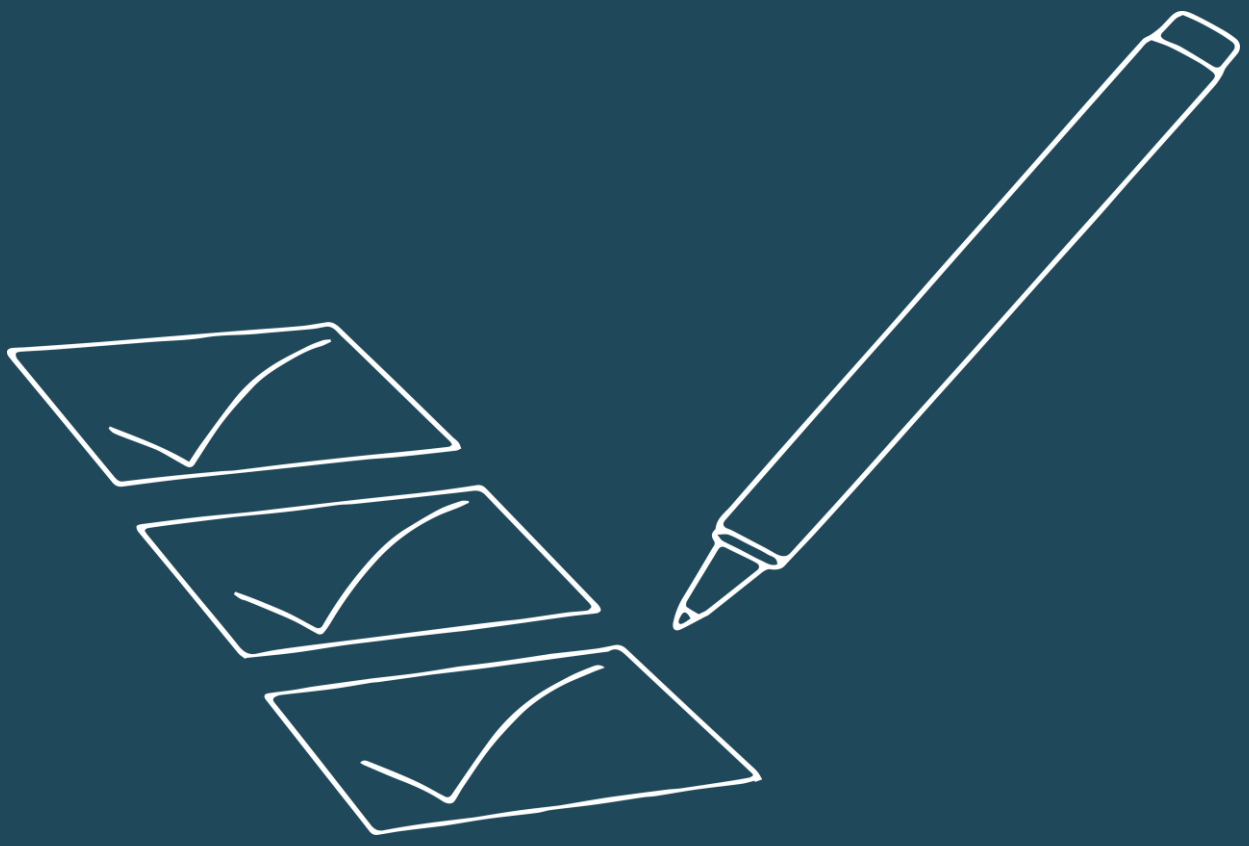
The General Data Protection Regulation

A quick guide



Thomson Snell & Passmore

The General Data Protection Regulation: A quick guide

Executive Summary

The UK government has confirmed that the UK will opt in to the General Data Protection Regulation (GDPR) before it leaves the EU.

The GDPR was adopted on 27 April 2016, and will be coming into force across Europe and the UK on 25 May 2018. It will apply to all data controllers and data processors in the UK and EU, as well as those who operate outside of the EU but who provide goods or services to EU citizens (or monitor their behaviour).

The GDPR is one of the most sweeping pieces of legislation that we have seen for some time, strengthening previous laws and introducing new requirements, such as data portability, the right to be forgotten and notification procedures for data breaches.

The good news is that the GDPR simply strengthens many of the good practices you will have already adopted under the Data Protection Act 1998 (DPA). However, since the GDPR also adds new responsibilities for data controllers and data processors, and new rights for individuals, it is best to get an early start on your transition preparations and identify any gaps in your current practices now.

This Guide provides some background information about the GDPR and practical tips about how to get your organisation ready for the new regime. It is not meant to be a comprehensive paper about all aspects of the Regulation, and we have only covered those areas that are most relevant to our main client base (note that there are certain areas which we have not covered at all, such as new rules for handling children's data). However, we are happy to discuss the full breadth of the Regulation, and how it could impact your business, at any time.

We expect that in the coming months there will be more guidance published by the government, regulators and the courts about complying with the GDPR. We will keep this Guide and our website updated with information that we think may be helpful to you, and we are always available to discuss your questions and concerns.

Joanne Gallagher
Partner/Head of Corporate & Commercial

Nick Hobden
Partner/Head of Employment

Contents

The General Data Protection Regulation: A Quick Guide

1. Principles of processing personal data

Under the GDPR, data controllers are responsible for, and must show compliance with, the following principles:

Personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up-to-date;
- 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; and
- Processed in a manner that ensures adequate security of the personal data using appropriate technical or organisational measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

2. A few definitions

You are a **data controller** if you say how and why personal data is processed. You are a **data processor** if you are the one processing the data on the data controller's behalf. Just because you are a data processor doesn't mean that you do not have data protection obligations! Under the GDPR data processors are subject to direct enforcement by the ICO and compensation claims by data subjects. Also, if you are a data controller you have additional responsibilities under the GDPR to make sure your contracts with data processors comply with the GDPR.

Personal Data is data relating to living individuals (**data subjects**) who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. It need not be confidential data. Personal data includes, among others:

- Names;
- Addresses and other location data;
- IP addresses and other online identifiers;
- Telephone numbers;
- Job titles;
- Salary details;
- Medical details;
- Spending preferences; and
- Dates of birth.

"**Processing**" means 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.

There are also "***special categories of personal data***" or "**sensitive personal data**" that require extra care, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, health data, sex life and sexual orientation data.

The GDPR introduces a new definition, called '**pseudonymisation**' (difficult to spell and pronounce!). Pseudonymisation means the processing of personal data in a way where it can no longer be matched to a specific data subject without additional information, and provided such additional information is kept separately and securely. Pseudonymous data (unlike anonymous data) is not exempt from the GDPR, but it enjoys more favourable treatment under certain provisions of the GDPR.

3. A note on fines

Businesses can incur significant administrative fines for breaching the provisions of the GDPR, and both data controllers and data processors are at risk. These fines are discretionary, and may be in addition to other measures ordered by the supervisory authorities. These fines are meant to be "effective, proportionate and dissuasive".

There are two main levels of administrative fines. A description of these levels, and some examples of triggering breaches, are set out below.

Lower Level: Up to **€10,000,000** or, in the case of an undertaking (e.g. group company), up to 2% of the total worldwide turnover of the preceding financial year, whichever is higher.	**Higher Level**: Up to **€20,000,000** or, in the case of an undertaking, up to 4% of the total worldwide turnover of the preceding financial year, whichever is higher.
Examples: • Breaching the obligations imposed by a monitoring or certification body • Failing to notify in the event of a data or security breach • Not having the necessary technical/organisations measures in place to adequately protect data • Not keeping proper written records of processing activities	Examples: • Breach of a basic processing principle, such as meeting the conditions for consent • Breaching the data transfer restrictions, whether to an international organisation or a recipient in a third country • Breaching the rights of data subjects

Note also that supervisory authorities will have broad investigative and corrective powers under the GDPR, such as the ability to undertake on-site data protection audits, apply temporary or permanent bans on processing activities, suspend data flows overseas, and issue public warnings.

4. Current information & steps to take

4.1 Check of current data

You should document what personal data you hold, where it came from and who you share it with. It may be helpful to do this as part of an information audit, which basically is a process where you take stock of all the information you have (sometimes referred to as data mapping).

As part of your information audit you should:

- Understand the types of personal data held and processed by you and your third party contractors.
- Document your legal basis for processing personal data under the GDPR, and keep a record of this for the future.
- Check to see if there is a record of the consent that was given. This record should specify how and when consent was given.
- Ensure that the data already collected from data subjects has been done in accordance with your data privacy policies, which have been made available to the data subjects.
- Review your security procedures for storing personal data.
- Review whether your current retention periods are appropriate.
- Understand how you destroy personal data.

4.2 Legal bases for processing personal data

There are six legal bases for processing Personal Data (set out in Article 6(1) of GDPR). These are:

- **Consent:** the individual has given you consent to process his/her personal data for one or more purposes.
- **Contracts with the individual:** you need to process personal data for the performance of a contract with the individual, or to take steps (at the individual's request) leading up to such contract. For example, the supply of goods and services, or fulfilling obligations under an employment contract.
- **Compliance with a legal obligation:** if the processing of the personal data for a particular purpose is required by UK or EU law.
- **Vital interests:** if the processing of personal data is required to protect the data subject's life or someone else's life.
- **Public tasks:** you need to process personal data to fulfil your official functions or to perform a task in the public interest. This is likely to be the legal basis for most UK public authorities.
- **Legitimate interests:** if you have a genuine legitimate reason, including commercial benefit, to process the personal data provided that this does not override the interests or fundamental rights and freedoms of the data subject. This means the processing should not have an unwarranted impact on them, and it should still be fair, transparent and require accountability. This is an important basis for the private sector.

There are other bases for processing special category data, such as for employment law, health and social care, and research. These are set out in Article 9(2) of the GDPR.

4.3 Consent

As mentioned above, consent is one of the legal bases that you can rely on to process personal data, but it is by no means the easiest to establish.

Where you already rely on consent that was sought under the DPA or the EC Data Protection Directive (95/46/EC) you will not be required to obtain fresh consent from individuals **IF** the standard of that consent meets the new requirements under the GDPR.

Under the GDPR, consent must be:

> *Freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

In practice, this introduces a much higher compliance standard for obtaining a valid consent from the individual in comparison with the DPA. For this reason, it is inevitable that you will need to review and update how you obtain, record and manage your requests for consent.

What is 'consent' under the GDPR?

To understand how to obtain a valid consent, the Information Commissioner's Office has produced some detailed draft guidance[1] on each of the requirements stated above, which include some helpful practice points:

- **Freely given**
  If the individual is unable to refuse consent without detriment, or if they are unable to withdraw their consent at any time, then the consent has not been 'freely given' and is therefore invalid.

- **Specific and informed**
  - You must identify yourself and, if you are going to share the personal data with any third parties, you must explicitly identify who they are.
  - You will need consent for each purpose and activity of the processing operation.
  - Within your request for consent, provide details on how the individual can withdraw their consent.
  - Be clear about what you are asking for. If your request is vague, sweeping or difficult to understand it will be invalid. Avoid confusing language like double negatives, and inconsistent or technical language (including too much "legalese").

[1] As issued in March 2017. See: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

- **Unambiguous indication – by statement or clear affirmative action**
  The individual must know what they have consented to, and having them confirm they have read general terms and conditions is not enough. There must be a deliberate action by them signifying consent, such as:
  - ticking an opt-in box;
  - signing a consent statement;
  - oral confirmation;
  - choosing from a binary choice presented with equal prominence (e.g. “yes” or “no” boxes); or
  - switching technical settings away from the default.

Failure to opt-out is not consent; you cannot rely on:

- silence;
- inactivity;
- default settings;
- pre-ticked boxes; or
- general terms and conditions.

There is still the potential for implied consent to be valid, but this can be risky and should not extend beyond what is necessary and obvious.

What is explicit consent?

You should note that the GDPR requires ‘explicit consent’ where you are processing sensitive personal data. Although not defined in the GDPR, the ICO suggests this explicit consent must be an express statement confirmed in words versus other affirmative actions, like just ticking a “yes/no” box. Explicit consent can never be implied.

How long does consent last?

This depends upon the context. You will need to review the scope of the original consent and consider the individual’s expectations at that time. Consent won’t continue beyond:

- where your purpose for obtaining the data has expired or changed;
- where your use of the data has changed;
- withdrawal of consent; or
- if parental consent was originally obtained and the child subject comes of age.

Who can give consent?

Consent must be informed. You can assume that adults can give consent, unless you have reasons to believe otherwise.

Children

If your services are aimed directly at children then you must obtain parental consent for processing their data, and you must take reasonable steps to verify that it was the parents who have given consent. The ICO has issued additional guidance on this.[2]

For other types of processing, you should consider the individual child and whether they have competency to give consent. This may be difficult, so instead you could potentially consider another basis for legal processing as described below.

How should you write a consent request?

Don't bundle your consent requests with your general terms and conditions. Make sure your request is clear and that the wording is free from technical or legal jargon. Avoid using vague terms or blanket wording, and if you are obtaining multiple consents (e.g. for a number of purposes) try to use similar methods/mechanisms for each requests.

You should include the following pieces of information:

- the name of your organisation and any third parties who would rely on the consent;
- why you want the data;
- what you will use the data for; and
- confirmation that people can withdraw their consent at any time.

Methods to obtain consent

Where the request for consent is clear, the ICO suggests the following methods would be GDPR compliant indications of the individual's consent:

- signing a consent statement;
- ticking an opt-in box on paper or electronically;
- clicking an opt-in button or link online;
- selecting 'yes' or 'no' options;
- choosing technical settings or preference dashboards settings;
- responding to an email requesting consent;
- answering "yes" orally; and
- filling in optional fields with "just in time" notices (these appear on-screen at the point the person inputs data, with a brief message about what the data will be used for).

The following would not constitute valid consent:

- silence;
- inactivity; and
- pre-ticked boxes or opt-out boxes.

[2] https://ico.org.uk/about-the-ico/consultations/children-and-the-gdpr-guidance

How should you record and consent?

You need to keep an audit trail of how you obtained consent. If audited, you may be asked to provide the following information:

- who consented;
- when they consented;
- what they were told;
- how they consented; and
- whether they have withdrawn their consent.

Once you have obtained consent, your use of the personal information should be reviewed regularly to ensure you are still using it for the intended purpose. If not, you will need to request new consent.

The right to withdraw

In your request for consent, you must include information about how individuals can withdraw their consent. They must be able to withdraw consent without suffering detriment, and it must be as easy to withdraw consent as it is to give it. It should be easily accessible and a one-step process. Upon receipt of the withdrawal of consent, you should stop processing the data immediately.

When is consent inappropriate

Consent isn't the appropriate basis for processing if you cannot offer individuals a genuine choice over how you use their data. These include situations where:

- **You would still process the data on a different lawful basis if consent was refused or withdrawn**. In essence, this would be a false choice, and as the ICO states this would present "only the illusion of control". Instead, you should identify the correct legal basis from the start.
- **You ask for consent to the processing as a precondition of accessing the services**. This may not count as valid consent. If you believe that processing is necessary for the services, then you can rely on the alternative legal basis of "processing is necessary for the performance of the contract". The ICO warns that if processing is a condition of service, but not actually necessary for that service, then consent would be presumed to be invalid.
- **You are in a position of power over the individual**. If someone feels they have no choice but to agree because they fear the consequences of saying "no", then this is not a true choice and will not be valid consent. This is a particular concern for public authorities and employers, and they may need to rely on other bases, e.g. "performance or a public task" and "legitimate interests".

If you have difficulty meeting the standard for consent, stop and ask yourself whether consent is actually the most appropriate basis of processing!

Don't forget about the PECR!

You must still comply with the Privacy and Electronic Communications Regulations (PECR) which have additional consent requirements for electronic communications.

5. Accountability & governance

5.1 Records and processing activities

All organisations subject to the GDPR must provide comprehensive, clear and transparent privacy notices to individuals. Some of the requirements for these privacy notices can be found in the "right to be informed" section below. **Tip: do not bury these policies on your website. Make them easy to find and easy to understand, and also make sure they are kept up-to-date.**

If your organisation has more than 250 employees, you must also keep internal records of your processing activities, and these records may be requested by a supervisory authority during an investigation. These records should memorialise:

- Name and details of your organisation;
- Purposes of the processing;
- Description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Details of transfers to other countries including documentation of the transfer mechanism safeguards in place;
- Retention schedules; and
- Description of technical and organisation security measures.

Also, if your organisation has less than 250 employees, it is still a good idea to keep the above records.

Note that organisations of ANY SIZE are required to maintain records of activities related to: (1) higher risk processing such as those relating to special categories of data (sensitive personal data); (2) those that could jeopardise the rights and liberty of individuals; or (3) processing that is "not occasional".

5.2 Data protection officer

Does everyone need a DPO?

If you are a public authority/body, have core activities that require carrying out large scale systematic monitoring[3] of individuals (e.g. private security companies carrying out surveillance in public spaces), or have core activities that require carrying out large scale processing of special categories of data (e.g. a hospital's use of patient data) or data relating to criminal convictions or offences, then you must appoint a Data Protection Officer (DPO). This applies to both data controllers and data processors.

[3] Examples of "systematic monitoring" given in the ICO's Guidance Notes include: operating telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment such as credit scoring, fraud prevention and detection of money laundering; location tracking; loyalty programs, behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices (e.g. smart meters, smart cars, home automation, etc.).

Even if you are not obliged to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to comply with your obligations under the GDPR. In view of this, you may find it easier to simply appoint a DPO even if not required or at least have a data coordinator in charge of your compliance efforts. DPOs are not personally responsible for non-compliance with the GDPR. This remains the responsibility of the data controller or data processor.

Role of the DPO

The DPO must:

- Be able to perform the role of DPO independently. The DPO must not have other duties that will conflict with the role of DPO – for example, the DPO cannot have a position where he/she decides how the organisation processes personal data. The ICO's Guidance Notes indicate that conflicting positions may include senior management positions such as the CEO, COO, CFO, Chief Medical Officer, Head of Marketing, Head of HR, and Head of IT), but could also include less senior roles depending on their level of decision making about determining purposes and means of processing personal data.
- However, you can allocate the role of DPO to an existing employee as long as the professional duties of such employee are compatible with those of the DPO. You can also choose to engage an external DPO as a consultant, for example;
- Be comfortable reporting to the highest management level (i.e. the Board or similar);
- Be the first point of contact for supervisory authorities and data subjects (note that you will be required to publish the contact details, but not necessarily the name, of the DPO to ensure data subjects and supervisory authorities can easily, directly and confidentially contact the DPO);
- Have professional experience and expert knowledge of data protection law and practices (with level of expertise to be appropriate for the sensitivity, complexity and amount of data an organisation processes). No specific credentials are necessary, but the DPO will be required to keep up-to-date on the obligations to comply with the GDPR and other data protection laws, and keep the organisation and other employees informed; and
- Monitor compliance with data protection laws, including managing data protection activities, provide advice on data protection impact assessments, conduct internal audits and train other staff.

Resources for DPO

The amount of resources required to support the DPO depends on the level of complexity and/or sensitivity of the business's processing operations. Resources include:

- Active support of the DPO function by senior management;
- Sufficient time for DPO's to fulfil their duties. If the DPO will be balancing his/her DPO duties with other duties, then a percentage of time should be allocated for the DPO-specific duties, potentially with a work plan put in place;
- Sufficient financial resources, infrastructure and staff;
- Official communication of the designation of DPO to all staff;
- Necessary access to other services so that the DPO can receive essential support (e.g. from HR, IT, Legal, etc.)
- Continuous training; and
- Potential for a DPO team, if appropriate.

For additional information, please see the DPO guidance issued by EU data protection regulators (**Guidance Notes**): http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

5.3 Code of conduct

Check to see if there is a code of conduct or certification scheme that covers your processing activity, and work towards it as a way of demonstrating compliance. If you sign up to a Code of Practice, you will be subject to mandatory monitoring by the accredited body. Non compliance with the standards of a scheme you have signed up to may result in a fine (up to €10million or 2% of global annual turnover).

5.4 Third parties and outsourcing

If any data processing is outsourced (e.g. payroll administration, internet service providers) you must ensure the third party provider complies with data protection laws.

You (the data controller) must enter into a written contract with the processor which requires the data processor to act only on your instructions, limits the use of the personal data and imposes security measures equivalent to those which the data controller itself is required to implement. Among other requirements, the contract must include:

- A description of the subject matter;
- Duration of the processing;
- Nature and purpose of the processing;
- Types of personal data and categories of data subjects; and
- The obligations and rights of the Data Controller.

Article 28(3) sets out a detailed list of other terms that must be included in the contract.

5.5 Transferring data outside the European Economic Area (EEA)

You may transfer personal data to a non-EEA country (a "third country") or international organisation if: the commission has decided that that organisation, country, territory or sector ensures adequate levels of protection of personal data through its domestic law or international commitments **(an adequacy decision)**; (ii) you have ensured the organisation has **adequate safeguards** in places; or (iii) derogation is permitted by the GDPR.

Firstly, check to see whether the Commission has made an adequacy decision that covers your proposed transfer.[4] If an adequacy decision has not been made (or if it has, but you wish to have additional protection in place), then you should ensure that the organisation receiving the data has adequate safeguards in place. You must also ensure that individuals' rights are enforceable and there are effective legal remedies. Adequate safeguards for transferring data to organisations outside the EU include the following:

[4] See https://ec.europa.eu/info/law/law-topic/data-protection_en

- The organisation uses approved model data protection clauses, such as those published by the European Commission;
- Multinational groups of companies can transfer data internally on the basis of ICO-approved BCRs (**Binding Corporate Rules**). BCRs have been officially recognised under the GDPR; or
- The organisation receiving the data complies with a code of conduct approved by a supervisory authority or is certified under an approved mechanism.

If you wish to transfer data to an organisation which is not subject to an adequacy decision or does not have suitable approved safeguards, you should consider whether the GDPR allows a special exception (a derogation) in that specific situation. The GDPR provides derogations from the general prohibition on transfers of personal data for certain situations. These derogations include (for bodies other than public authorities), transfers that are:

- Made with the individual's informed consent;
- Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- Necessary for the performance of a contract made in the interests of the individual between the controller and another person;

And, for all organisations, including public bodies, transfers that are:

- Necessary for important reasons of public interest;
- Necessary for the establishment, exercise or defence of legal claims;
- Necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- Made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

If derogation is permitted, you should require the organisation to put safeguards in place to ensure that the data is protected. If derogation is not permitted, transfer can only take place in very limited circumstances as described in Article 49, having informed both the supervising authority and the data subject.

5.6 Data Protection Impact Assessment

Data Protection Impact Assessments, also known Privacy Impact Assessments **(PIAs),** are tools that help organisations find the best way to comply with their data protection obligations. PIAs were not required (but were encouraged by the ICO as part of "privacy by design") under the DPA, and the ICO has some useful guidance for how to create and conduct a PIA. A template PIA can be found at annex two of the ICO guidance.

Under the GDPR, you are required to carry out PIAs when using new technologies or when data processing is likely to result in a high risk to individual's rights and freedoms. Examples of "high risk" processing include:

- Systematic and extensive processing activities, including profiling, that intend to initiate a course of action that will have significant effects on individuals;
- Large scale processing of sensitive personal data or personal data relating to criminal convictions or offences.
- Large scale, systematic monitoring of public areas (such as CCTV recordings);
- Data sharing initiatives where two or more organisations seek to pool or link sets of personal data; and
- Using new databases which consolidate information held by separate parts of an organisation.

Before beginning any of the above, you should carry out a PIA and keep a record of it. It should address questions such as:

1. **What is the activity meant to achieve?** Have clear objectives, ascertain what data needs to be processed or shared with whom and record these considerations. As part of this, you should record the processing operations envisaged and purposes of the processing or sharing, including records of any legitimate interests.

2. **What risks does the activity pose?** Consider whether an individual would be harmed? Would an individual object to the processing? Would sharing or processing that data undermine an individual's trust in the organisation? You must asses the risks to the rights and freedoms of data subjects, and document the measures you are taking to address those risks.

3. **Could the objective be achieved without sharing or processing personal data?** Personal data should never be shared when the objective can be met by alternative means, for example, by providing anonymised or statistical data. You are required to assess the necessity and proportionality of the processing operation in relation to the purposes.

5.7 Breach notification

A **data breach** is "a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data." There are tight timescales for reporting a data breach, and so it is important that you have a robust internal procedure in place covering the detection, investigation and reporting of breaches.

You have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to individuals' rights and freedoms (e.g. potential reputational damage, financial loss, discrimination, loss of confidentiality, etc.). This must be done without "undue delay" and, where feasible, within 72 hours of your organisation becoming aware of the breach, and the GDPR sets out a list of information that must be included in the notification (Article 33(3)). Due to this tight timescale, the DPO should ensure that members of staff are able to identify when a breach requires notification, and the procedures that should be followed.

If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, then you must also inform the relevant data subjects of the breach without undue delay, subject to certain exceptions set out in Article 34.

Failure to notify a breach when required to do so can result in a fine (up to €10million or 2% of global annual turnover).

6. Compliance with individuals' rights

Individuals have a number of continuing rights to their data under the GDPR, including:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling.

A short explanation of each of these rights, and how you they affect you, are set out below.

6.1 The right to be informed

You must provide fair processing information to individuals. If you rely on your privacy notice to provide the required information, make sure it is up-to-date at the time you obtain the relevant personal data from the individual.

Your data privacy notice should provide (Article 13):

- The identity and contact details of the data controller (and where applicable, the controller's representative) and the data protection officer;
- Purpose of the processing and the legal basis for the processing;
- The legitimate interests of the controller or third party, where applicable;
- Any recipient or categories of recipients of the personal data;
- Details of intended transfers to third countries, and safeguards;
- Retention period or criteria used to determine the retention period;
- The existence of each of data subject's rights;

- The right to withdraw consent at any time, where relevant and details of how to do so;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement to enter into a contract, and possible consequences of failing to provide such personal data;
- The right to lodge a complaint with a supervisory authority and details of how to do so;
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences; and
- Categories of personal data.

If you obtain certain personal data indirectly (not from the data subject itself), then you will also need to notify the data subject about the type of information you hold and how you intend to use it. The requirements are largely similar to those above, but there are additional obligations as well such as describing the categories of personal data concerned and the sources of such information (see Article 14 of GDPR for details).

You should provide your data privacy notice (or other documentation including the above information):

- If obtaining data directly from the data subject, at the time the data are obtained; or
- If obtaining data in any other way:
  - If the data is used to communicate with the individual, at the latest, when the first communication takes place; or
  - If disclosure to another recipient is envisaged, at the latest before the data are disclosed.
  - In any event, within one month of obtaining the data.
- If you intend to further process personal data for a new purpose you must provide the data subject with information about that new purpose (and any other relevant information) *before* you begin any further processing.

6.2 The right of access

Under the GDPR, individuals have the right to obtain (usually free of charge):

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information (e.g. as described in the privacy policy section, above).

You should prepare a standard procedure to deal with such subject access requests, and for larger companies perhaps consider implementing an online system for data subjects to submit requests and receive information.

Subject access requests are frequently used by former employees to obtain information, so it is helpful for HR personnel to be familiar with the requirements in this respect.

There are strict timelines for responding to requests. The response should usually be within one month of your receipt of the request, although in some circumstances this can be extended by two months. It may be helpful to input any deadlines on a central system to ensure that these deadlines are not missed.

Individuals should be informed (with reasons) if you decline their request or if you intend to extend the deadline.

6.3 The right of rectification / erasure

Individuals have the right to have their personal data rectified if it is inaccurate or incomplete. Individuals also have a new "right to be forgotten" under the GDPR and may have their information erased if there is no compelling reason for its continued processing. You must respond to a request for rectification in one month, which can be extended by two months in the event of a complex rectification request. The right to erasure is more complicated. There are certain criteria that need to be met in order for a legitimate request for erasure to be made, and there are certain bases for refusal. You should investigate these with your DPO.

Irrespective of whether a data subject requests rectification or erasure, you should have review procedures in place to determine whether you should erase or restrict the processing of data.

You should identify when personal data is no longer necessary in relation to the purpose it was initially collected/processed and take steps to either erase the data or, alternatively, to restrict the data if the individual opposes the erasure of data or requires the data to establish, exercise or defend a legal claim.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, or its erasure, unless it is impossible or involves disproportionate effort to do so. If you lift a restriction on processing, you should inform the individuals.

6.4 The right to restrict processing

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data but cannot process it further. You can retain just enough information about the individual to ensure that the restriction is respected in future.

You will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or for the purposes of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual;
- When processing is unlawful and the individual opposes erasure and requests restriction instead; and
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You should review your internal procedures to ensure that you can restrict the processing of personal data as above, if required.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

6.5 The right to data portability

This is a new right under the GDPR, which provides individuals with the right to obtain and use their personal data across different services. In order to fulfil this obligation and to assist other organisations who will use the data, you should provide personal data in a structured, commonly used and machine readable form.

You should respond to a data portability request within one month, which can be extended by two months in the event of complex or numerous requests. You may be required to transmit data directly to another organisation, if this is technically feasible.

You should consider whether the data requested concerns more than one individual and, if it does, whether providing the data would prejudice the rights of any other individual. If you decide not to take action in response to a request, you must explain why to the individual and inform them of their right to complain.

The right to data portability only applies to personal data the individual has provided to the data controller:

- Where the processing is based on the individual's consent or for the performance of a contract; or
- When processing is carried out by automated means.

6.6 The right to object

Individuals have a right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

You should inform the data subject of their right to object in your privacy notice and at the first point of communication. You should make this information explicit and separate to other information. It should be brought to the attention of the data subject. If your processing activities are carried out online, you must offer individuals a way to object online. How you respond to an objection will depend on why you are processing the personal data.

For direct marketing purposes: You must stop processing the personal data as soon as you receive an objection.

For research purposes: Individuals must have grounds relating to their particular situation in order to object to data processing. Where the processing of data is necessary for a public interest task, you are not required to comply with an objection to processing.

For the performance of a legal task or your organisation's legitimate interests: Individuals must have grounds relating to their particular situation in order to object to data processing. You must comply with the objection unless you can either (a) demonstrate compelling legitimate grounds for processing, which override the interests, rights and freedoms of the individual; or (b) the processing is for the establishment, exercise or defence of legal claims.

6.7 Rights in relation to automated decision making and profiling

You must ensure that individuals are able to (i) obtain information about the logic involved in any automated decisions, (ii) obtain human intervention, (iii) express their point of view, and (iv) obtain an explanation of the decision and challenge it. Individuals have a right not to be subject to a decision based on automated processing where it produces a legal effect or a similarly significant effect on the individual unless:

- The decision is necessary for entering into or performance of a contract between you and the individual;
- The decision is authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or
- The decision is based on explicit consent.

In view of all these individuals' rights, consider whether there are steps you can take to tailor your technical and organisation processes to meet your data protection obligations. For example:

- Consider implementing an online self-service system where data subjects can securely access their data and submit requests for rectification, erasure and portability or any objections and be updated as to the progress of any such request or objection. If you obtain data electronically, you are obliged to implement a way in which data subjects can object etc. electronically.
- Ensure that when you rectify, erase or restrict data any third parties to whom you have disclosed the data to are informed.
- If your data is obtained off-line, you should also ensure there is an off-line process by which data subjects can request access to their data, rectification, erasure and portability or any objections and be updated as to the progress of any such request or objection, and for verifying the identity of the individuals making such requests.

Pulling it all together - checklist

Have you:

- ✓ Conducted an information audit?
- ✓ Identified any gaps between your current data protection practices and the new requirements, and developed plans to address these?
- ✓ Updated your privacy policies?
- ✓ Confirmed that you have records of all relevant processing activities?
- ✓ Conducted privacy impact assessments for high risk processing activities?
- ✓ Appointed a data protection officer (if required) and ensured the DPO will have adequate resources to perform his/her role?
- ✓ Checked your third party contracts to ensure adequate safeguards have been included to protect personal data and, if not, have a plan in place to amend these?
- ✓ Tracked your data flows (including intragroup) to understand what data is being shared with what organisations, and where?
- ✓ Confirmed whether non-EU transfers of personal data are being made in accordance with GDPR?
- ✓ Developed an internal breach procedure for the detection, investigate and reporting of breaches?
- ✓ Updated internal procedures to ensure compliance with data subjects' rights?
- ✓ Have plans in place to train staff on the new Regulation and the importance of data protection to your business?

Glossary of legal terms

Consent

Freely given, specific, informed statement that agrees to the processing of their personal data.

Personal data

Any information related to a person or 'Data Subject' that can be used to identify the person.

Data subject

A natural person whose personal data is processed by a controller or processor.

Genetic data

Data concerning the characteristics of an individual which give unique information about the health or physiology of the individual.

Biometric data

Any personal data relating to the physical, physiological, or behavioural characteristics of an individual which allows their identification.

Right to be forgotten

Also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Subject access right

Also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

Processing

Any operation performed on personal data, whether or not by automated means, including collection, use, recording etc.

Data portability

This is the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Personal data breach

A breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data.

Privacy by design

A principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

Data protection officer

An expert on data privacy who works independently to make sure organisations are adhering to the GDPR.

Data controller

The entity that determines the purposes, conditions and ways in which we process personal data.

Data processor

The entity that processes data on behalf of the Data controller.

Contact us

For further information please speak to your usual contact from our Corporate & Commercial team, or contact Joanne Gallagher using the details below.

Joanne Gallagher
Partner and Head of Department
Corporate & Commercial
01322 623708
joanne.gallagher@ts-p.co.uk

Where we are based:

Tunbridge Wells
Heathervale House
2-4 Vale Avenue
Tunbridge Wells
Kent TN1 1DJ

Thames Gateway
Corinthian House
Galleon Boulevard
Crossways Business Park
Dartford
Kent DA2 6QE

@pragmaticlawyer

Last updated February 2018.

Thomson Snell & Passmore