with an erasure request. Achieving erasure could be difficult in practice, particularly if information is transferred to third parties.</p>
<b>Restriction of Processing</b>	as an alternative to erasure, data subjects are entitled to restrict processing of their personal data. This right is available where there is a question as to the accuracy of the personal data, processing is unlawful, the controller no longer needs the data or there is an objection pending the verification.
<b>Data Portability</b>	this is a new concept introduced by the GDPR which enables data subjects to receive and transmit data from one service provider to another. The personal data should be in a machine-readable format (such as a download) which can easily be transferred. It is important to note that the original data controller may have continued obligations towards the data subject, such as erasure or subject access requests.
<b>Right to object to data processing</b>	this is not a new concept, however it is extended by the GDPR. Whilst there is no general right to object, the GDPR lists instances in which a data subjects will given such right. This includes processing for direct marketing and for scientific, historical or statistical research purposes.
<b>Automated processing</b>	<p>the GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. This includes profiling which is a form of automated decision making. This right does not exist where the processing is:</p> <ol style="list-style-type: none"> <li>1. necessary for entering into or performance of a contract between you and the individual;</li> <li>2. authorised by law (eg for the purposes of fraud or tax evasion prevention); or</li> <li>3. based on explicit consent.</li> </ol> <p>Data controllers must ensure that processing is fair and transparent by providing meaningful information about the logic involved. Appropriate mathematical or statistical procedures should be used for the profiling.</p>
<b>Notifying third parties regarding rectification, erasure or restriction</b>	where a controller has transferred data to third parties, and the data subject has subsequently exercised any of the rights of rectification, erasure or restriction, the controller must notify those third parties of the data subject's exercising of those rights. The data subject is also entitled to request information about the identities of those third parties. Organisations that disclose data to third parties on a large scale may find this obligation particularly burdensome.

### Increased Accountability

A key aim of the GDPR is to increase the accountability of controllers and processors. This can be seen in a number of new requirements (discussed in more detail below) such as the need to maintain documentation recording processing activities, data protection impact assessments for

risky data processing and the new concept of “privacy by design and default”. In order to prepare for the enhanced accountability, data controllers and processors should:

1. Review their existing compliance programmes, and ensure that those programmes are updated and expanded as necessary to comply with the GDPR.
2. Ensure that they have clear records of all of their data processing activities (so that such records are available to be provided to a relevant authority on request).
3. Appoint a Data Protection Officer.

## **Risk, Compliance and Security**

### **Risk based approach**

Data security plays a prominent role in the GDPR and introduces a number of preventative and reactive measures in relation to data protection breaches. The GDPR adopts a risk-based approach to compliance and the notion of “risk” is a key concept of the GDPR. Data controllers are encouraged to implement protective measures corresponding to the level of risk of their data processing activities. The GDPR imposes heightened requirements on controllers that engage in “high risk” activities. The guidance suggests that “high risk” activities are those that are likely to result in a risk to the rights and freedoms of the data subjects. Three examples are provided:

1. Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect the individual.
2. Processing on a large scale of special categories of data.
3. Systematic monitoring of a publicly accessible area on a large scale.

Organisations bear responsibility for assessing the degree of risk that their processing activities. Low-risk processing activities may face a reduced compliance burden.

### **Privacy by design and default**

This is a new concept requiring organisations to build consideration of privacy into their product and service design processes in certain circumstances.

**Privacy by design** requires data controllers to implement appropriate technical and organisational measures to enhance safeguards. Data controllers should consider using encryption technologies or use of pseudonyms to make the data subject harder to identify.

**Privacy by default** requires data controllers to implement technological and organisational measures to ensure that only personal data which is necessary for the specific purpose is processed. Data controllers should review the amount of data collected, the extent of processing, the period of storage and the accessibility of the data.

### **Privacy Impact Assessments (PIAs)**

A PIA is a process to help organisations identify, assess and mitigate or minimise privacy risks with data processing activities. This is by no means a new concept and has been encouraged by the ICO for some time. Under the GDPR, PIAs are mandatory where the processing activity is likely to result

in a high risk to data subjects. This closely linked to the new concept of privacy by design and default and also plays a key component in the accountability principle, helping organisations demonstrate compliance with the GDPR.

The PIA should consider whether processing is necessary and proportionate and include measured plans to address the risks including safeguards and security measures. Organisations which process large-scale personal data should ensure that engineers and compliance teams complete PIA questionnaires so that an informed assessment can be made. Importantly, where processing will result in a high risk, data controllers are required to consult with the ICO.

### **Data Protection Officers**

The GDPR introduces a requirement for both data controllers and processors to appoint a Data Protection Officer (“DPO”) where:

1. processing is carried out by a public authority;
2. where the core activities of the processor consist of regular systematic monitoring on a large scale; or
3. where processing relates to special categories of data or relate to criminal convictions.

If an organisation appoints a DPO (regardless of whether they are obliged to) they must ensure that they have sufficient staff and skills to discharge their obligations under the GDPR. DPOs have a statutory responsibility to advise organisations and their employees on the law, monitor compliance and report to senior management. Moreover, organisations must ensure that a DPO is sufficiently resourced to fulfil their role. Careful consideration should be given to these responsibilities before voluntarily appointing a DPO.

### **Notification Procedure**

Data processors are required to notify controllers of a data breach without undue delay. A controller has a corresponding duty to the data subject where the breach is likely to present a high risk to the rights and freedoms of natural persons. The GDPR does not define “high risk” so the onus is on the organisation to determine and be able to demonstrate (under the accountability principle) what and why they did or did not consider the breached data a “high risk”. Notification will not be required where:

1. the data controller has implemented security measures which render the personal data intelligible for example using encryption; or
2. measures have been taken to ensure that the risk is no longer likely to materialise; or

it would be disproportionate to notify, in which circumstances data controllers should make a public announcement to those affected. In the event of a breach, controllers should notify the relevant authority within 72 hours of becoming aware of the breach, failing which a reason must be furnished for the delay.

### **Record Keeping**

Data controllers must keep a data breach register to enable the ICO to verify compliance with the controller’s notification obligations. Records must detail the remedial action taken by the controller

in relation to the breach. In preparation for implementation of the GDPR on 25 May 2018, data controllers should prepare template security breach notifications and put procedures and policies in place to deal with a breach within the necessary timescales.

### **Preventative Steps**

Organisations should introduce technical and organisational measures to ensure that the risk presented by the data processing is matched with an appropriate level of security. The GDPR also introduces the concept of “pseudonymous data” which in simple terms, concerns the processing of personal data in such a way as to prevent an individual being identified from that data without additional information.

Although pseudonymous data is still considered a type of personal data and so is subject to the requirements of the GDPR, organisations that pseudonymize their data will benefit from relaxations of certain provisions of the GDPR. For example in the event of a data breach of pseudonymous data, the data controller may not need to notify the relevant authority or data subject because loss of pseudonymised data is unlikely to create risk of harm.

### **One Stop Shop**

One of the key changes to be introduced by the GDPR is the ‘One-Stop-Shop’ mechanism. It was hoped that it would achieve supervision by one lead authority to organisations with a presence in more than one member state. However, the mechanism is in fact more complicated than many had anticipated as it distinguishes between cross-border and domestic processing. Where the ‘One-Stop-Shop’ mechanism does apply, there are complex cooperation and coordination procedures. In order to enable individuals to have their cases dealt with locally, the GDPR contains a detailed regime with the relevant lead supervisory authority and concerned authorities working together.

## **Enforcement**

### **Powers**

The GDPR places greater power in the hands of the ICO, including the power to carry out audits and issue orders compelling data controllers or processors to cease operations, notify data subjects of a breach, rectify, restrict or erase personal data, suspend or prohibit processing or order suspension of data flows to third countries.

### **Fines**

Fines can be imposed for any infringement of the GDPR provided that the ICO ensures the level of the fine is “effective, proportionate and dissuasive”. The level of fine depends upon the nature of the breach. Less serious breaches may result in fines of up to €10,000 or, up to 2% of worldwide annual turnover of the preceding financial year (whichever is the greater).

For breaches of more serious breaches, such as processing without a relevant processing condition or failing to respond to a request from a data subject, fines can be up to €20,000,000 or in the case of an undertaking, 4% of total worldwide annual turnover in the preceding financial year (whichever is greater).

## Compensation

The GDPR provides data subjects with the right to a judicial remedy against data controllers and data processors. The data subject must have suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the data controller or data processor. This presents a risk for data controllers and processors and heightens the need for compliance. Data processors are protected to the extent that liability is limited to damage caused by processing where it has not complied with its specific obligations or acted contrary to the lawful instructions of the data controller.

**GDPR Team**  
01244 354 815  
alison.brennan@dtmlegal.com

---

Alison Brennan

Partner



Edward Barnes  
Head of Corporate and Commercial



Fredrica Reid  
Solicitor

