A practical guide to the
General Data Protection Regulation

Version 1.0, September 2017
How we can help

If you need specialist advice on any aspects of this Guide, our Data Protection team would love to hear from you. Our team is able to assist with:

- Contract Drafting & Reviews
- Cybersecurity Strategy
- Data Protection Audits
- Data Protection Impact Assessments
- Policies & Procedures
- Privacy Notices
- Regulatory Enforcement
- Reputation Management
- Subject Access Requests
- Training

To get in touch:

Call: +44(0)117 906 9400
Email: enquiries@gregglatchams.com

Disclaimer

Although we have taken great care in preparing this Guide, it is not intended to constitute legal advice on which you should rely. Data protection law is a complex and highly context-specific area of law. We give no warranties of any kind, express or implied, with regard to the accuracy, timeliness or completeness of any information contained in this Guide. If you have any questions arising from this Guide, please contact the solicitor or other member of staff with whom you usually deal.

Regulatory Information

Gregg Latchams is a limited company registered in England & Wales (company number 06899567) and is authorised and regulated by the Solicitors Regulation Authority (SRA number 607476). For further information about how we are regulated, please visit the Regulatory Info page on our website.

© 2017 Gregg Latchams Limited
# Contents

<table>
<thead>
<tr>
<th>Introduction</th>
<th>A note on Brexit</th>
<th>How the GDPR works</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Recitals and provisions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Derogations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supervisory authorities and the EDPB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scope</th>
<th>Principles</th>
<th>Lawful processing</th>
<th>Information notices</th>
<th>Rights of data subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Living individuals</td>
<td>Lawfulness, fairness and transparency principle</td>
<td>The six grounds for lawful processing</td>
<td>Fair and transparent processing</td>
<td></td>
</tr>
<tr>
<td>The definition of ‘personal data’</td>
<td>Purpose limitation principle</td>
<td>Consent</td>
<td>Information to be given</td>
<td></td>
</tr>
<tr>
<td>Automated and manual processing</td>
<td>Minimisation principle</td>
<td>Legitimate interests</td>
<td>When information must be given</td>
<td></td>
</tr>
<tr>
<td>Territorial scope</td>
<td>Accuracy principle</td>
<td>Consent v. Legitimate interests</td>
<td>How information should be given</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accountability</th>
<th>The eight rights of data subjects</th>
<th>Right to be informed</th>
<th>Right of access</th>
</tr>
</thead>
</table>
A practical guide to the **General Data Protection Regulation**

Right to rectification .................................................................................................................. 31
Right to erasure (‘right to be forgotten’) .................................................................................. 32
Right to restrict processing ....................................................................................................... 33
Right to data portability ........................................................................................................... 34
Right to object ......................................................................................................................... 35
Rights relating to automated decision-making and profiling .................................................. 36

<table>
<thead>
<tr>
<th>Transfers of personal data</th>
<th>38</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background ..................</td>
<td>38</td>
</tr>
<tr>
<td>Conditions for transfer ...</td>
<td>38</td>
</tr>
<tr>
<td>Adequacy decisions ..........</td>
<td>39</td>
</tr>
<tr>
<td>Appropriate safeguards ......</td>
<td>40</td>
</tr>
<tr>
<td>Derogations ..................</td>
<td>40</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Processors</th>
<th>42</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obligations on processors</td>
<td>42</td>
</tr>
<tr>
<td>Contractual requirements</td>
<td>42</td>
</tr>
<tr>
<td>Sub-processors</td>
<td>42</td>
</tr>
<tr>
<td>Processors becoming controllers</td>
<td>43</td>
</tr>
<tr>
<td>Accountability, record-keeping and disposal</td>
<td>43</td>
</tr>
<tr>
<td>Security of processing</td>
<td>43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Breach notification</th>
<th>45</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifying the ICO ...</td>
<td>45</td>
</tr>
<tr>
<td>Notifying the data subject</td>
<td>46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enforcement</th>
<th>47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to lodge a complaint</td>
<td>47</td>
</tr>
<tr>
<td>Right to judicial remedy against a supervisory authority</td>
<td>47</td>
</tr>
<tr>
<td>Right to judicial remedy against controllers and processors</td>
<td>47</td>
</tr>
<tr>
<td>Right of representation</td>
<td>48</td>
</tr>
<tr>
<td>Right to compensation</td>
<td>48</td>
</tr>
<tr>
<td>Administrative fines</td>
<td>48</td>
</tr>
<tr>
<td>Other powers</td>
<td>49</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other aspects</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymisation and pseudonymisation</td>
<td>50</td>
</tr>
<tr>
<td>Appointment of representatives</td>
<td>50</td>
</tr>
<tr>
<td>Data Protection Officers</td>
<td>50</td>
</tr>
<tr>
<td>Data protection by design and by default</td>
<td>52</td>
</tr>
<tr>
<td>Data Protection Impact Assessments</td>
<td>52</td>
</tr>
<tr>
<td>Codes of conduct and certification</td>
<td>54</td>
</tr>
</tbody>
</table>

| Achieving compliance | 55 |
A practical guide to the **General Data Protection Regulation**

## Glossary

Below, we have included a glossary of key terms as they are used throughout this Guide. However we would strongly advise the reader to consult the definitions in the GDPR, which are contained in article 4 of the GDPR, directly.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>controller</strong></td>
<td>a person (whether an individual, legal entity or other body) which, alone or jointly with others, determines the purposes and means of the processing of personal data</td>
</tr>
<tr>
<td><strong>data subject</strong></td>
<td>a living individual who can be identified, directly or indirectly, from personal data</td>
</tr>
<tr>
<td><strong>DPA</strong></td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td><strong>GDPR</strong></td>
<td>EU Regulation 2016/679, which has the short title of the ‘General Data Protection Regulation’. The original text is published on the <a href="https://eur-lex.europa.eu">European legislation website</a>. However a more readable copy can be found on the <a href="https://www.gdpr-info.eu">GDPR Info</a> website (both are third party websites over which we have no control)</td>
</tr>
<tr>
<td><strong>ICO</strong></td>
<td>Information Commissioner’s Office, which will continue to be the supervisory authority for the UK</td>
</tr>
<tr>
<td><strong>personal data</strong></td>
<td>any information relating to a data subject including an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject (see further commentary on this definition within the <strong>Scope</strong> section)</td>
</tr>
<tr>
<td><strong>process</strong></td>
<td>any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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</td>
</tr>
<tr>
<td><strong>processor</strong></td>
<td>a person (whether an individual, legal entity or other body) which processes personal data on behalf of a controller</td>
</tr>
</tbody>
</table>
special category data
previously defined in the DPA as ‘sensitive personal data’, this is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual’s sex life or sexual orientation

supervisory authority
in respect of each member state of the EU, an independent public body which is responsible for monitoring and enforcing compliance with the GDPR

WP29
the Article 29 Working Party, an independent advisory body which provides harmonised guidance (in the form of ‘guidelines’ and ‘opinions’) on matters relating to European data protection law. Under GDPR, this will become the European Data Protection Board (EDPB).
Introduction

Subject to a few regulated exceptions, we all have the right to respect for our private and family lives, our homes and our communications with others. This is a fundamental human right, which is entrenched in European law and enshrined in UK law through the Human Rights Act 1998. Data protection law plays an important role within the framework for protecting our fundamental human right to privacy, through regulating the way in which organisations collect and process our personal data.

The European approach to data protection law is regarded as one of the most comprehensive and restrictive in the world – certainly more so than the USA, which conspicuously does not have an overarching data protection framework (instead, there are a number of federal sector-specific laws and state privacy laws).

Enter the GDPR, which represents the most significant development in European data protection law for over 20 years. Adopted on 8 April 2016 after four years of negotiations, the GDPR significantly raises the bar for organisations that collect and process personal data – including controllers and processors based outside the EU that collect and process personal data relating to individuals within the EU. After a two year run-in period, the GDPR will apply on and from 25 May 2018. Until that date, the DPA will continue to apply (however in this Guide we will refer to the DPA in the past tense).

Although the GDPR is not conceptually dissimilar to the DPA, it augments, extends and updates the law in a number of important ways (the top 10 key changes are summarised on our infographic). In broad terms, it can be said that the ‘gold standard’ for compliance under the DPA represents the ‘baseline standard’ for compliance under the GDPR. Thus, as the ICO noted in its ‘GDPR myths’ blog series, “the new regime is an evolution in data protection, not a revolution.”

If your organisation does not have a framework in place for complying with the DPA, preparing for the GDPR will certainly require a considerable amount of effort in terms of time and, in some cases, money. However for those organisations that do have an existing compliance framework in place, and therefore a good understanding of the DPA’s requirements, preparing for the GDPR should be a less arduous and threatening task, beginning with a gap analysis to identify where the key risk areas are (see Achieving compliance).
At the time of writing, many webpages and column inches have been dedicated to the subject of the GDPR and no doubt many more will follow. Unfortunately, even some of the most authoritative and popular sources have misreported the application and implications of the GDPR.

A common theme amongst commentators is a focus on the significantly increased administrative fines for non-compliance with the GDPR. While the threat of such fines is undeniably going to be a concern for many organisations, the reality of such fines being levied has been significantly overblown (see this article as a case in point). In another of the ICO’s mythbusting articles, Information Commissioner Elizabeth Denham stated: “It’s true that we’ll have the power to impose fines much bigger than the £500,000 limit the DPA allows us...But it’s scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm...We have always preferred the carrot to the stick.”

In any case, to focus on the threat of significant fines is to undermine the importance of the entire exercise and, indeed, the opportunity for many organisations. For controllers, achieving compliance with the GDPR should be about building and securing trust amongst customers/users, reputation and ultimately value. For processors, achieving compliance with the GDPR should be about providing assurance to controllers that they are the right partner and maintaining a competitive edge. And for other organisations that provide services to controllers and processors – from marketing agencies to payroll providers – there is an opportunity to add considerable value to their customers through providing compliance-enabling solutions.

We are not the first law firm to write a guide on the GDPR. However over the course of the past 12 months, we have had the benefit of European level guidance from WP29; updated and draft guidance from the ICO; announcement of the Government’s proposals for a new Data Protection Bill; and publication of the Government’s policy paper for the protection of personal data following Brexit. Where relevant, we have drawn on these resources in preparing this Guide and also provided links to those resources at the end of each section.

We hope that you find this Guide (and our supplementary guides) useful and we are also very keen to receive feedback from readers on where they feel it could be improved.

Ed Boal, Senior Associate
edward.boal@gregglatchams.com

Hannah Gordon, Solicitor
hannah.gordon@gregglatchams.com
A note on Brexit

No guide to the GDPR would be complete without a note on Brexit.

Before the UK formally leaves the EU, the position is clear: as the GDPR is a regulation and not a directive, it will be directly applicable in the UK on 25 May 2018. To avoid confusion, the Government has confirmed in a statement of intent that the DPA will be repealed, presumably in time for or with effect from that date.

After the UK formally leaves the EU the position is, as you might expect, less clear. We know that the GDPR will become UK law “on and after exit day” by virtue of the European Union (Withdrawal) Bill (also known as the Great Repeal Bill). However we do not know the extent to which the Government will amend data protection law subsequently. It seems unlikely that the Government would seek to water down the GDPR for three main reasons:

1. It would cause confusion for organisations both inside and outside the UK if there were dual standards for the UK and the EU;

2. Given the investment that is being made by organisations in complying with the GDPR, there would be no real benefit to the UK (in terms of competition or otherwise) in diverging significantly from the GDPR (see Territorial scope);

3. Data protection law in the UK must remain ‘essentially equivalent’ to that of the EU in order for the Commission to adopt an adequacy decision for the UK (see Transfers of personal data).

With regard to the final point in particular, on 24 August 2017 the Government published its position paper on the exchange and protection of personal data after the UK leaves the EU. In that paper, the Government proposed that the European Commission should adopt an adequacy decision for the UK, while also allowing the ICO to play an ongoing role in the development of EU data protection law.

We will continue to monitor progress with the Brexit negotiations relating to data protection and will post updates on our website.

How the GDPR works

Recitals and provisions

The GDPR consists of 173 recitals and 99 operative provisions. The recitals do not (or at least should not) have any legal effect, only the operative provisions do. However the recitals, which we will draw on throughout this Guide, are useful in providing some background and context to the operative provisions.

Derogations

Although, as a regulation, the GDPR has direct effect and does not require the UK or another other Member State to pass any law to implement it, the GDPR allows Member States to implement certain aspects of the GDPR in their own way under what are known as ‘derogations’. Most of these derogations relate to matters such as national security, the prevention and detection of crime and other important public interests. We summarised some of the key derogations announced by the Government in its statement of intent for a new Data Protection Bill.

Supervisory authorities and the EDPB

Each Member State must appoint a supervisory authority as an independent body responsible for monitoring and enforcing compliance with the GDPR. A supervisory authority does not, however, have any judicial authority, which remains with the courts.

The GDPR creates a new body called the European Data Protection Board (EDPB) which will consist of members from each of the EU’s supervisory authorities (though the ICO’s position after the UK leaves the EU is unclear) plus the European Data Protection Supervisor. It will have legal status as an independent EU body and will have responsibility for overseeing the consistent application of the GDPR, amongst other tasks. It will also resolve disputes between supervisory authorities.
Scope

Living individuals

As with the DPA, the GDPR does not apply to personal data relating to deceased individuals, except to the extent that such personal data would identify a living individual (for example, medical records which identify a relative or joint bank account records). However the GDPR provides that Member States may establish their own rules for this type of processing (which countries such as Bulgaria, Estonia and France have done) and some organisations use ‘deceased suppression records’ to ensure that their marketing databases are up-to-date.

The GDPR does not apply to the processing of personal data for purely personal household activity (for example keeping an address book, recreational use of social media and home CCTV), nor does it apply to data relating to legal entities such as limited companies.

The definition of ‘personal data’

The definition of ‘personal data’ under the GDPR is not dissimilar to that under the DPA. However in relation to data that may indirectly identify an individual, the GDPR confirms that personal data includes identification numbers, online identifiers (though there is ongoing debate about whether this always includes IP addresses), location data and other factors relating to an individual’s behaviour. Organisations providing online services or relying on the use of tracking technologies will therefore need to review their data processing practices to ensure that they align with the GDPR’s requirements.

The GDPR also includes new definitions of ‘genetic data’ and ‘biometric data’, which are included within the definition of special category data.

See also Anonymisation and pseudonymisation.

Automated and manual processing

The GDPR will apply where personal data are processed wholly or partly by automated means or the manual processing of personal data which forms part of a filing system or is intended to form part of a filing system.
Any processing which does not, or is not intended to, form part of a filing system will therefore not fall within the scope of the GDPR. However in practice, this exception is unlikely to apply to most organisations, as most records are structured in some way based on some criteria in order to make them easily accessible.

**Territorial scope**

The GDPR broadens the territorial scope of EU data protection legislation. Organisations which were previously not bound by the DPA, may now find that their activities cause the GDPR to bite.

**Organisations inside the EU**

If an organisation has an establishment in the EU and processes personal data "in the context of its activities", the GDPR will apply regardless of whether the processing itself takes place within the EU. The GDPR does not define ‘establishment’, however the recitals suggest that ‘establishment’ implies "the effective and real exercise of activity through stable arrangements" and, following a European court ruling in 2014, WP29 updated its guidance to adopt an ‘inextricable link’ test.

**Organisations outside the EU**

The GDPR will apply if an organisation which is based outside the EU, processes personal data of a data subject who is ‘in the EU’ (see below) relating to:

- offering goods or services (regardless of whether a payment is made); or
- monitoring behaviour.

In considering whether a data subject’s behaviour is being ‘monitored’, the GDPR refers to whether people are tracked on the internet and whether data processing techniques such as profiling are employed (see Rights relating to automated decision-making and profiling).

**When is a data subject ‘in the EU’?**

The GDPR makes it clear that it protects the processing of personal data relating to data subjects regardless of their nationality or place of residence, as long as the processing is subject to the GDPR. However, for the purposes of considering whether an organisation outside the EU is caught by the GDPR, the GDPR does not clarify exactly what it means by the statement of a data subject being ‘in the EU’. The assumption is that it refers to a data subject being physically present in the EU at some stage rather than having to be a citizen of an EU member state.
For example, an American tourist who travels to an EU member state on holiday will be ‘in the EU’ for the duration of their stay. If a controller or processor is outside the EU, but processing personal data in the course of offering goods or services to that tourist or monitoring their behaviour, such processing will fall within the scope of the GDPR.

**Does the GDPR apply to my organisation?**

Do you have a branch, office, subsidiary or other establishment in the EU that processes personal data (whether or not the processing itself takes place in the EU)?

Do you:

- target customers in the EU?
- offer to ship products to customers in the EU?
- accept payment in Euros or the currency of another Member State?
- offer services in the language of a Member State?

Do you collect location information or track the internet browsing of individuals ‘in the EU’ and use that information to predict their behaviours?

If you have answered ‘yes’ to any of those questions then the GDPR will apply.

**References**

WP29, *Opinion on applicable law (16 December 2010)*

WP29, *Update of opinion on applicable law in light of the CJEU judgement in Google Spain (16 December 2015)*
Principles

Introduction

Those familiar with the DPA will recall the eight data protection principles set out in Schedule 1. Even though there are only six of them, the data protection principles under the GDPR are not dissimilar, though they are more detailed and underpinned by a ‘new’ Accountability principle (the seventh principle, you might say).

The principles in the GDPR are closely related to other requirements under the GDPR. For example, the lawfulness, fairness and transparency principle below is closely linked to consent and the provision of information to data subjects.

Lawfulness, fairness and transparency principle

“Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”

The references to lawfulness and fairness are the same as under the DPA. However, the reference to “transparent manner” is new and reflects the central importance of transparency to the GDPR. The relevant recital adds:

“The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used...[Data subjects] should be made aware of risks, rules, safeguards and rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.”

Controllers must therefore ensure that:

- They understand the purposes for which they are collecting personal data at the time of collection;
- Those purposes are clearly explained to data subjects in a clear manner and in straightforward language; and
- They keep data subjects informed of any changes to the basis on which their personal data are processed before such processing takes place.
Purpose limitation principle

“Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes...”

There is some crossover between this principle and the fairness and transparency elements of the principle described above. However this principle broadly requires a controller to obtain consent where personal data are ‘repurposed’, unless such repurposing would be compatible with the original purposes for which the personal data were collected.

Where a controller does not have consent and is unable to rely on some other exemption to processing personal data for a new purpose (see Legitimate interests), the GDPR provides a list of factors which should be considered when determining whether such new purpose is “compatible” with the original purposes:

- any link between the purposes for which the data were collected and the new purpose;
- the context of the collection, in particular the relationship between the controller and data subject;
- the nature of the personal data, for example whether it is special category data or relates to criminal convictions and offences;
- the possible consequences of processing personal data for the new purpose; and
- the existence of safeguards, for example encryption or pseudonymisation.

Minimisation principle

“Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”

This is not dissimilar to the principle under the DPA. However rather than saying that personal data shall not be “excessive”, this principle provides that personal data shall be “limited to what is necessary...” which is arguably more restrictive. Essentially, controllers should not collect more personal data than they need. Very often, signup forms for online services and newsletters ask for a lot of information about users – online forms will therefore need to be reviewed to ensure that non-essential fields are deleted or not made compulsory. This principle is closely related to the Purpose limitation principle.
A practical guide to the General Data Protection Regulation

Accuracy principle

“Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.”

This is very similar to the DPA. Controllers need to ensure that they have systems in place to amend or delete inaccurate or outdated personal data. How this is achieved will depend on the context of the processing and the complexity of a controller’s systems.

Storage limitation principle

“Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed...”

This principle requires controllers to consider how long they retain personal data for, regularly review the personal data that they hold and, where necessary, delete it. Clearly the longer personal data are retained, the less accurate the personal data are likely to be and the weaker the case for retaining the data will be. Complying with this principle will therefore facilitate compliance with the other principles stated above.

Neither the DPA nor the GDPR establish any minimum or maximum time periods for storing personal data. We would advise controllers to take the view that the shorter the period that personal data are retained, the better. Factors that controllers may take into account when establishing a retention policy include:

- whether the data were collected for a single, one-off purpose, or in the context of an ongoing relationship;
- the nature of the personal data, for example whether it is special category data or relates to criminal convictions and offences (which may become ‘spent’ after a period of time and therefore cannot be used to disadvantage the data subject to whom they relate);
- the costs, risks and liabilities associated with retaining the personal data; and
- regulatory requirements (for example, financial services and regulated professions).

Organisations should therefore review their retention policy and consider creating a ‘retention schedule’ for each of the categories of personal data that they process.

This principle is closely related to the Right to erasure (‘right to be forgotten’).
Integrity and confidentiality principle

“Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

This is very similar to the DPA. It is this principle which creates the close relationship between data protection law and the fields of information security and cybersecurity. It is also a failure to comply with this principle which often leads to headline-grabbing fines (see TalkTalk, for example), as maintaining the security of personal data is central to the protection of a data subject’s fundamental human right to privacy.

What is considered “appropriate” will depend upon:

- the volume of personal data collected and/or scale of processing; and
- the nature of the personal data, for example whether it is special category data or relates to criminal convictions and offences

The size of a controller or its budget for maintaining the security of personal data is unlikely to be relevant or provide a controller with any real defence.

This principle is underpinned by a specific obligation on controllers and processors to ensure the Security of processing.

A note on cybersecurity

Although there is considerable overlap between the fields of data protection and cybersecurity, they should not be conflated when it comes to achieving compliance with the GDPR. Protecting personal data which has been collected, processed and transmitted by electronic means against unauthorised access, use, destruction and/or disclosure – the objective of cybersecurity – is only one piece of the compliance jigsaw. Organisations should be careful not to invest in cybersecurity at the expense of implementing a broader data protection and information security framework.

The Government-backed Cyber Essentials Scheme is a cost-effective way for organisations to implement basic cybersecurity measures and is a pre-requisite to tendering for all Government contracts which involve handling personal data and providing IT and related services.
Accountability

“When the controller shall be responsible for, and be able to demonstrate compliance with, [the data protection principles].”

‘Accountability’ is both a principle and an overriding concept under the GDPR and may have considerable implications for organisations processing personal data.

Accountability broadly requires a controller to evaluate the risks associated with its processing activities, ensure that such risks are mitigated to the greatest extent possible (including through properly assigning roles and responsibilities within an organisation) and be able to demonstrate that it has complied with the data protection principles in mitigating those risks.

While a failure to comply with the accountability principle does not itself give rise to any fine under the GDPR, if an organisation cannot demonstrate compliance with one or more of the above principles this would indicate a breach of such principles which would potentially give rise to a fine.

Where an organisation employs more than 250 people and in certain other circumstances, an organisation is required to maintain documentation of its processing activities (an activity which was previously trapped by the requirement for controllers to register with a supervisory authority).

WP29 Working Party, Opinion on the principle of accountability (13 July 2010)
Lawful processing

The six grounds for lawful processing

Processing ‘ordinary personal data’ (see Consent and sensitive personal data and Consent and children) will only be lawful if one of the following six grounds applies (subject to any exemptions and derogations, see How the GDPR works):

1. **Consent** – a data subject has consented to the processing of their personal data for one or more specific purposes (see Consent);

2. **Contractual arrangements** – the processing is necessary for entering into or performing a contract with a data subject (for example, an application for a credit card or an insurance company processing a claim);

3. **Legal obligations** – the processing is necessary for compliance with a legal obligation to which a controller is subject under EU or Member State law (for example, the sharing of data between banks for fraud prevention purposes);

4. **Vital interests** – the processing is necessary to protect the vital interests of a data subject or another person such as a child of a data subject (for example, processing by emergency services to save a person’s life);

5. **Public interest tasks** – the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a controller or a third party to whom the data are disclosed, in each case under EU or Member State law (for example, a local authority processing council tax notices); and

6. **Legitimate interests** – the processing is necessary for the purposes of legitimate interests pursued by a controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of a data subject (in particular where a data subject is a child) (see Legitimate interests).

In this Guide, we will focus on consent and legitimate interests. However it should be noted that there is no hierarchy within these grounds: if processing can be justified on one of these grounds, such processing will be considered lawful.
Consent

Although, as noted above, there is no hierarchy within the grounds for processing, consent is often perceived to be a ‘silver bullet’ or ‘gold standard’ for establishing a lawful basis for processing. However by requiring consent to be “unambiguous” and given by a “statement or by a clear affirmative action”, the GDPR sets a higher, more dynamic standard for consent which may be impractical and/or difficult for a controller to obtain, such that another ground for processing may prove more appropriate and/or convenient.

One of the recitals states that where a controller has already obtained consent under the DPA, they do not have to refresh that consent under the GDPR, provided the consent obtained under the DPA meets the standard established by the GDPR. However given the higher standard set by the GDPR, and the requirement that consent must be evidenced (see Accountability), many controllers will find that their methods for obtaining and recording consent are insufficient for the purposes of the GDPR and that they will need to bring such consent ‘up to standard’ (which some are calling ‘re-permissioning’). In any case, the ICO has made it clear in its draft consent guidance that consent is not a “one-off compliance box to tick and file away.”

Standard of consent

Consent from a data subject must be:

- **Freely given**: the data subject must have a genuine and free choice without any risk of suffering detriment or any other negative consequences if they do not give, or later withdraw, their consent. If there is an imbalance in the relationship between a controller and a data subject, controllers will need to consider one of the other grounds for processing;

- **Specific**: blanket consent to all processing activities will not be valid. Instead, consent must be granular, enabling consent to be given based on a data subject’s personal preferences (see Purpose limitation principle);

- **Informed**: a data subject should be provided with clear information about the identity of the controller and each purpose for which their personal data will be processed (see Information notices);

- **Unbundled**: consent to the processing of personal data should not be combined with other terms and conditions. Not only does this confuse consent to the processing of personal data with the terms that relate to use of a service, it may indicate that consent is not freely given; and
Easily withdrawn: a data subject should be provided with clear information about the identity of a controller and each purpose for which their personal data will be processed.

Does the GDPR always require explicit consent?

The GDPR requires ‘explicit consent’ for the processing of special category data and may be used to legitimise automated decision-making (see Profiling) and the transfer of personal data outside of the EEA (see Transfers of personal data). However there is some confusion over whether ‘explicit consent’ (a clear written or oral ‘I agree’ or ticking an unticked box) is always required for the processing of ‘ordinary personal data’ under the GDPR, as opposed to implied consent.

It is clear from the negotiations that led to the GDPR that omission of the word ‘explicit’ was not an error, and the recitals do say that consent can be given by “another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data.” Confusingly in its draft guidance, the ICO said that “all consent must be opt-in consent – there is no such thing as opt-out consent…The idea of an affirmative act does still leave room for implied consent in some circumstances, particularly in more informal offline situations.”

Whether explicit consent is required therefore depends on the nature of the personal data being processed and the context. The ICO gives, as an example of where implied consent would be acceptable, the example of someone who drops a business card into a box for a prize draw, where they are clearly indicating that they consent to the processing of their contact details if they win a prize (but not to any other processing).

Consent and special category data

The GDPR prohibits the processing of special category data unless one or more of ten grounds applies, including consent. However in addition to meeting the standard of consent for ‘ordinary personal data’, such consent must be explicitly given.

Consent and children

The GDPR contains a specific provision relating to the provision of online services (other than preventive or counselling services) to children. If such services are offered to children under the age of 13 and a controller wants to rely on consent, they will need to obtain consent from a person having ‘parental responsibility’ for the child. Once a child reaches the age of 13, the consent given by the holder of parental responsibility will lapse and a controller will need to obtain fresh consent from the data subject.
The GDPR requires a controller to make “reasonable efforts” to verify whether consent has been given or authorised by a person having parental responsibility for a child which, the ICO has said, will require age-verification measures to be implemented within online services.

Method of obtaining consent

The GDPR does not prescribe any method by which consent must be obtained. However, the GDPR requires consent to be given by a “clear affirmative act”, which may be given “...by a written statement, including by electronic means, or an oral statement.” The method of obtaining consent will therefore very much depend on the context. Methods of obtaining consent may therefore include:

- checking an opt-in box (opt-out boxes are essentially the same as pre-ticked boxes, which are specifically banned) or clicking a link;
- selecting yes/no options (where, in order to ensure consent is freely given, neither option is more prominent than the other);
- choosing technical settings or preferences;
- responding to an email requesting consent;
- answering ‘yes’ or a similar statement to an oral request; or
- volunteering information, for example, completing a survey, filing optional fields in a form or dropping a business card into a box (though in each case, there should be a notice explaining the purposes for which the personal data will be processed if not immediately obvious).

Remember consent must be specific, so sometimes a controller will need consent to more than one statement, or more than one checkbox, for consent to be validly given.

In the context of online services, one of the recitals provides that consent must be “clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.” Given the amount of information which must be given to data subjects under the GDPR (see Information notices), providers of online services will need to think about user-friendly methods for obtaining consent such as ‘layered’ and ‘just-in-time notices’.

Recording consent

Where consent is relied upon as a ground for processing, the GDPR requires a controller to be able to demonstrate that a data subject has consented to the processing of their personal data. This will require adequate measures to be in place to record how and when consent was given, by whom and what they were told at the point at which consent was given. Similarly, as consent has to be capable of being withdrawn at any time (see Withdrawal of consent), this will need to be recorded.
Time limit for consent

Neither the DPA nor the GDPR set a specific time limit for how long consent given by a data subject will last. However it has always been understood that consent has a ‘shelf life’ and that, depending on the circumstances, a data subject’s personal data will either need to be deleted after some defined period of time (see Storage limitation principle) or their consent refreshed.

The ICO advises that consent should be seen as a dynamic part of the ongoing relationship between a controller and data subject, with a data subject having ongoing choice and control over the processing of their personal data.

A controller may therefore want to establish a regular review policy, either by simply setting calendar reminders to review records or by automated means. The ICO recommends refreshing consent at least every two years, though a longer period may be justifiable in the circumstances.

Withdrawal of consent

A data subject has the right to withdraw consent “at any time” and it must be as easy for a data subject to withdraw consent as it was for them to give it. The key points are:

- Withdrawal of consent should be a one-step process;
- Individuals must not suffer any detriment as a result of withdrawing their consent (see Right to data portability);
- Withdrawal of consent does not affect the lawfulness of any processing carried out before such time; and
- Once consent has been withdrawn, no further processing should take place, unless one of the other grounds for processing can be

Legitimate interests

Although this ground existed under the DPA, there is a greater focus on legitimate interests given the higher standard for consent and the need for controllers to demonstrate that consent has been given under the GDPR.

Processing will only be lawful under the legitimate interests ground where “it is necessary for the purposes of the legitimate interests pursued by the controller...” except where the controller’s interest/stake in the processing of personal data outweighs the “…interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”
One of the recitals provides that “…the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.” An industry body called the Data Protection Network (DPN) has published helpful guidance on undertaking this assessment, which they call a Legitimate Interests Assessment (LIA). Guidance from the ICO on legitimate interests is expected before the end of 2017.

The three stage test

The DPN suggests a three-stage test for undertaking an LIA:

1. **Identify a legitimate interest**: this involves identifying the purpose(s) for which personal data are to be processed and the controller’s interest(s) in such processing. The DPN’s guidance suggests that such interest must be “real and not too vague”, for example making a profit is unlikely to be a legitimate interest in and of itself;

2. **Establish whether the processing is ‘necessary’**: just because a controller has a legitimate interest(s) in processing personal data, this does not mean that such processing is necessary for the pursuit of such interest(s). This limb of the test requires an assessment of whether there are other ways of pursuing a legitimate interest(s) – if there isn’t, or another way would require disproportionate effort, then the processing may be considered necessary;

3. **Conduct a balancing test**: finally, a controller must consider whether its legitimate interests are outweighed by the interests or fundamental rights and freedoms of the data subject, taking into account the nature of the interest(s), impact of the processing and any safeguards which are or could be put in place. Clearly there is some scope for conflict and bias within this limb of the test, and a controller may wish to consider engaging a consultant or obtaining legal advice to obtain a fair and unbiased view in this regard.

Recording the LIA

Having carried out an LIA, it is advisable for a controller to keep a record of the fact that it has been completed, and how they reached a conclusion that they did/did not pass the balancing test to establish whether the legitimate interests ground could be relied upon. Of course, if the scope of the processing were ever to change then the decision to rely on legitimate interests would need to be reviewed, and a fresh LIA carried out to ensure that the ground was still justifiable in the context of the new processing activity. Such review and fresh LIA should of course also be documented.
The DPN’s guidance includes a useful LIA template, which can be modified to suit an organisation’s particular needs.

**Consent v. Legitimate interests**

Given the increased standard for consent, many organisations will look to rely on legitimate interests where there is no other appropriate ground for processing. When deciding which of these two grounds to rely upon, a controller should consider:

- The nature and context of the processing. For example, although financial data is not considered special category data under the GDPR, it is still likely to be considered as such by data subjects and will almost certainly be confidential information. The ICO expressed some reservations during the negotiation of the GDPR about the categorisation of personal data as ‘sensitive’, instead favouring a purpose-based approach. Although the GDPR requires a controller to inform a data subject if it is rely on legitimate interests, this may be perceived as more invasive, making consent more appropriate;
- Whether the processing activities proposed are *necessary* to fulfil the controller’s legitimate interests. If not, then the legitimate interests ground cannot be relied upon and consent should be considered;
- Whether its legitimate interests are compelling enough without putting in place additional safeguards;
- Whether it is confident that it is able to justify processing based on legitimate interests and still meet the requirement to be transparent; and
- Whether it will be able to uphold a data subject’s **Right to object**, which applies to processing based on legitimate interests, not consent (withdrawal of consent may be considered less onerous that the right to object).

---


[Data Protection Network, *Legitimate Interests Guidance*, (Version 1.0, 10 July 2017)](https://www.dataprotectionnetwork.co.uk/guidance/privacy/legitimate-interests/legitimate-interests-v2.0-17080001) (Requires free registration)
Information notices

Fair and transparent processing

Regardless of the ground relied upon by a controller for the processing of personal data, the Lawfulness, fairness and transparency principle requires a controller to communicate with data subjects in a transparent manner regarding its processing activities. In particular:

- data subjects should be informed about a controller’s identity and understand how their personal data are collected, used, consulted or otherwise processed and the extent to which they are or will be processed;
- data subjects should understand the risks, rules, safeguards and rights they have in relation to such processing;
- information should be easily accessible and easy to understand; and
- clear and plain (non-legal) language should be used.

Information to be given

The GDPR requires more information to be given to data subjects than under the DPA. The information that needs to be given also depends on whether personal data are collected from a data subject, or obtained from someone other than a data subject (either bought-in databases or personal data shared by other organisations):

<table>
<thead>
<tr>
<th>Information to be provided</th>
<th>Obtained from data subject</th>
<th>Obtained from third party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity and contact details of the controller and any representative</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Contact details of any data protection officer</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Purposes of the processing and legal basis for processing</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Categories of personal data processed</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Recipients or categories of recipients, if applicable</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
A practical guide to the General Data Protection Regulation

<table>
<thead>
<tr>
<th>Information regarding transfers of personal data outside the EEA and appropriate safeguards</th>
<th>✓</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retention period, or criteria used to determine the retention period</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Existence of data subject’s rights</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Right to withdraw consent at any time, if consent is the ground used for processing</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Right to lodge a complaint with a supervisory authority</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Source that the personal data originates from and whether it came from publicly accessible sources</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Whether the provision of any personal data is a legal or contractual requirement or obligation and the consequences of not providing such information</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Existence of automated decision-making, including profiling, if applicable and information about the logic involved and significance and consequences of such processing</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Regardless of the source of the personal data, the above information does not need to be given where a data subject has already been given the information.

In relation to personal data collected from third parties specifically, there are a number of further exemptions which should be exercised with caution, including where the provision of such information would be impossible or require a disproportionate amount of effort, particularly if collected for public interest, scientific, historical research or statistical purposes.

**When information must be given**

Where personal data are collected from a data subject, the relevant information must be given at the time of collection.
Where personal data are collected from a third party, the relevant information must be given within a reasonable period of time and in any case within one month from the date of receipt, unless the personal data are to be:

- used to communicate with a data subject, in which case the information must be provided at the time of the controller’s first communication (at the latest); or
- shared with another recipient, in which case the information must be provided when the personal data are first shared (at the latest).

**How information should be given**

The GDPR does not prescribe how the relevant information should be given, though it suggests that information may be provided “...with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing.” Although the use of iconography is not a new idea, opinion is divided on the value of this approach given the variety and complexity of data processing activities.

The ICO’s guidance on information notices (or privacy notices, as the ICO calls them and as they are generally known by) has been updated to reflect the GDPR and should be consulted by controllers when developing their approach to providing the necessary information.

[ICO, Privacy notices, transparency and control (Version 1.0.33, 7 October 2016)]
Rights of data subjects

The eight rights of data subjects

The GDPR builds upon the rights contained in the DPA and, to reflect modern times, creates some new and enhanced ones. The eight rights are:

1. Right to be informed;
2. Right of access;
3. Right to rectification;
4. Right to erasure;
5. Right to restrict processing;
6. Right to data portability;
7. Right to object; and
8. Rights relating to automated decision-making and profiling.

Right to be informed

This right is underpinned by the overarching concepts of accountability and transparency and is integral to complying with the Lawfulness, fairness and transparency principle. See Information notices.

Right of access

This right, also known as the ‘subject access right’, is regarded by many as the most important of the eight rights. It gives individuals the right to obtain confirmation that their personal data are being processed and, if that is the case, to access and be provided with a copy of their personal data easily and at reasonable intervals in order to be aware of, and verify, the lawfulness of a controller’s processing activities.

The right of access is not a new right. However, as noted under the headings below, it has been enhanced under the GDPR and will arguably increase the administrative burden on controllers to comply with such requests.

This right is closely related to the Right to data portability.

Information that must be provided

A data subject has the right to be provided with the following information:
the purpose of the data processing;
the categories of personal data being processed;
the recipients or categories of recipient to whom the personal data have been or will be disclosed and in particular where those recipients are in countries outside the EEA or are international organisations (see Transfers of personal data);
where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period;
the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
the right to lodge a complaint with a supervisory authority;
where the data has not been collected from the data subject, any available information as to their source; and
the existence of automated decision making, including profiling, and meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing for the data subject.

Format of requests

Unlike the DPA, the GDPR does not expressly require access requests to be made in writing although, in practice, access requests will be made in writing (including by email, text, fax or post). Controllers will need to ensure that staff are properly trained to identify whether an access request has been made, particularly given the timescale for fulfilling requests.

Identifying the data subject

As with the DPA, the GDPR permits a controller to request further information to satisfy itself as to the identity of any person making a request where it has “reasonable doubts”. Once a controller has satisfied itself that it is dealing with the data subject or some person authorised by them, it must comply with the request.

Method of providing information

Where any access request is made by electronic means, the GDPR requires a controller to provide the necessary information in a “commonly used electronic form”, unless the data subject requests otherwise. The GDPR does not say whether the expression refers to common use by controllers or data subjects (for example, XML is a commonly used format, but few data subjects would have the ability to read such files), however it does say that information must be provided in an “intelligible and easily accessible form”.
In relation to requests that are not made by electronic means, controllers should discuss the format in which the information will be provided with the data subject.

If a controller holds a large quantity of personal data on a data subject, it may ask the data subject to specify the information or processing to which their request relates.

**Timescale for responses**

The GDPR reduces the timescale for fulfilling access requests from 40 calendar days to a maximum of one month from receipt of the request (though access requests should be fulfilled “without undue delay”). However this time period may be extended by up to two further months where necessary, taking into account the complexity and number of requests made. A controller can only benefit from this time extension if it has informed the data subject within one month from the receipt of their request and provided its reasons for doing so.

**Charging fees for access requests**

Under the DPA, controllers were permitted to charge a maximum fee of £10 per request. Under the GDPR, requests must be fulfilled free of charge. However for any further copies requested, the controller can charge a “reasonable fee based on administrative costs”. Furthermore, where a controller can demonstrate that any requests from a data subject are “manifestly unfounded or excessive, in particular because of their repetitive character”, a controller may refuse to act on the request or charge a “reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested”.

**Right to rectification**

Often used in conjunction with the Right to restrict processing, this right remains largely unchanged under the GDPR.

Where a controller holds inaccurate (which may mean incorrect or misleading) personal data about a data subject, that data subject has the right to obtain from the controller the rectification of their personal data without undue delay. A data subject also has the right to have incomplete personal data completed, including by means of the controller providing a supplementary statement.

A controller is under an obligation to communicate any rectification of personal data to any recipient to whom personal data have been disclosed, unless to do so would be impossible or involve disproportionate effort. If a data subject requests, then a controller must inform the data subject about who the recipients of their personal data are.
Right to erasure (‘right to be forgotten’)

Background

One of the most publicised and widely reported areas of the GDPR is the ‘right to be forgotten’. Building upon a right that established by the judgment in a highly controversial case brought against Google Spain in 2014, the GDPR provides a broader right for data subjects to ask any type of controller, not just internet search engines, to actually erase their personal data in certain circumstances.

Conditions for exercising the right

While the press often makes it sound as though the power to exercise the right to erasure is entirely in the hands of the data subject, this is not the case. A controller is only obliged to comply with such a request if one the following circumstances apply:

- the data are no longer required for the purposes for which they were originally collected or processed (and no new lawful purpose exists);
- the data subject withdraws their consent, where this was the basis for the processing, (and no other lawful ground exists);
- the data subject exercises their right to object to the processing and there are no overriding legitimate grounds for continuing the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation to which a controller is subject; or
- the personal data are processed in relation to the provision of online services to a child (in the UK this means they were under 13, see Consent and children).

Exceptions to the right to erasure

There are some exceptions where the right to erasure will not apply. A data subject’s right cannot be exercised where processing of personal data is necessary:

1. for the exercise of the right of freedom of expression and information;
2. for compliance with a legal obligation to which the controller is subject;
3. for the performance of a task carried out in the public interest or in the exercise of official authority;
4. for public health reasons;
5. for archival, research or statistical purposes; or
6. if required for the establishment, exercise or defence of legal claims.
The ‘right to be forgotten’ bit

Where a controller has made personal data public and is obliged for one of the above reasons to erase the data, the controller has an obligation to take “reasonable steps” to inform other controllers who are also processing the data that the data subject has requested erasure. Erasure should include any links to, or copy or replication of the personal data. This is the function which gives the ‘right to be forgotten’ its name.

Communication of erasure

As with the Right to rectification and the Right to restrict processing, a controller must communicate the erasure of personal data to each recipient to whom personal data have been disclosed, unless it would be impossible to do so or would involve disproportionate effort.

Right to restrict processing

This right is similar to the ‘right the block’ under the DPA and provides a data subject with the right to request that a controller restricts the processing of their personal data in the following circumstances:

1. The accuracy of personal data are contested by a data subject (until the controller has verified its accuracy) (temporary restriction);

2. The processing is unlawful and a data subject opposes erasure of the personal data and chooses its restriction instead (permanent restriction);

3. A controller no longer needs the personal data for the purposes of processing, but it is required by a data subject for the establishment, exercise or defence of legal claims (permanent restriction); or

4. The data subject has exercised their Right to object and wishes the processing of their personal data to be restricted pending confirmation from a controller as to whether it has “compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject” (temporary restriction).

A ‘restriction of processing’ means that a controller can continue to store the data, but will not be able to process it unless either the data subject consents, or processing is necessary for the establishment, exercise or defence of legal claims or for the protection of the rights of another individual or legal entity or for reasons of important public interest of the EU or a Member State.
If a restriction is in place, a controller must notify the data subject before lifting it. As with the **Right to rectification** there is also an obligation on a controller to communicate any restriction of processing to any recipient to whom personal data have been disclosed, unless to do so would be impossible or involve disproportionate effort. If a data subject requests, then a controller must inform the data subject about who the recipients of their personal data are.

### Right to data portability

**Background**

The GDPR introduces a new right to ‘data portability’. This new right aims to give individuals greater control over personal data which has been processed by automated means, by allowing individuals to receive a copy of their personal data and to request the transmission of their personal data to another controller in a “commonly used and machine-readable format”. It is considered that this right will improve competition by enabling consumers to switch service providers with greater ease.

There is some confusion over the scope of this right. The relevant provision of the GDPR provides that where the conditions for exercising the right are met, an individual is only entitled to a copy of all personal data *which they have provided* to a controller; which suggests personal data provided using online forms. However in its guidance, the WP29 takes a broader viewer, suggesting that this covers “data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity.” The WP29 further suggests that the right should extend to ‘observed data’, being data “provided by the subject by virtue of the use of the service or the device”. This is not, however, what the GDPR says and, indeed, the European Commission itself has said that it considers WP29’s interpretation to be too broad. It therefore remains to be seen how this right will be enforced in practice.

Some commentators have also labelled this right as a ‘false promise’, as it will require controllers to invest a significant amount of money and effort in upgrading systems and processes. That being said, the recitals suggest that there should not be an obligation on controllers “to adopt or maintain processing systems which are technically compatible” with controllers instead being “encouraged to developer interoperable formats that enable data portability”.

**Conditions for exercising the right**

A data subject may only exercise the right to data portability, where:
1. The lawful basis for processing is either a data subject’s **Consent** or the performance of a contract to which a data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; and

2. The processing is carried out by **automated means**.

If these conditions are met, a controller will need to be able to provide the personal data to a data subject in a “structure, commonly used and machine-readable format” so that the data subject is able to transmit those data to another controller without hindrance.

Where it is technically feasible to do so, a data subject can request that the existing controller transfers the personal data directly to a new controller.

With reference to the first condition in particular, this may provide another reason for controllers to rely on the **Legitimate interests** ground to justify processing.

**Right to object**

A data subject can exercise the right to object to their data being processed in three circumstances:

1. If the processing of personal data is being carried out on the basis that processing is necessary for:
   a. a task carried out in the public interest;
   b. a task carried out in the exercise of official authority vested in a controller; or
   c. the purpose of the **legitimate interests** of a controller or a third party,

   a controller must cease processing unless:
   - it can demonstrate compelling legitimate grounds for the processing which overrides the interests of the data subject; or
   - the processing is necessary for the establishment, exercise or defence of legal claims.

   Under the DPA, a data subject had to establish compelling grounds that would override the controller’s right to process data for public interest purposes or for their own legitimate interests. Under the GDPR, the data subject is granted a right to stop the processing, and the burden is on the controller to justify why it should be able to continue.

2. If the processing of personal data is being carried out for direct marketing purposes (including profiling, see **Rights relating to automated decision-making and profiling**), a controller must stop processing their data for such purposes.
“Direct marketing” is not defined in the GDPR, however it was defined in the DPA as “the communication, by whatever means, of any advertising or marketing material which is directed to particular individuals” and it is likely that this will continue be an appropriate definition.

3. If the processing of personal data is being carried out for scientific, historical research, or statistical purposes, a data subject can, on grounds relating to their particular situation, object to processing of personal data, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

A controller must, where it is processing personal data for any of the reasons set out at points 1 and 2 above, notify a data subject of their right to object. This must be done at the time of the controller’s first communication with the data subject (at the latest), and the right to object must be presented clearly and separately from any other information.

Rights relating to automated decision-making and profiling

Background

The DPA was arguably ahead of its time, as it gave a data subject the right not to be subjected to decisions based solely on automated processing of data for the purpose of personal evaluation, except in certain limited circumstances. The GDPR extends this right to ‘profiling’ (such as analytical technologies) which is defined as:

“any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a [data subject], in particular to analyse or predict aspects concerning that [data subject’s] performance at work, economic situation, health, personal preferences, interest, reliability, behaviour, location or movements.”

The definition of ‘profiling’ is likely to cause concern for non-EU online service providers such as social media networks, given that the monitoring of an individual’s behaviour within the EU will bring them within the Territorial scope of the GDPR.

However the scope of the restriction in relation to automated processing and profiling is narrower than it appears. First, both activities must lead to a decision being taken, which is not always the case with profiling. Second, that decision must produce “legal effects concerning [the data subject] or similarly significantly affect [the data subject]” which, unfortunately, the GDPR does not provide examples of (would profiling for the purposes of online advertising, which does not require any decision to be taken, significantly affect a data subject?).
A controller will always need to ensure that it has a lawful basis for any processing which involves profiling (see Lawful processing). If this is the case, then it must ask whether such profiling results in a decision being taken that will produce a ‘legal effect’ or otherwise ‘significantly affect’ a data subject.

Conditions for exercising the right

There are circumstances in which a data subject could be subject to an automated decision based on profiling if the decision:

1. is necessary for entering into, or performance of, a contract between the data subject and a controller;

2. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or

3. is based on the data subject’s explicit consent.

If decisions are made based on the circumstances set out in points 1 or 3 above, a controller is obliged to implement suitable measures to safeguard the data subject’s rights, freedoms and legitimate interests. As a minimum, a data subject must have the right to obtain human intervention on the part of a controller, and to express their point of view and to contest the decision.

Sensitive personal data

A decision based on profiling (for example, calculating health insurance premiums based on health data collected from a data subject’s wearable device) cannot be based on sensitive personal data unless one of the following conditions applies:

1. the data subject has given their explicit consent to that processing; or

2. the processing is necessary for reasons of substantial public interest.

If one of the above conditions does apply, then a controller must ensure that suitable measures are in place to safeguard a data subject’s rights, freedoms and legitimate interests.

ICO, Subject access code of practice, (Version 1.2, 9 June 2017)

WP29, Guidelines on the right to data portability (5 April 2017)
Transfers of personal data

**Background**

This section of the Guide relates to the transfer of personal data to recipients outside the EEA (i.e. cross-border transfers). The GDPR acknowledges that the flow of personal data to and from countries outside the EEA is necessary for the purposes of international trade and cooperation, but also acknowledges the associated challenges and concerns of data subjects whose fundamental rights should not be undermined as a result of such transfers.

The provisions on cross-border transfers under the GDPR are broadly similar to those under the DPA, with some differences that are considered below.

**Conditions for transfer**

As with the DPA, the GDPR maintains a general prohibition against the transfer of personal data by controllers and processors outside the EEA unless one of the conditions for transfer has been met. The transfer of personal data outside the EEA (to so-called ‘third countries’) will therefore only be compliant with the GDPR in the following circumstances:

1. An **adequacy decision** has been made by the Commission in relation to a particular third country;

2. A controller or processor has provided **appropriate safeguards** to protect the personal data outside the EEA;

3. A controller or processor has adopted **binding corporate rules** for the transfer of personal data which have been approved by a supervisory authority;

4. There is neither an adequacy decision nor appropriate safeguards, but **one of the GDPR’s derogations** applies.

In this guide, we will focus on (1), (2) and some the derogations under (4) above.
A practical guide to the General Data Protection Regulation

Adequacy decisions

The Commission can decide that a country, a territory, or one or more specified sectors within a country, or an international organisation, has an “adequate level of protection” in place so that data transfers can take place without any specific authorisation.

The GDPR sets out the factors which the Commission will take into account when assessing adequacy, which are more prescriptive than under the DPA. If an adequacy decision is made, it must be reviewed periodically and at least every four years. The Commission is also under an obligation to monitor developments in third countries and international organisations that could affect previous adequacy decisions, and act to amend/repeal them if necessary. Existing adequacy decisions will remain in force until they are amended, replaced or repealed by a Commission decision under the GDPR. Given the more onerous requirements for adequacy decisions under the GDPR, changes are highly likely and organisations that rely on adequacy decisions should keep a close eye on developments in this regard.

A note on transfers to the US and Privacy Shield

For well over a decade, controllers relied upon the ‘Safe Harbour Framework’ to legitimise the transfer of personal data to US-based organisations. Under the Framework, which was supported by an adequacy decision, processors based in the US would self-certify compliance and their details would be entered onto an official list.

Following the explosive Snowden revelations in 2013, an Austrian law student called Max Schrems challenged the transfer of personal data between Facebook’s Irish and US legal entities under the Framework. When a number of questions were referred to Europe’s highest court, it ruled that the adequacy decision was invalid on the basis that US national security interests were given priority over the principles established by that decision.

After two years of negotiations, a new framework – Privacy Shield – was adopted under a new adequacy decision, providing greater assurances around the bulk collection of personal data by intelligence agencies and providing greater redress for data subjects in respect of processing by US-based organisations. Almost 2,500 organisations have self-certified compliance with the Privacy Shield Principles so far.

However Privacy Shield is due to be reviewed at the end of September 2017 and it is anticipated that there may be another challenge before the European courts. As such, the future of Privacy Shield remains unclear and controllers may therefore want to consider whether any further appropriate safeguards should be explored additionally.
Appropriate safeguards

In the absence of an adequacy decision, personal data may be transferred outside the EEA if a controller or processor has “...provided appropriate safeguards, and on condition that data subject rights and effective legal remedies for data subjects are available.” The GDPR lists these ‘appropriate safeguards’ as:

- a legally binding and enforceable instrument between public authorities;
- binding corporate rules;
- standard contractual clauses adopted by the Commission;
- standard contractual clauses adopted by a supervisory authority and approved by the Commission;
- an approved code of conduct; or
- an approved certification mechanism.

Of the above safeguards, the most popular is the use of standard contractual clauses (or ‘model clauses’) adopted by the Commission. The existing model clauses will remain valid until amended, replaced or replaced in accordance with the GDPR.

Derogations

In the absence of either an adequacy decision or appropriate safeguards, the GDPR provides some circumstances in which personal data can still be transferred to a third country or an international organisation under one of seven derogations which are similar to those under the DPA:

- explicit consent;
- contractual necessity;
- protection of the vital interests of a data subject where they are physically or mentally unable to consent;
- important reasons of public interest;
- establishing, exercising or defending legal claims; or
- transfers from a public register which is intended to provide information to the public and where specific conditions are fulfilled.

There is also a new limited derogation which can apply if no other derogations are applicable. A transfer must be:

- non-repetitive;
- concerning only a limited number of data subjects; and
necessary for the purposes of compelling legitimate interests of a controller, which are not overridden by the interests or rights and freedoms of a data subject.

A controller must have also assessed the circumstances of the transfer and provided suitable safeguards regarding protecting the personal data. A controller must also notify the ICO of the transfer, and inform a data subject of the transfer and the compelling legitimate interests upon which it is relying.

ICO, *Using the privacy shield to transfer data to the US (Version 1.0, 30 June 2017)*
Processors

Obligations on processors

Perhaps one of the most significant changes under the GDPR is that a processor can no longer hide behind a controller in the event of regulatory action being taken. In addition to any breach of contract claim that a controller may have against a processor, the GDPR imposes direct obligations on processors and exposes processors to enforcement action and penalties if those obligations are not complied with. This is not to say that the liability of controllers and processors is the same: the responsibility for complying with the GDPR primarily rests with a controller.

One of the main concerns arising from this change is that if a processor’s costs increase in order to comply with its new obligations, those costs will be passed on to its customers. It is also likely to make negotiations over contractual provisions rather interesting, in particular indemnity clauses for breaches of data protection provisions, given the increased penalties under the GDPR (see Administrative fines).

Contractual requirements

While the DPA required a controller to put in place a written agreement with a processor, the GDPR appears to impose an obligation on both a controller and a processor to do so. Such agreement may be in electronic form and must include a number of provisions which are stipulated by the GDPR. Both controllers and processors will need to review their agreements to ensure that they meet the GDPR’s requirements in this regard.

Sub-processors

A processor cannot engage a sub-processor without a controller’s prior specific or general authorisation. Where general authorisation has been given, a processor is under an obligation to notify a controller of any proposed changes concerning the addition or replacement of any sub-processor and to give a controller the opportunity to object. Although the GDPR does not say as much, it seems logical that if any objection cannot be resolved, the processor cannot make any proposed change and the processor may therefore need a mechanism to terminate the contract in such circumstances (in particular, where it would be impractical to make an exception for a single controller).
A processor must put in place a written agreement with any sub-processor which contains “the same data protection obligations as set out in the contract...between the controller and the processor” and in any case, a processor will remain fully liable to a controller for the performance of any sub-processor’s obligations.

**Processors becoming controllers**

While the GDPR acknowledges that in certain circumstances, there may be joint controllers, it expressly provides that if a processor is found to have infringed the GDPR by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing. It is therefore important that parties clearly define their respective roles and responsibilities in any agreement.

**Accountability, record-keeping and disposal**

One of the requirements for written agreements with processors is that a processor makes available to a controller “all information necessary to demonstrate compliance with the obligations laid down in [the processor provisions of the GDPR] and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.” As such, a processor will need to have the necessary systems and processes in place to fulfil this obligation. The GDPR does not provide whether a processor can or cannot charge for contributing to audits or inspections, which is likely to be a point for negotiation.

When the processing of personal data has been completed, a processor must, at the choice of a controller, either return or delete the personal data, unless there is a requirement to store it under Union or Member State law to which a processor is subject.

**Security of processing**

Both a controller and a processor must implement “appropriate technical and organisational measures” to ensure a level of security appropriate to the risk to the rights and freedoms of a data subject. In order to establish what will be ‘appropriate’ measures to implement, a controller and processor should consider the state of the art, the costs of implementation and the nature, scope, context and purposes of processing.

Security measures which the GDPR sets out should be taken, as appropriate, include:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
A practical guide to the General Data Protection Regulation

— the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
— a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
Breach notification

Notifying the ICO

While providers of public electronic communications services have been required for some time to notify the ICO of any ‘personal data breach’, this has not been a requirement for other organisations under the DPA. However the GDPR now requires that, unless a personal data breach is unlikely to result in a risk to individuals, a controller is obliged, without undue delay and where feasible within 72 hours of becoming aware of it, to notify the ICO.

If a notification is not made within the 72 hour timeframe, a controller will have to explain the reasons for the delay to the ICO at the time of informing them of the breach.

The notification to the ICO shall at least:

1. Describe the nature of the breach including, where possible, the categories and approximate number of personal data records concerned;

2. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

3. Describe the likely consequences of the personal data breach;

4. Describe the measures taken or proposed to be taken by the controller to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

If it is not possible for a controller to give all the above information at the time it notifies the ICO of the breach, then it can provide the information in phases as and when it is able to, provided that it does so without undue delay.

A controller must document any personal data breaches, including the facts relating to the breach, its effects, and any remedial action taken. The documentation should be made available to the ICO at their request so that they can satisfy themselves that the controller is complying with its obligations.

In relation to personal data breaches affecting a processor, a processor is obliged to notify the controller without undue delay after becoming aware of it, rather than notifying the ICO.
Notifying the data subject

If a breach is likely to result in a high risk to the rights and freedoms of individuals, a controller must also notify the data subject without undue delay. A controller must use clear and plain language to explain to the data subject the nature of the breach, and it must also provide at least the same level of information as set out in points 2-4 above.

However, in the following circumstances the obligation on a controller to inform the data subject of a breach will not bite:

1. Where a controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to anyone who isn’t authorised to access it, for example encryption;

2. A controller has taken measures following the breach which mean that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

3. It would involve disproportionate effort for a controller to inform the data subject. In these cases it will be acceptable for a controller to inform the data subject using a public communication or similar measure to issue a blanket notification to multiple data subjects.

The ICO can compel a controller to communicate a breach to data subjects if it feels that there is a high risk to them following a breach.

WP29, Opinion 03/2014 on Personal Data Breach Notification (25 March 2014)

ICO, Notification of data security breaches to the ICO (Version 1.0) (23 July 2012)
Enforcement

Right to lodge a complaint

Every data subject has the right to lodge a complaint with the supervisory authority in the Member State of their habitual residence, place of work or place of alleged infringement of the GDPR. For data subjects in the UK, they would lodge such a complaint with the ICO.

If a complaint is lodged, the ICO (or other supervisory authority) will inform the data subject of the progress and outcome of their complaint, including the possibility of a judicial remedy.

Right to judicial remedy against a supervisory authority

If the ICO (or other supervisory authority) were to make a legally binding decision concerning them, a data subject has the right to an effective judicial remedy against such a decision.

If the ICO (or other supervisory authority) fails to handle a complaint, or does not inform the data subject within three months on the progress or outcome of a complaint, then a data subject will have the right to an effective judicial remedy.

Right to judicial remedy against controllers and processors

A data subject will have the right to a judicial remedy where their rights under the GDPR have been infringed as a result of their data being processed in a non-compliant way.

This goes further than the current framework under the DPA, which only allowed for a judicial remedy against the controller, but not the processor.

Proceedings against a controller or processor are to be brought in the Member State where they have an establishment. However, as long as a controller or processor is not a public authority acting in the exercise of its powers, a data subject can bring proceedings before the courts of the Member State where they live.
**Right of representation**

The GDPR allows data subjects to appoint a not-for-profit body, organisation or association which has statutory authority to represent them and lodge a complaint on their behalf, and, if permitted by law, to exercise rights to recover compensation from controllers or processors on their behalf.

**Right to compensation**

Any person (which includes any individual or organisation) who has suffered damage (whether financial or otherwise, including distress or loss of reputation) as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor. A controller will be liable for damage caused by processing which infringes the GDPR.

A processor will be liable only for damage caused by any processing in breach of its obligations under the GDPR, or where it has acted outside or contrary to a controller’s lawful instructions (which may render it a controller in any case, see Processors becoming controllers).

Where more than one controller or processor are involved in the same processing which gives rise to damages, they will both be held liable for the entire amount. However to the extent that a controller or processor did not cause the breach giving rise to the claim, it may claim back an amount from the other controllers or processors.

Neither a controller nor a processor will be liable to pay damages for infringement if it can prove that it was not in any way responsible for the event giving rise to the damage. However it is unclear whether this would extend to events outside a controller or processor’s reasonable control (so-called ‘force majeure events’) or criminal activity, in each case provided the controller or processor complied with its obligations under the GDPR.

**Administrative fines**

The most headline-grabbing aspect of the GDPR has been the increased level of fines that may be issued by a supervisory authority either together with or as an alternative to other corrective actions. The GDPR provides that a supervisory authority shall impose fines on a case by case basis and that they should be “effective, proportionate and dissuasive.”

Unless Member State law provides otherwise, fines may not be imposed on public authorities and other bodies, only private sector ‘undertakings’.
The GDPR lists a number of factors which a supervisory authority must give “due regard” when deciding whether to impose a fine, including the nature, gravity and duration of the infringement and 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.

There are two levels of fines: a lower level with maximum fines up to €10 million or 2% of global turnover and a higher level with maximum fines up to €20 million or 4% of global turnover. The GDPR lists the infringements that would give rise to the appropriate level of fine.

**Other powers**

The GDPR also gives supervisory authorities a range of other powers which are not dissimilar to those under the DPA. These include the power to:

- request information from a controller or processor;
- undertake data protection audits;
- issue warnings and reprimands;
- order compliance with a request made by a data subject;
- order communications of a personal data breach to a data subject;
- order compliance with the GDPR;
- order the suspension of data transfers outside the EEA;
- impose temporary or permanent restrictions or bans on processing;
- withdraw any certification held by a controller or processor.
Other aspects

Anonymisation and pseudonymisation

Anonymisation is the process of manipulating data so that it cannot, without considerable effort and resources, identify an individual by those data or in combination with other data. If data cannot identify an individual, the GDPR will not apply. Anonymisation is not, however, as easy as it sounds. Both the ICO and WP29 have produced helpful guidance on anonymisation, while the UK Anonymisation Network has produced a more detailed and technical framework.

Pseudonymisation is the process of replacing data that directly identifies an individual with data that indirectly identifies them (a ‘pseudonym’). This is usually a unique identifier such as an alphanumeric string. Pseudonymisation is less rigorous than anonymisation and for that reason, is pseudonymised data is still treated as personal data for the purposes of the GDPR.

The GDPR regularly makes reference to pseudonymisation and acknowledges that the use of such techniques can reduce the risks to data subjects in relation to the processing of their personal data.

Appointment of representatives

Controllers and processors who are not established in the EU (see Territorial scope) must designate a representative in the EU. The representative must be established in the EU member state where the organisation’s data subjects are located, and be a point of contact for the supervisory authority either instead of or as well as the controller or processor itself.

Data Protection Officers

Appointment

In order to harmonise the approach taken by different Member States, the GDPR requires a controller or processor (and in some cases both, in respect of the same processing activity) to appoint a data protection officer (DPO) where:
A practical guide to the General Data Protection Regulation

- the processing is carried out by a public authority or other body (except courts the courts acting in their judicial authority);
- the core activities of the controller or processor consist of processing operations which, by virtue of their nature, scope or purpose, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or processor consist of processing on a large scale special categories of data and data relating to criminal convictions and offences.

The phrases “core activities” and “large scale” are not defined in the GDPR. However guidance issued by WP29 provides that ‘core activities’ means “key operations to achieve the controller’s or processor’s objectives” and ‘large scale’ should be determined on the basis of a number of factors, including the number of data subjects, volume of data, duration of processing activity and geographic extent.

Even where one of the above circumstances does not apply, a controller or processor may or, where required by Member State law shall, designate a DPO.

Where applicable, a controller or processor must publish the contact details of the DPO and also communicate them to the ICO (or other supervisory authority).

Qualifications

The GDPR states that a DPO should be chosen on the basis of their “professional qualities and, in particular, expert knowledge of data protection law and practices.” They must also be capable of fulfilling the tasks required to be undertaken by them.

A DPO may be an employee of an organisation or an external third party providing the services of a DPO.

Role and tasks

The role of a DPO is to promote and monitor compliance with the GDPR by a controller or processor and as a result, to protect the rights and freedoms of data subjects. The GDPR lists the tasks of a DPO as including:

- informing and advising a controller or processor and the employees who carry out processing of their obligations under the GDPR;
- monitoring compliance with the GDPR, any other relevant legal obligations, and with the policies of a controller or processor in relation to the protection of personal data;
- providing advice where requested in relation to Data Protection Impact Assessments and monitoring its performance;
cooperating with supervisory authorities; and

being the point of contact for supervisory authorities on issues relating to processing and, where appropriate, any other matter.

Data protection by design and by default

In addition to the Principles, the GDPR introduces two new concepts which are framed as mandatory obligations on controllers: data protection by design and data protection by default.

‘Data protection by design’ requires a controller to design its systems, policies and procedures in a way that facilitates compliance with the GDPR at the time when it determines how data are to be processed and at the time of the processing itself, rather than as an afterthought.

‘Data protection by default’ requires a controller, in line with the Minimisation principle, to ensure that it only collects personal data that are strictly necessary for each specific purpose of the processing by default. In so doing, a controller must implement “appropriate technical and organisational measures.”

While both obligations require a controller to implement “appropriate technical and organisational measures” to achieve their ends; a controller may take a more risk-based approach in relation to the data protection by design obligation, which permits a controller take “into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of [data subjects].”

In each case, a failure by a controller to comply with these obligations may give rise to a lower level administrative fine (see Administrative fines).

Data Protection Impact Assessments

Where a type of data processing is likely to result in a high risk to the rights and freedoms of a data subject, a controller is obliged to carry out a Data Protection Impact Assessment (DPIA).

The factors which a controller should take into account when considering the level of risk and whether such an assessment is necessary are the type of processing, in particular if new technology is to be used, and the nature, scope, context and purposes of the processing.
Circumstances in which an assessment will be required

In the following circumstances, undertaking a DPIA will be mandatory:

1. where a systematic and extensive evaluation of personal aspects relating to a data subject which is based on automated processing, including profiling, will be used to base decisions about a data subject that will produce legal effects or otherwise will significantly affect them;

2. where there will be processing of special categories of personal data (known as sensitive personal data under the DPA) on a large scale, or there will be processing of personal data relating to criminal convictions and offences; or

3. where there will be a systematic monitoring of a publicly accessible area on a large scale.

There is an obligation placed on the ICO to establish and make public a list of any other processing operations which they consider will require a DPIA. Should they wish to, the GDPR also states that the ICO may establish and make public a list of any processing operations which will not require a DPIA.

When considering what to include on these lists, the ICO should apply the ‘consistency mechanism’ which the GDPR sets out. This is to ensure that the ICO and other supervisory authorities across the EU cooperate with each other. In this context it would mean ensuring that they achieve a consistent approach where processing activities are related to the offering of goods or services or monitoring of behaviour across several member states, or where the free movement of data within the EU could be affected.

Factors covered by a DPIA

A DPIA should contain at least:

1. a systematic description of the proposed processing operation and its purposes including, where being relied upon as the lawful ground for processing, the legitimate interest being pursued by the controller;

2. an assessment of the necessity and proportionality of the processing in relation to the purposes;

3. an assessment of the risks to the rights and freedoms of the data subject; and

4. the measures which are proposed to address the risks and ensure protection of personal data, including safeguards and security measures.
Review against a DPIA

Once a DPIA has been completed, a controller should review whether the relevant processing is being performed in accordance with the DPIA. Such a review should be carried out at least when there is a change to the risk of represented by processing activities.

Codes of conduct and certification

There is a provision of the GDPR which encourages the drawing up of codes of conduct intended to contribute to the proper application of the GDPR. Compliance by controllers and processors with any such codes of conduct which are prepared will be taken into account when assessing the impact of processing operations performed, particularly for the purposes of a DPIA.

A controller should also, where appropriate, seek the views of data subjects or their representatives on the intended processing.

- ICO, Anonymisation: managing data protection risk code of practice
- ICO, Conducting privacy impact assessments code of practice (Version 1.0, 25 February 2014)
- WP29, Draft guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of the GDPR (4 April 2017)
- WP29, Guidelines on Data Protection Officers ('DPOs') (5 April 2017)
- WP29, Opinion 05/2014 on Anonymisation Techniques (10 April 2014)
Achieving compliance

As noted in the Introduction to this Guide, compliance with the GDPR (for the purposes of avoiding enforcement action) should not be an end in and of itself. From increased security to improved customer trust, there are a number of benefits that compliance with the GDPR can bring and focussing on those benefits should make it easier to obtain ‘buy in’ throughout an organisation.

For organisations that already have some form of data protection framework in place, a good starting point is to undertake a gap analysis. Short of undertaking a comprehensive audit, a gap analysis will enable you to identify where your organisation is vulnerable and where you should focus your efforts and your resources. The ICO has produced an online data protection self assessment tool which provides a useful ‘litmus test’ and suggested actions depending on the responses given to a series of questions. A more rigorous gap analysis would involve reviewing existing systems and processes against the requirements of the GDPR outlined in this Guide, perhaps combined with interviewing members of staff and commissioning a review of your organisation’s physical and digital security measures and information management processes.

For organisations that do not already have some form of data protection framework in place, the ICO has produced a simple 12-step checklist for organisations to follow in preparing for the GDPR. It will be important to raise awareness of the GDPR throughout the organisation before undertaking a full audit of its data processing activities. This means going back to basics and asking questions such as:

- What categories personal data do we collect and process?
- How do we process personal data?
- Which lawful basis of processing applies to each category of personal data?
- Do we have clear and up-to-date records of our processing activities?
- Who has access to personal data?
- How would we respond to a request to access personal data?
- Do we have any processors? Do we have written agreements with them?
- Do we have a data processing policy? When was this policy last reviewed?
- Are staff aware of the organisation’s data protection obligations?
- Do we transfer personal data outside the EEA? If so, on what basis?
- How would we identify and report a personal data breach?
- Do we need to appoint a Data Protection Officer?
A practical guide to the General Data Protection Regulation