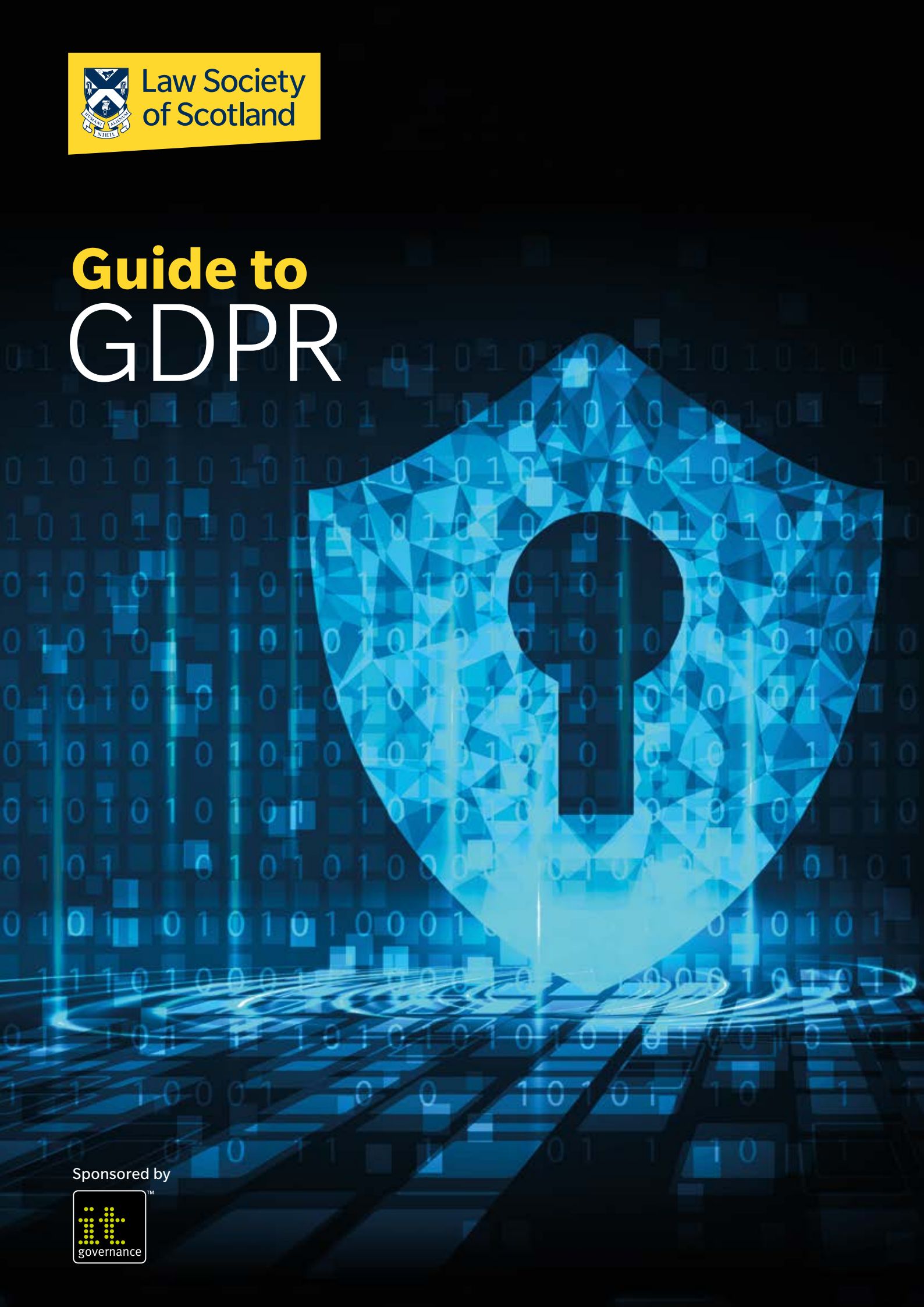
Law Society of Scotland

Guide to GDPR



Sponsored by

IT governance™

Index

Introduction

Law firms have to comply with the General Data Protection Regulation, just like all other organisations that process personal data.

We have produced this GDPR guide specifically for law firms. While they are not Law Society rules, we thought it would be helpful to look at the regulation and the Data Protection Act from the perspective of a legal practice. The Act is still in draft form at the time of writing but we wanted to provide guidance in advance of 25 May 2018 and will disseminate any updates required should the provisions or guidance in relation to those provisions change. For example, the Information Commissioner's Office (ICO) has not issued any guidance in relation to the legal professional privilege exemption referred to throughout this guide. You should check the ICO guidance when it is published. The exemption is similar to the exemption under the Data Protection Act 1998, but not quite the same.

Part of this guide includes a data audit we carried out with a high street firm to look at its data processing. Many high street firms will recognise the information gathered in the audit and can use it to evaluate their own data processes.

In many instances, it is left to each firm to determine how to comply depending on the nature and volume of work undertaken. On that basis, this guide is for information only; the tables and templates are illustrative and should be amended to take account of your firm's unique circumstances.

Responsibility for regulating GDPR lies with the ICO, not the Law Society of Scotland.

April 2018

GDPR ten steps

	Step	Detail	Relevant section headings *(from the guide)*
1	**Register with the Information Commissioner's Office (ICO)**	Your firm is a data controller and must be registered with the ICO. From 25 May 2018, data controllers will require to pay a data protection fee.	• Law firms as data controllers
2	**Audit your data processing**	Map out how you process your clients' personal data from the moment it comes into your office through to storage and file destruction. Don't forget to map the personal data of your staff. In the guide, we show what a data audit of a high street firm might look like. You are required to keep a record of certain data processing activities and this audit will provide you with the information that needs to be recorded and which is required to meet other GDPR obligations.	• What counts as personal data • Create a record of data processing • High street case study • Marketing
3	**Identify all the third parties you share data with**	You must have a GDPR-compliant contract in place with data processors and appropriate arrangements in place with other controllers. You may wish to have arrangements with other organisations that you pass personal data to in relation to security and retention.	• Sharing and transferring personal data to third parties
4	**Create a data retention policy**	You can only store data for as long as it is necessary for the purpose for which it was processed.	• Data retention
5	**Have a written data protection policy**	Your data protection policy sets out your approach to data protection and privacy.	• See template on Law Society website
6	**Create new privacy policies for data processing**	There is now an obligation to provide anyone whose personal data you process with a lot more information about how you handle their data.	• Data protection principles • Lawful processing • Fair processing information/ privacy policies • Confidentiality and limited exemptions

	Step	Detail	Relevant section headings *(from the guide)*
7	**Have a written process for dealing with data subject requests, including subject access requests**	You must have a policy detailing how you will deal with requests from clients (and employees/ex-employees) regarding the information that you hold about them. Individuals also have the right to ask for their personal data to be erased in certain circumstances. This can be included in your data protection policy.	• Clients and third parties – subject access requests • Confidentiality and limited exemptions
8	**Have a process and written guidance for what to do in the event of a personal data breach – this could include a cyber-attack or loss of paper files**	Have in place a written process to set out what to do in the event of a breach and who is responsible for reporting to the ICO/data subject. Ensure that all staff can identify a data breach and are aware of who to inform.	• Reporting personal data breaches
9	**Review your approach to marketing to ensure it is GDPR compliant**	This is regulated by the Privacy and Electronic Marketing Regulations, which tell us consent is generally required for marketing to individuals and sole traders but not business contacts. You may be able to use the soft opt-in for clients.	• Marketing • Consent (appendix 1) • Fair and transparent processing
10	**Train your staff**	It is crucial that everyone in your firm who handles client data understands and adheres to your policies for handling personal data. Arrange training to ensure that they are up to speed.	• Data protection policy (on website) • Data subject rights (data protection policy) • Requests for client personal data • Reporting personal data breaches

Law firms as data controllers

Law firms are data controllers in relation to the personal data they hold for their employees and clients. This guide will deal mainly with the relationship that law firms have with their clients, who are data subjects.

The data controller can be an individual (for example, a sole practitioner).

All data controllers are currently required to register with the Information Commissioner's Office (ICO) and from 25 May 2018, all data controllers are required to pay an annual data protection fee. This won't be due until your current notification runs out. The level of fee will depend on which tier your organisation fits into:

- Tier 1 – micro organisations – identified as having a maximum turnover of £632,000 for the financial year or no more than ten members of staff. The fee is £40.
- Tier 2 – small and medium organisations – identified as having a maximum turnover of £36 million for the financial year or no more than 250 members of staff. The fee is £60.
- Tier 3 – large organisations – if your organisation does not fall into the above categories then the fee is £2,900.

Failing to pay the fee/the correct level could result in the ICO taking enforcement action, including imposing an administrative fine of up to £4,350.

Data Controller (Art 4(7))
The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data.

Data Subject (Art 4(1))
An identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Data Processor (Art 4(8))
A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Employees of a law firm process data on behalf of the data controller but are not, as an individual, a data controller or a data processor.

Processing data covers the gathering, storing, accessing, sharing and deleting of personal data. It is a very broad term.

Processing (Art 4(2))
Any operation or set of operations which is performed upon personal data or 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, erasure or destruction.

What counts as personal data?

Personal data is information stored digitally or in a paper file from which an individual can be identified or is identifiable. It includes information that can be used to inform a decision that you might take about an individual. It includes:

- Name
- Contact details
- Photographic images
- CCTV footage
- Passport number and copies of passport
- Bank account details
- Meeting notes

Personal data (Art 4(1))
Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Information about clients which are corporate entities is not regulated by the GDPR, although information about their employees is.

Special category data
There is a sub-category of personal data called special category data (previously known as sensitive personal data) which includes the following:

- Data revealing racial or ethnic origin
- Data revealing political opinions
- Data revealing religious or philosophical beliefs
- Data revealing trade union membership
- The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- Data concerning health, including physical or mental health of an individual and the provision of health services
- Data concerning a natural person's sex life or sexual orientation

Criminal conviction and offence data is dealt with separately under the GDPR. This includes the alleged commission of offences or proceedings for an offence which includes disposal and sentence. The provisions and restrictions are essentially the same but will be found in the new Data Protection Act. In this guide when special category data is referred to, it will include criminal conviction and offence data.

Case study

Our high street law firm has taken steps to register with the ICO. As a data controller, the firm is aware of the types of personal data that it is processing. It is also aware that it holds some special category data.

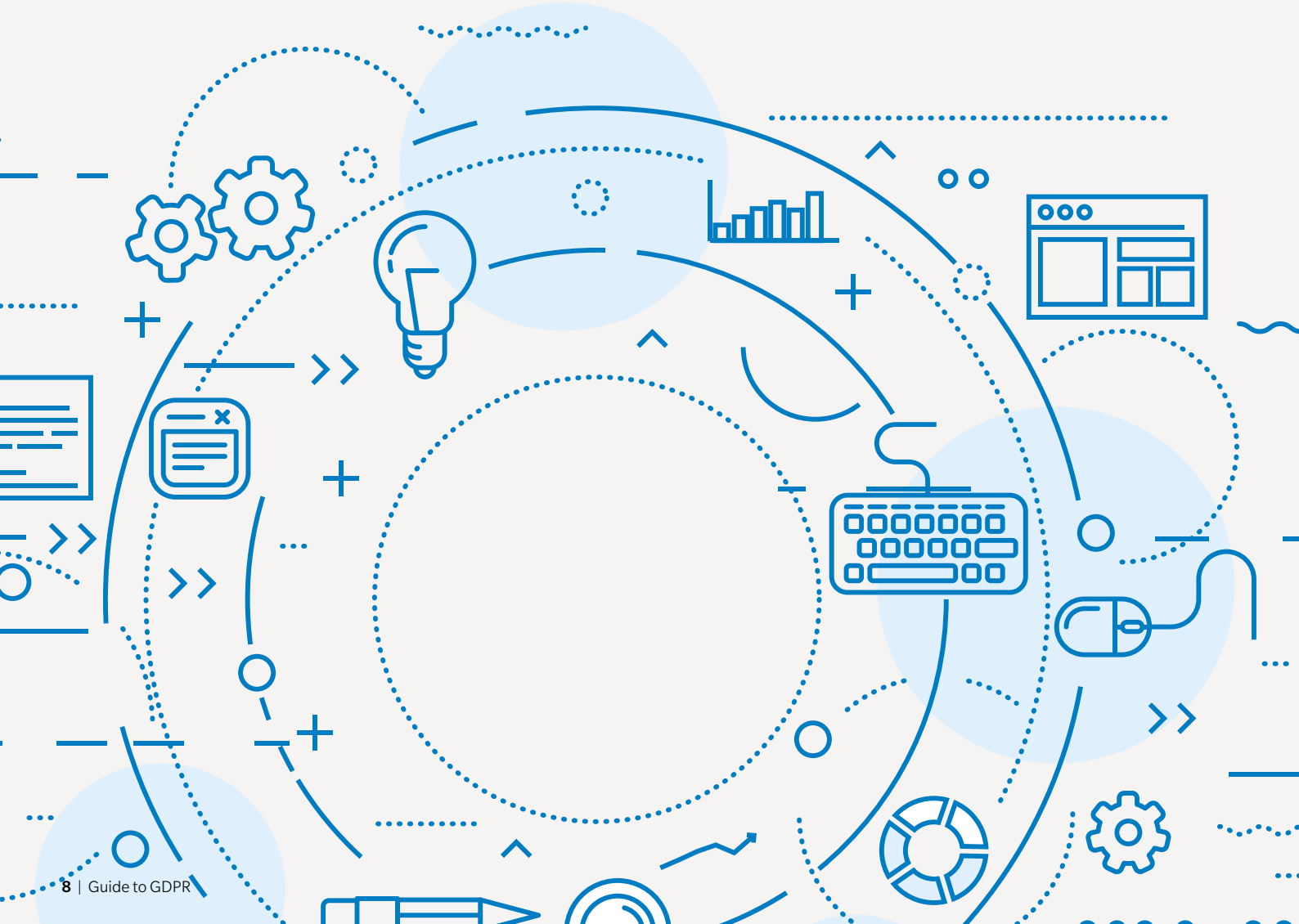
Create a record of your data processing

All law firms should know what personal data they are processing and why, and be able to identify what is happening to it. This includes who it is being shared with, including the location of the cloud server storing your data.

All firms need to decide how long they will retain personal data and what security measures they have in place when it is being stored or when it is being sent out of the organisation, depending on the risks inherent in the processing of that data. For example, more care should be taken over special category data and financial data, which can easily be used to harm or cause distress to individuals.

Solicitors are generally very aware of client confidentiality but the GDPR requires the processes to be documented, and working out what personal data you are processing is essential to even begin to do this effectively.

Go to www.ico.org.uk and see the section on GDPR/documentation for more information.



Record of processing

All data controllers must maintain a record of processing activities under their responsibility. Most law firms will be required to do this, although the GDPR limits this obligation for smaller firms.

Organisations with 250 employees or more must record the information set out below about all the personal data processing activities they carry out.

If you have fewer than 250 employees, you are only required to record this information about certain processing activities as listed here:

- Processing you carry out which is likely to result in a risk to the rights and freedoms of data subjects, or
- Processing which is not occasional, or
- Processing which includes special categories of data

For law firms, processing the personal data of clients is likely to involve risks, and it is not occasional. Similarly, processing the personal data of employees is not occasional.

You must record the following information:

- Name and details of your organisation (and, where applicable, of joint controllers, your representative and data protection officer)
- Purposes of the processing (and we suggest recording the legal basis too)
- Description of the categories of data subjects and categories of personal data
- Categories of recipients to whom personal data will be disclosed
- Details of transfers to third countries and international organisations, including documentation of the transfer mechanism safeguards in place
- Time limits for erasure of personal data where possible
- A general description of technical and organisational security measures where possible

Even if you don't have 250 employees or feel your processing is occasional, it is important to work out what data you are processing so that you can comply with the other GDPR obligations. As already pointed out, much of the processing will require to be recorded anyway and so we recommend that a record of all your data processing is maintained and updated to ensure that your risk is kept to a minimum and to ensure that data protection accountability is built into the organisation's processes and procedures.

You may be required to make these records available to the ICO, but they do not require to be made public.

Case study

Our high street law firm does not have 250 employees but, does carry out processing which is 'not occasional' and includes some special category data. On that basis, our law firm has created a record of data processing based on the data audit which it carried out.

The audit

Examples of information required for your record of data processing

Our high street firm has audited the data flows in its areas of work. Below is a record of the information that we gathered based on conveyancing, court work and executries.

Conveyancing – house purchases and data of clients

Category of Data	How do you get the data?	Purpose and Legal Basis	Potential Recipients	Where is the data stored?	Notes
Information about the client					
Name, address and contact details of client	• Through website • From client	Necessary to provide the legal services associated with purchasing a house (Article 6b)	• Conveyancing department • Property centre • Seller's solicitor • Photographer • Planner • Person who puts up the 'For Sale' sign • Surveyors • Viewing assistant	• Document management system • Paper file • On mobile phone • Software provider • IT system support	This information can be passed to many different parties. You do not require consent for this processing but clients should be told that this processing will take place in case they have concerns. For example, the purchaser may not want the seller to know their address. How do you secure your phone to ensure personal data can be deleted if lost/stolen?
National insurance number	• From client	Only necessary for Revenue Scotland if LBTT being paid (Article 6c)	• Revenue Scotland	• Document management system • Paper file	If the NI number is not required, then you should not collect and store it.
Identification documentation	• From client	Necessary to carry out AML checks as required by law (Article 6c)	• Receptionist • AML partner	• Document management system • Paper file	Consider whether this documentation requires to be stored on both the paper file and the system.
Bank details for client	• From client	To carry out financial transactions as part of service (Article 6b)	• Conveyancing department • Cash room • Financial adviser	• Document management system • Paper file	Consider security and who has access to these details and who can change them.
Information in missives	• From client • Financial adviser	Necessary to carry out conveyancing (Article 6b)	• Conveyancing department • Seller's solicitor	• Document management system • Paper file	
Information about others					
Information about source of funds from client, including bank statements or other financial documentation	• From client	Necessary to ensure compliance with the law (Article 6c)	• Conveyancing department	• Document management system • Paper file	
Information about source of funds from third party, including bank statements or other financial documentation	• From client and/ or third party	Necessary to ensure compliance with the law (Article 6c)	• Conveyancing department	• Document management system • Paper file	If you are processing information about a third party, then you need to provide them with a fair processing notice.
Information in standard security	• Client • Bank	To facilitate any mortgage used to purchase house (Article 6b)	• Conveyancing department • Mortgage provider • Registers of Scotland	• Document management system • Paper file	

Court work – family law case

Category of Data	How do you get the data?	Purpose and Legal Basis	Potential Recipients	Where is the data stored?	Notes
Information about the client					
Name, address and contact details of client	• Online • From client	Necessary to provide legal advice and representation (Article 6b)	• Court department • Solicitor for the other party/parties • Court • Expert witnesses and advisers • Court-appointed reporters • Scottish Legal Aid Board	• Document management system • Software provider • IT system support • Paper files • On mobile phone	This information can be passed to many different parties. You do not require consent for this processing but clients should be told that this processing will take place in case they have concerns. For example, one party may not want the other party to find out their address. How do you secure your phone to ensure personal data can be deleted if lost/stolen?
More personal information about the client's life/marital status/health/criminal convictions etc and that of the other parties involved, which could include information about former partners and children	• From client in person or via phone calls and emails • From other party's solicitor in person, via phone and email	Necessary to provide legal advice and representation (Article 6b and 9f)	• Court department • Solicitor for the other party/parties • Court • Expert witnesses and advisers • Court-appointed reporters • Party litigants • Scottish Legal Aid Board	• Document management system • Handwritten notes on paper and typed-up notes • Paper file	Consider the security of emails being used to transfer personal data and special category personal data without encryption or other security measures.
Identification documentation	• From client	Necessary to carry out AML checks as required by law (Article 6c)	• Receptionist • AML partner	• Document management system • Paper file	Consider whether this documentation requires to be stored on both the paper file and the system, particularly if the paper files are going out of the office, ie to court.
Bank details for client	• From client	Necessary if money is to be transferred as part of settlement (Article 6b)	• Court department • Cash room	• Document management system • Paper file	Consider security and who has access to these details and who can change them.
Information about others					
Details about children involved in the dispute who are not clients in their own right	• From client • From child	Necessary to provide legal advice and representation about a claim to the client (not the child) (Article 6f)	•Court department • Solicitor for the other party/parties • Court • Expert witnesses • Court-appointed reporters • Party litigants	• Document management system • Handwritten notes on paper and typed-up notes • Paper file	Children are deemed to have the capacity to consent to processing in Scotland from the age of 12. If a child is not the client, then you need another legal basis for processing their data, which will probably be legitimate interests and necessary for the establishment, exercise or defence of legal claims if special category. Age-appropriate, fair-processing notices may be required.

The audit (continued)

Executries

Category of Data	How do you get the data?	Purpose and Legal Basis	Potential Recipients	Where is the data stored?	Notes
Information about executors					
Name, address and contact details of executors	• From the will • Direct from person who contacts you to notify of death – could be executor or third party	Necessary to provide legal services (Article 6b)	• Private client department • Court for confirmation • Department of Work and Pensions • HMRC • Private pension fund • Banks	• Document management system • Software provider • IT system support • Paper file • On mobile phone	If this information did not come from the executor, then they should be told where it came from and fair processing information provided. This is still required if they decide to deal with the estate themselves. How do you secure your phone to ensure personal data can be deleted if lost/stolen?
Identification documentation	• From clients/ executors	Necessary to carry out AML checks as required by law (Article 6c)	• Receptionist • AML partner	• Document management system • Software provider • IT system support • Paper file	Consider whether this documentation requires to be stored on both the paper file and the system.
Information about others					
Personal details for beneficiaries, including bank details	• From will • From executors • From other family members • From beneficiary • Via email	So that the instructions contained in the will can be carried out (Article 6f)	• Private Client Department • Cash room • Financial adviser (if beneficiary underage)	• Document management system • Software provider • IT system support • Paper file • Mobile phone	It will be common for this information to come from a third party and not direct from the beneficiary. The beneficiary should receive fair processing information.
Personal details for claimants or potential claimants, which could include bank details	• From executors • From other family members • From claimant • Via email	In order to comply with The Succession (Scotland) Act 1964, which obliges solicitors to find and process this data (Article 6c)	• Private client department • Cash room	• Document management system • Software provider • IT system support • Paper file • Mobile phone	It will be common for this information to come from a third party and not direct from the claimant. The claimant should receive fair processing information.

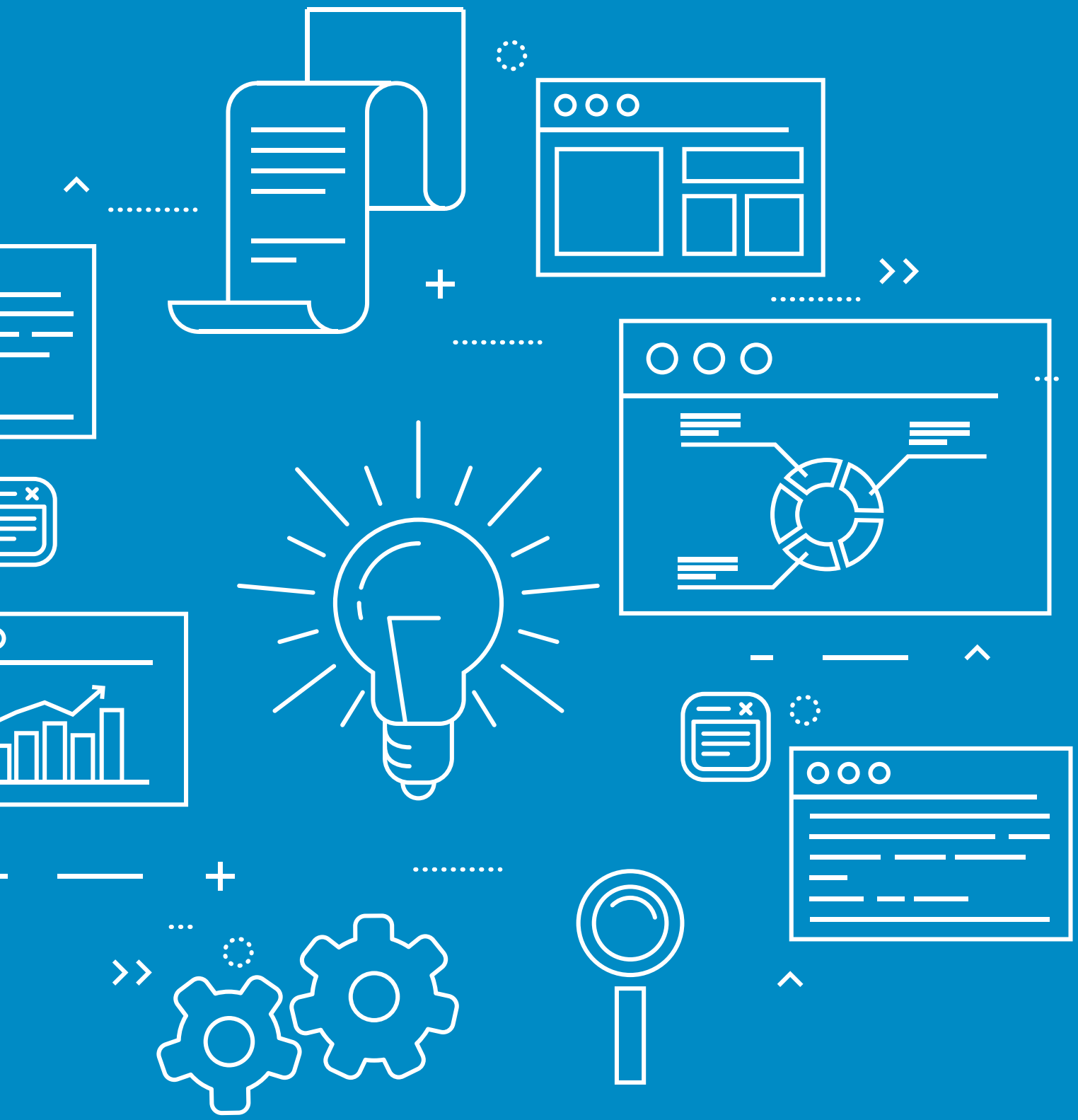
Example of a record of data processing

Using the information from its audit, our high street law firm created a record of data processing as required by the GDPR.

Record of Data Processing of High Street Law

Contact details of Controller: 1 High Street, Edinburgh EH1 1LP; Tel: 0131 222 2222; E: info@highstreet.co.uk

Data set	Purpose of processing (identify legal basis)	Categories of data subjects	Categories of personal data	Categories of recipients of personal data	Transfers to a third country or international organisation noting safeguards	Time limits for erasure	How do we ensure information is updated	Description of technical and organisational measures to secure
Identification documentation for clients	To ensure compliance with AML obligations under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Article 6c)	Individual clients and beneficial owners of corporate clients	Copy of passport or driver's licence and/ or copy of bank statement	Third party who carries out identity checks Cloud-based server hosted by third party	NA	Five years after the transaction is complete	Our AML policy indicates how often we require to update the AML checks	Held in a secure area of our document management system to which access is restricted to staff involved in AML checks. Paper copies are destroyed securely.
Contact details provided by family law client	To contact the client about their case under a contract with them or using legitimate interests if the contract is with their employer (Article 6b)	Individual clients and employees of corporate clients	Name, home or work address, email address and phone number	Cloud-based server hosted by third party Documented on paper files Solicitor's mobile phone	NA	Five years after the matter is complete if no further instructions.	Client is asked in terms and conditions to inform us of changes. We will confirm contact details on receiving new instruction. We will update on database and paper file.	Held in our client management system which is hosted on a cloud server (third party). All laptops and other end-user devices which can access the information in the cloud server are encrypted.
Case information provided by family law client	To provide legal advice under contract (Article 6b and 6f)	Client, former partner, children	Information about the legal issue about which advice is being sought	Court department Solicitor for the other party Court Expert witnesses and advisers Court-appointed reporters Party litigants Scottish Legal Aid Board Cloud-based server hosted by third party	NA	Five years after completion (Law Society guidance on divorce and consistorial matters)	NA – information updated as case progresses	Paper files and locked in a cabinet unless they are in use. Paper files remain in the office unless required for court etc. Information is held in our document management system, which is stored in a cloud server hosted by a third party. End-user devices which can access the database are encrypted. All special category data is encrypted when it is sent outside the organisation.



Data protection principles and your data protection policy

All personal data must be processed in compliance with the data protection principles, which are set out below. They lead to particular obligations under the GDPR but must be considered when dealing with any personal data to inform decision making.

Lawfulness, fairness and transparency	Processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	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.
Storage limitation	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.
Integrity and confidentiality	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.

There is an additional principle under the GDPR – accountability. That means organisations must not only comply with the GDPR but must also demonstrate that they comply. Ensure that you have documented policies and processes in place to demonstrate compliance.

Case study

Our high street law firm's work on data protection is underpinned by these principles, which are included in the firm's data protection policy. The firm's policy is based on the Law Society of Scotland's data protection policy template (available at lawscot.org.uk/gdpr).

Lawful processing

In order to process personal data lawfully, you must comply with all legal obligations and you must be able to rely on one of the following bases for processing.

Personal Data (Article 6)

a. The data subject has given consent to the processing of their personal data for one or more specific purposes
b. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
c. Processing is necessary for compliance with a legal obligation to which the controller is subject
d. Processing is necessary in order to protect the vital interests of the data subject or of another natural person
e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
f. Processing is necessary for the purposes of the legitimate interests condition – this is where you (or a third party) have a legitimate interest in processing the data which is not outweighed by any detriment caused to the data subject

Under the GDPR, consent is the least attractive basis as it can be difficult to maintain; law firms will be relying on one of the other legal bases. Solicitors will need to process the personal data of individuals in order to provide them with legal services under the contract, and may also need to process certain data to comply with legal obligations as a member of a regulated profession and because it is in the legitimate interests of the firm and/or client.

Special Category Data (Article 9)

If you are processing special category data on behalf of your client, you need additional justification from at least one of the following:
a. The data subject has given explicit consent to the processing of this personal data for one or more specified purpose
b. Processing is necessary for employment and social security and social protection law if required to comply with a legal obligation and there is an appropriate policy in place which explains the procedures for securing compliance with the data protection principles and, in particular, explains the employer's policies on retention periods and erasure of data
c. Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent
d. Certain activities carried out by not-for-profit bodies with a political, philosophical, religious or trade union aim, provided appropriate safeguards are in place and the processing takes place in relation to members or former members who have regular contact in connection with its purposes and the information is not disclosed beyond the organisation
e. The processing relates to personal data which is manifestly made public by the data subject
f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
g. Processing is necessary for reasons of substantial public interest on the basis of EU or UK law which sets out the relevant safeguards, which in the UK cover the following areas: parliamentary, statutory or governmental purposes; equality of opportunity or treatment; preventing or detecting unlawful acts; protecting the public against dishonesty; journalism in connection with unlawful acts or dishonesty; preventing fraud; suspicion of terrorist financing or money laundering; counselling; insurance; third-party data processing for group insurance and insurance on the life of another; occupational pensions; political parties; elected representatives responding to requests; informing elected members about prisoners; and, provided an appropriate policy is in place

h. Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems if by or under the responsibility of a health professional, social worker or anyone else who owes a duty of confidentiality under an enactment or rule of law and as long as an appropriate policy is in place, or

i. Processing is necessary for reasons of public interest in the area of public health which is carried out under the supervision of a health professional or by another person who owes a duty of confidentiality under an enactment or rule of law, or

j. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes with appropriate safeguards in place, including data minimisation and pseudonymisation – data should not be processed using this legal basis if it has an impact on a particular data subject or it is likely to cause substantial damage or substantial distress to an individual.

Case study

Our high street firm has determined a number of bases for processing personal data.

It is necessary to process the personal data of clients to provide a legal service under contract (6b, see left).

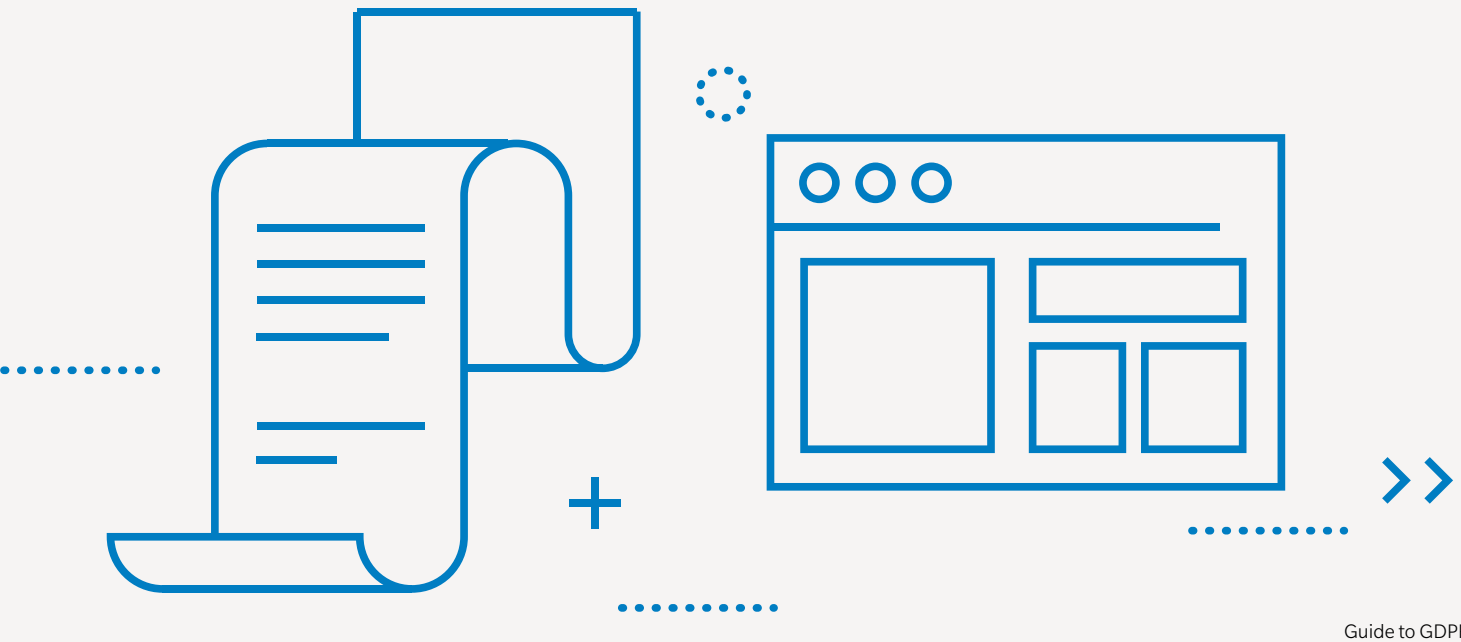
Additionally, processing is necessary to meet a legal obligation, such as anti-money laundering requirements (6c).

Finally, in relation to third parties (individuals who are not clients and do not have a contract), our firm will rely on the sixth legal basis listed, as it is in the firm's legitimate interests, or its clients' legitimate interests, to process this data (6f).

Because our law firm handles special category data, it is generally relying on the basis that processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (9f).

The processing must be necessary for these purposes.

The firm recorded its decision in its record of data processing.



Fair and transparent processing

In order to process personal data fairly, the processing must be in line with the data subject's expectations. In other words, only use the data for the reasons you collected it. Would the data subject expect it, if you wanted to do something else with it? And would you be happy to tell the data subject what you are doing with their data because this is now required by the GDPR?

There are exemptions to this principle. For instance, when solicitors are processing personal data of a third party in connection with a matter which is confidential or where the information would be regarded as privileged they do not need to comply with the requirement to ensure transparent processing and to provide the information required to ensure transparent processing as set out below when to do so would conflict with the provision of the legal service being provided.

The transparency principle means you have an obligation to supply all data subjects whose data you are processing with the following information when you are collecting personal data obtained directly from them – unless they already have this information or the exemption applies. Most organisations will deliver this information in a privacy notice which can be accessed through their website. Think about delivering the required information in a way that suits your clients. You may wish to provide some of this information to new clients when you send out your terms of engagement and then refer them to your website. You may want to make the privacy notice available in your office if that is how your clients interact with you. If you are processing the data of a child or vulnerable person, then you must adapt your privacy notice to ensure that it is clear and written in a way that will be understood.

Information which must be made available when personal data is collected:

- **Identity and contact details of the controller**
- **Contact details of the data protection officer, if applicable**
- **Purposes of processing and the legal basis of the processing**
- **The legitimate interests you are relying on**
- **The recipient or categories of recipients of the data**
- **Information about transfers to third countries, including how to ensure that it will be safe**
- **The period for which the data will be stored/criteria used to determine that period**
- **The consequences of failing to provide information if the processing is based on a statutory or contractual requirement**
- **The existence of any automated decision making/profiling etc; how it works and the consequences of this processing for the data subject**

You must also tell the data subject about:

- **Their right to request access to, rectification of, erasure of, restriction of processing, or to object to processing the data; and the right of data portability**
- **The right to withdraw consent to processing (where processing is based on consent)**
- **The right to lodge a complaint with the Information Commissioner's Office**

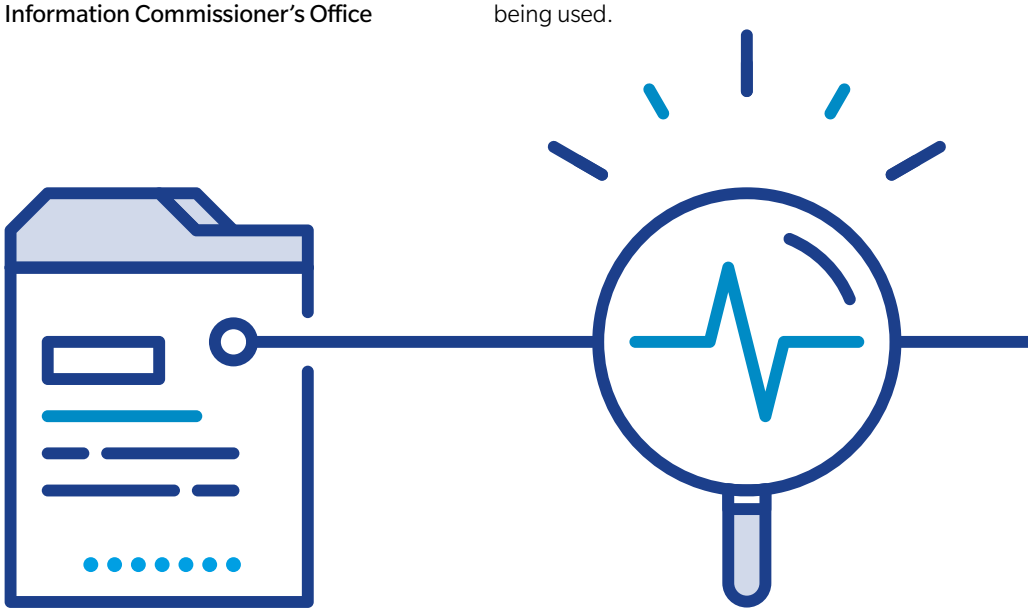
You have a duty to ensure that the information is delivered in an appropriate manner and you will be the best judge of how to that, but do avoid complex, legalistic language.

Although the obligation is not retrospective, there is an expectation that organisations will provide up-to-date information to individuals whose data they already hold. This may be done through your website, but you must decide how best to do this to ensure transparency.

If you receive personal information about an individual from a third party and not directly from the data subject, then you have an obligation to provide that third party with fair processing information unless:

- **They already have that information, or**
- **It would be impossible, or it would involve disproportionate effort, or**
- **The personal data must remain confidential where legal professional privilege applies**

Information must be provided to a data subject in this case within a reasonable time after having received the data, but within one month or when the data is being used.



Marketing

Most law firms will carry out marketing to some extent. If law firms are gathering information through their websites, then they must have a fair processing notice/privacy notice describing what is happening to the contact details that they are collecting in this way.

If law firms are carrying out any direct marketing activities using email addresses, then they must also comply with the Privacy and Electronic Communications Regulations 2003. These generally require that consent is in place before direct marketing emails are sent.
From 25 May 2018, it is likely that this consent will have to be GDPR compliant.

Law firms can send direct marketing emails to existing clients without consent as long as:

- They provided the individual with the option of opting out of receiving such messages at the time the data was collected, and
- They provide an opt-out every time a message is sent

These rules do not apply to business-to-business marketing and so sending an email to a named member of staff at an organisation does not require consent.

Case study

Our high street firm has written a privacy notice which covers the relevant information for fair processing for clients and others whose data it processes in the course of its business.

The privacy notice is on the firm's website and clients will be directed to where the information can be found.

The firm has also decided to send the relevant information from the privacy notice to new clients along with its terms and conditions as it recognises that not all their clients access their website.

Another privacy notice has been produced for all existing and new staff.

Client confidentiality, legal privilege and limited exemptions from the GDPR provisions

The forthcoming UK Data Protection Act contains provisions which mean that, in some circumstances, solicitors are exempt from certain duties of the GDPR when dealing with personal data that is subject to client confidentiality/contained within communications that are legally privileged.

The provisions limit:

- The requirement to provide fair processing information; and
- The information that is required to be disclosed in response to a subject access request

These exemptions exist to ensure that the obligations under the GDPR do not prejudice the confidentiality of the work that law firms are carrying out for their clients. They do not apply to all the processing of personal data that is carried out by the firm.

Client confidentiality/legal professional privilege in Scotland

It can sometimes be challenging to identify what information client confidentiality attaches to. It will not apply to all your client matters and it will not apply to all the information contained in your client files. You should consider this matter carefully.

Legal professional privilege can be claimed by a client to avoid disclosure of documents. Broadly speaking, there are two main categories of documents to which privilege can attach:

- Confidential communications between a client and solicitor, where the client seeks, and the solicitor gives, legal advice (legal advice privilege).
- Confidential communications between a client and solicitor in contemplation of litigation (legal litigation privilege). This extends beyond communications solely between solicitors and clients to cover communications with third parties (eg experts and witnesses), but only applies where the overarching, dominant purpose of the communication is for use in actual, pending or reasonably contemplated litigation.

The exemption

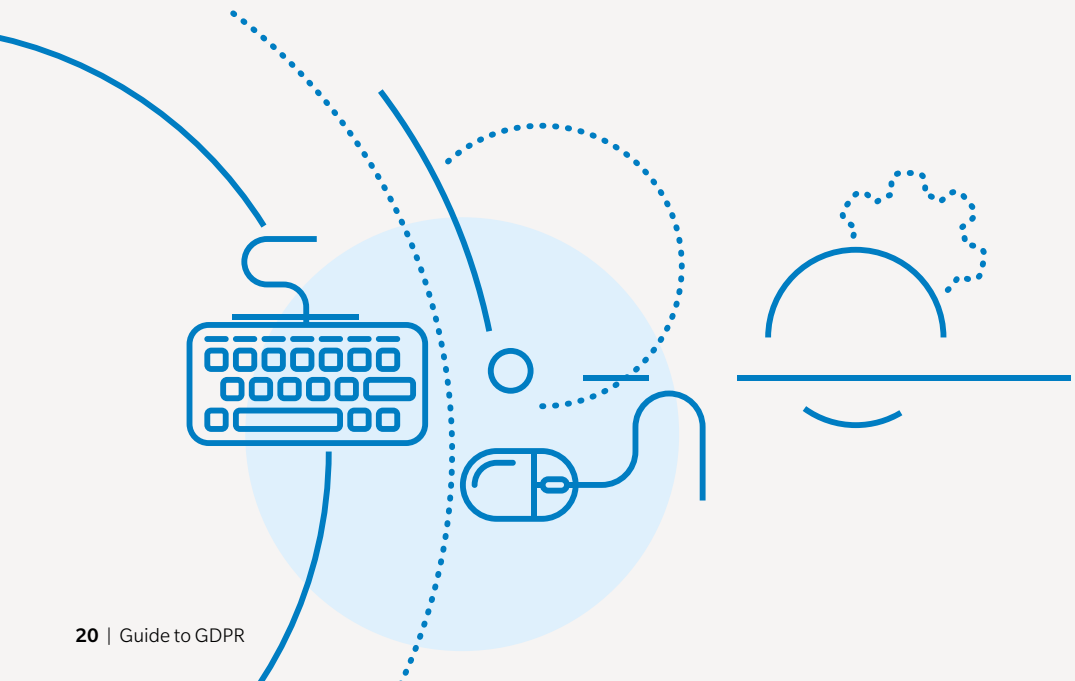
Our interpretation of the exemption is that, where personal data is being processed by solicitors and it is personal data to which a claim of legal privilege attaches, then the exemption should be taken into account. The exemption means that in certain circumstances:

- There is no requirement to provide fair processing information to other individuals involved in the matter; and
- Information does not require to be disclosed in response to a subject access request involving the personal data of your client

In each case, you should consider whether the provision of such information would prejudice your advice or your client's interests.

In practice, you will need to provide fair processing information to your client. However, if your client provides information about their spouse while giving instructions to you in relation to a divorce, you would not need to send fair processing information to the spouse. The same would apply to the beneficiaries of, or executors appointed under, a will prior to the death of the deceased.

However, in another example, if a client was getting financial assistance from his/her parents to buy a property, you should provide the parents with fair processing information about what will happen to their personal data.



Data retention

Retention policy

You should set out your information retention periods and how you will erase or dispose of personal data, whether held electronically or in paper form.

For many firms, this issue will be challenging and our advice is to create a plan in relation to retention and work towards compliance based on a risk-based analysis of the personal data you hold. Focus on the riskiest areas of data processing, ie any files holding health or criminal offence data. Then ensure that you monitor compliance with this plan and record this in your record of processing.

Retention periods

The GDPR states that personal data should be kept for no longer than necessary for the purpose for which it was processed. Data subjects must now be provided with information about the retention period for personal data at the point that data is collected, through the fair processing information that you provide them with.

As part of your record of processing, you will require to identify what personal data you hold, the purpose for which it is held and the relevant retention period for that personal data.

Law Society of Scotland guidance

The Law Society will be updating its guidance on the ownership and destruction of files in response to the introduction of the GDPR.

It is important to note that this will only deal with client files and will provide guidance on different types of client files. The onus is on each organisation to decide how long to keep personal data under the GDPR, although the retention period should be guided by legal requirements and professional guidelines. The Information Commissioner's Office states that if an organisation keeps personal data to comply with a requirement like this, it will not be considered to have kept the information for longer than necessary.

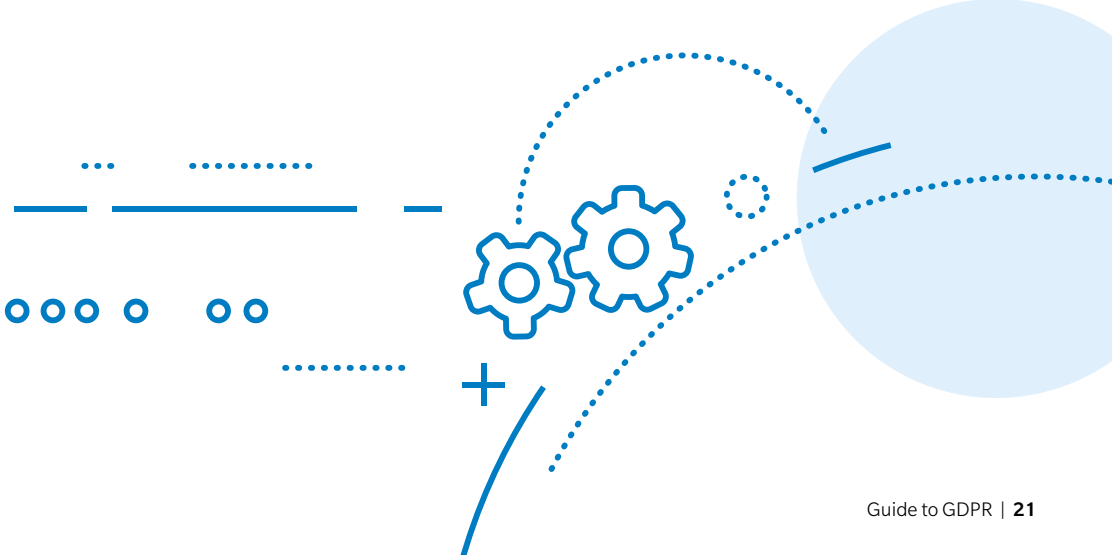
There will be several examples within the sector where the guidance is that papers should be kept indefinitely because it is very difficult to predict when they may still be required for the purpose of providing legal advice. This should be reviewed on a systematic basis.

Consideration will also have to be given to how long human resources records are retained in relation to staff.

Case study

Our high street firm already has a system in place for how long files are retained. It is using the record of processing to review the retention times for each data set. As our high street firm deals with family law, some of these files contain more sensitive information and these have been prioritised.

Our firm is recording the retention times in the record of processing.



Sharing and transferring personal data to third parties

It is useful to list all the organisations that you share data with on a regular basis. You will have already identified these organisations in your record of processing. Below are some examples.

It is important to distinguish between a data processor and a data controller as the obligations differ. Data controllers have the same obligations as you but data processors do not and, therefore, you must have a written contract in place to limit what they can do with your data.

Data controller	Data subjects	Third parties you share data with	
		Other data controllers	Data processors
Law firm	• Potential clients • Clients • Other individuals whose data is processed in order to provide legal services, ie witnesses, beneficiaries, executors • Employees	• Courts • Solicitors 'on the other side' • All those who assist with house sales, from financial institutions / surveyors to the person who puts the 'for sale' sign up • Expert witnesses • Registers of Scotland • Scottish Legal Aid Board • HMRC • Department for Work and Pensions • Financial advisers • Law Society of Scotland	• Client database (if not stored on your server) • Your cloud-based server provider if not in house • Confidential waste shredding company • Document storage company • Outsourced payroll provider • The company that photocopies large amounts of productions for court

Sharing data with data processors

Your obligations

• Carry out due diligence on the processor
• Monitor compliance with the GDPR and your contract
• Have an appropriate written contract in place with any processor

The level of due diligence and monitoring compliance carried out depends on the risk inherent in the processing. A greater level of due diligence is expected if special category data is being processed on an ongoing basis.

Written contract

There are enhanced obligations on the controller to have a written contract with any third-party data processing under the GDPR.

The contract must set out the following:

• The subject matter of the processing
• The duration of processing
• The nature of processing
• The purpose of processing
• The type of personal data to be processed
• The categories of data subjects whose data is to be processed
• The rights and obligations of the data controller

The contract must include the following instructions to the data processor:

• The processor must only process the data on the instructions of the controller
• Any individual processing data for the processor must have a commitment to confidentiality
• The processor must take appropriate security measures
• The processor must assist the controller to comply with data subjects' rights, including reporting any personal data breaches to the controller immediately
• The controller identifies whether the personal data should be deleted or returned to the controller at the end of the provision of services
• The processor must assist the controller with the provision of information for audit or inspection purposes

Sub-processors

If the data processor wishes to sub-contract any processing, they must obtain written authorisation from the controller. This can be provided in general terms in advance, but the processor must tell the controller the identity of any new sub-processor and any other changes. This allows you to ensure control over the data you hold and to advise the data subjects where their data is and what is happening to it, ensuring fair processing.

The processor should have a contract in place with any sub-processor to ensure that it has appropriate technical and organisational measures in place to ensure compliance with the GDPR. Any personal data breaches suffered by the sub-processor should be reported to the processor immediately.

Sharing data with other data controllers

There must always be a legal basis for sharing any personal data. Recipients (or categories of recipients) of the data must be identified in your fair processing/privacy notice.

Law firms should consider whether they require a written agreement to be in place with any organisation it passes data to. For example, you may wish to point out why the data is being shared and what should happen to it once there is no requirement for it to be processed by that party any longer. You should also consider security of processing and make attempts to ensure that the data will be held securely by the controller you are passing your data to.

The extent of this requirement will depend on the organisation and it is unlikely to be required when personal data is shared with the court, but perhaps should be considered when special category data is passed to an expert or other individual that the data controller has little knowledge of. Although these organisations or individuals have their own obligations as data controllers, you may decide to set out your expectations in your letter of instruction, particularly in relation to security and retention of personal data.

Case study

Through the record of data processing, our high street law firm has pulled together a list of all the data processors and data controllers that it deals with. Against each it is recording what arrangements are in place to ensure compliance. For example:

Name	Status	Contract with new T&Cs	Due diligence	Monitor
Case management system	Processor	Yes	Statement from supplier	At time of contract renewal

Data protection officers

The GDPR provides that certain organisations must appoint a data protection officer (DPO). Every organisation should have a data protection lead, whether or not they require a DPO.

The organisations which require a DPO are:

- All public authorities or public bodies, defined as those caught by freedom of information legislation – this includes all doctor and dental practices, colleges and universities but not currently housing associations, although this may change
- **Those whose core activities consist of processing 'special categories' of data (comparable to sensitive data, such as health data, trade union membership, political affiliation, biometric and genetic data etc) or data relating to criminal convictions or offences on a large scale – law firms and private health care organisations may fall into this category as well as certain housing association that provide care services**
- If the core activities of the organisation require regular and systematic monitoring of data subjects on a large scale – this includes organisations operating a telecommunications network; profiling and scoring for purposes of risk assessment (eg for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money laundering); location tracking, for example, by mobile apps; loyalty programmes; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices, eg smart meters, smart cars, home automation, etc

'Core activity' – one that is inextricably part of the function of the organisation and not a support activity, including activities where the processing of data forms an inextricable part of the controller's or processor's activity.

'Large scale' – number/proportion/volume and/or different types of personal data, including the geographical extent of the processing activity.

Sole practitioners are not required to appoint a data protection officer.

The second category may apply to some law firms. For instance, a criminal defence firm, or a personal injury firm, cannot provide legal services without processing special category data and so would appear to fall into the 'core activities' category. However, that may depend on the extent to which these areas of practice are the core activities of your firm.

It is difficult to determine what will be considered 'large-scale' processing. The guidance from the EU states that organisations should consider the following:

- The number of data subjects concerned, either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

The guidance provides examples of large-scale processing:

- Patient data in the regular course of business by a hospital
- Travel data of individuals using a city's public transport system (eg tracking via travel cards)
- Real-time, geo-location data of customers of an international, fast-food chain for statistical purposes by a processor specialised in providing these services
- Customer data in the regular course of business by an insurance company or a bank
- Personal data for behavioural advertising by a search engine
- Data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- Patient data by an individual physician
- Personal data relating to criminal convictions and offences by an individual solicitor

Whatever you decide for your firm, if you decide not to appoint a DPO, document your reasoning.

A DPO does not have to be an internal appointment – it can be an outsourced or shared service. Crucially, the DPO's role is to monitor and advise on compliance and not to make decisions about the processing of data as that would conflict with the role. Therefore, it can be very difficult to identify someone who can be independent of processing decisions to fill this role.

Data protection lead

Even if you do not appoint a DPO, you should nominate someone to take the lead in relation to this area and to be the point of contact for staff, clients and others. The restrictions in relation to who this person can be do not apply if they are not fulfilling the statutory role envisaged by the GDPR.

For more information about the role of the DPO, go to www.ico.org.uk

Case study

Our high street firm does process some special category data but it is not the core part of the business nor is it doing so on a large scale. On that basis, our firm will not appoint a data protection officer. It has identified someone in the firm who is the lead for data protection and it has made a record of its decision.

Security

Organisations processing data must have appropriate technical and organisational measures in relation to personal data held in paper files and stored digitally. The main difference is that data stored digitally can be held in larger quantities and, therefore, can present more risks if lost or misused. However, the loss of paper files still attracts fines from the Information Commissioner's Office (ICO) on a regular basis and many solicitors still work with large amounts of paperwork.

The same obligation existed under the Data Protection Act 1998 but the GDPR has provided more detail about what is expected, particularly in relation to digital data, taking into account advances in technology and the risk of cyber-attacks.

Considerations in relation to security of processing

In order to minimise the risk of personal data being misused, access controls should be in place to restrict the access of individuals to personal data on a 'need to know' basis.

If you are introducing a new processing system, then you should consider carrying out a data protection impact assessment. These are not covered in this guide but the ICO website (www.ico.org.uk) has guidance.

In relation to cyber security, the GDPR states that in deciding what security measures are appropriate, organisations should take into account the costs of implementation and the nature, scope, context and purposes of processing in relation to security. This means, in practice, that the level of security that an organisation is expected to take will depend on the technology and the resources available to the organisation. The organisation should evaluate the inherent risks in the processing and implement measure to mitigate those risks.

In addition, the GDPR also states that this assessment should take into account the likelihood and severity of any impact on the data subjects if personal data was lost or stolen etc, and that the security measures should be appropriate to the risk. The risks to be considered are those which could lead to physical, material or non-material damage and, in particular, this refers to discrimination, identify fraud or theft, financial loss, damage to reputation, loss of confidentiality where the information is protected by professional secrecy and any other significant economic or social disadvantage. Particular care must be taken over the data identified as special category.

Pseudonymisation and anonymisation

Pseudonymised data is data which has had the personally identifiable features removed but which can be combined with other data to re-identify the individual. This is a new term under the GDPR and pseudonymised data can reduce the risk of personal data being lost or unlawfully accessed if the additional information for attributing the data is kept separately.

Encryption

The ICO encourages making sure that any personal data being transferred digitally, whether by email or on a removable device, including laptops, is encrypted. This will reduce the likelihood of it being accessed if it is lost or stolen and may mean that there is no requirement to report the loss of such items.

Ensuring ongoing confidentiality, integrity, availability and resilience of processing systems

At the moment, the ICO recommends the following basic requirements in relation to cyber security and more information is available in the Law Society of Scotland's guide to cyber security:

- Install a firewall and virus-checking software on your computers
- Ensure that your operating system is set up to receive automatic updates
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities
- Do not let staff share passwords
- Securely remove all personal information before disposing of old computers
- Consider installing an anti-spyware tool

The ability to restore the availability of data in a timely manner

All organisations are vulnerable to cyber-attacks. In particular, the use of ransomware attacks has increased, meaning any business that relies on technology can be a target. The most common example is where malicious software gets into your IT system and encrypts the server. This could be through an email or the use or unsafe removable devices. A ransom is then sought from

the business before its data is returned.

The ICO's advice is to have a robust data backup strategy in place to protect against disasters such as fire and flood but also malware, such as ransomware. Backups should not be stored in a way that makes them permanently visible to the rest of the network. If they are visible, they can be encrypted by malware or the files could be lost. At least one of your backups should be offsite.

Have a process for testing security measures regularly

Regular vulnerability scans and penetration tests should be carried out on your systems for known vulnerabilities and to make sure that any issues identified are addressed.

Staff training

People are the weakest security link and staff should be trained in relation to data protection and security. Training should cover:

- What is expected of you in relation to data security
- Being wary of people who may try to trick you into giving out personal details
- Staff can be prosecuted if they deliberately give out personal details without permission
- The use of strong passwords
- Being wary of emails that appear to come from your bank and that ask for your account, credit card details or your password (a bank would never ask for this information in this way)
- Spam emails and not opening them, even to unsubscribe or ask for no more mailings

Reporting personal data breaches

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Obligation to report

The GDPR obliges the data controller to notify the Information Commissioner's Office (ICO) of a personal data breach without undue delay and within 72 hours after having become aware of it. This means you have a reasonable degree of certainty that a security incident has occurred. You do not need to report the personal data breach if it is unlikely to result in a risk to the rights and freedoms of individuals. If the notification is not made within 72 hours, then there must be a reasoned justification for that delay to accompany the notification.

Three types of breaches are identified and all three may take place at the same time:

'Confidentiality' breach
Where there is an unauthorised or accidental disclosure of, or access to, personal data.

'Availability' breach
Where there is an accidental or unauthorised loss of access to, or destruction of, personal data, which could be permanent or temporary.

'Integrity' breach
Where there is an unauthorised or accidental alteration of personal data.

In considering whether there is an obligation to report an incident, you should consider if there is likely to be an impact on the data subject's physical wellbeing, property and finances or reputation. Potential damage could include a loss of control over their personal data, or an impact on them in terms of discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional confidentiality or any other economic or social disadvantage to the individual concerned.

Contracts with processors must contain a requirement for personal data breaches to be reported to the data controller without undue delay, which has been interpreted as immediately.

What information must be provided to the ICO?

The notification to the ICO should include:

- A description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of data records concerned
- The name and contact details of the data protection officer or other contact point where more information can be obtained
- The likely consequences of the personal data breach
- The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects

It may not be possible to provide all this information at the time of notification, but it should then be provided without undue delay. We would recommend that information is only provided to the ICO after legal advice has been sought and once there is a clear indication of what has taken place. It will often not be possible to provide all of this information within 72 hours but every organisation should have a process in place to respond to breaches and professional advisers to call on to ensure that an immediate and effective investigation is carried out in response to a breach in order to fulfil the obligations under the GDPR.

The controller is under an obligation to document any personal data breaches, whether they are reported or not, in a personal data breach register. This should detail the facts surrounding the breach, its effects and the remedial action taken. It should be reviewed to identify any recurring security or other issues. The documentation must enable the ICO to verify compliance with the notification obligations and so must contain information about why a decision was taken not to report a breach.

Reporting data breaches to the data subject

If a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller is obliged to advise them without undue delay so that they can take the necessary precautions. The loss of, or unauthorised access to, any special category data is likely to require to be reported to the data subject, as would the loss of, or unauthorised access to, financial data, particularly if it can be used to access an individual's bank account and/or commit identity fraud.

The ICO may also be involved at this stage – advice how this is done and guidance issued by them should be followed. It may be responsible to advise data subjects before advising the ICO in cases where prompt action on the part of the data subject could avoid any potential damage.

Your clients should be advised of the breach in plain language and the notification should describe the nature of

the personal data breach, a description of the likely consequences and the steps taken to address the breach, including recommendations to the individual concerned to take action which may mitigate potential adverse effects. There should also be a point of contact where more information can be obtained from the controller.

Clients should be advised directly unless that would involve disproportionate effort, in which case it would be acceptable to provide a public communication.

Again, an assessment will be required about whether the breach requires to be reported. If you have implemented appropriate technical and organisational measures and, for example, all the electronic data compromised was encrypted, then you may not require to notify the data subjects concerned. Steps taken following the breach could also mean that any identified risks are no longer likely to materialise.

You need to take into account: the nature, sensitivity and volume of personal data; the ease of identification of individuals; the severity of the consequences for individuals; any special characteristics of the individuals; the number of individuals affected; and any special characteristics of the data controller, ie they owe a duty of confidentiality to the data subject over and above their obligations under the GDPR.

The ICO can insist that the controller notifies data subjects if it believes that there is a likelihood of a high risk.

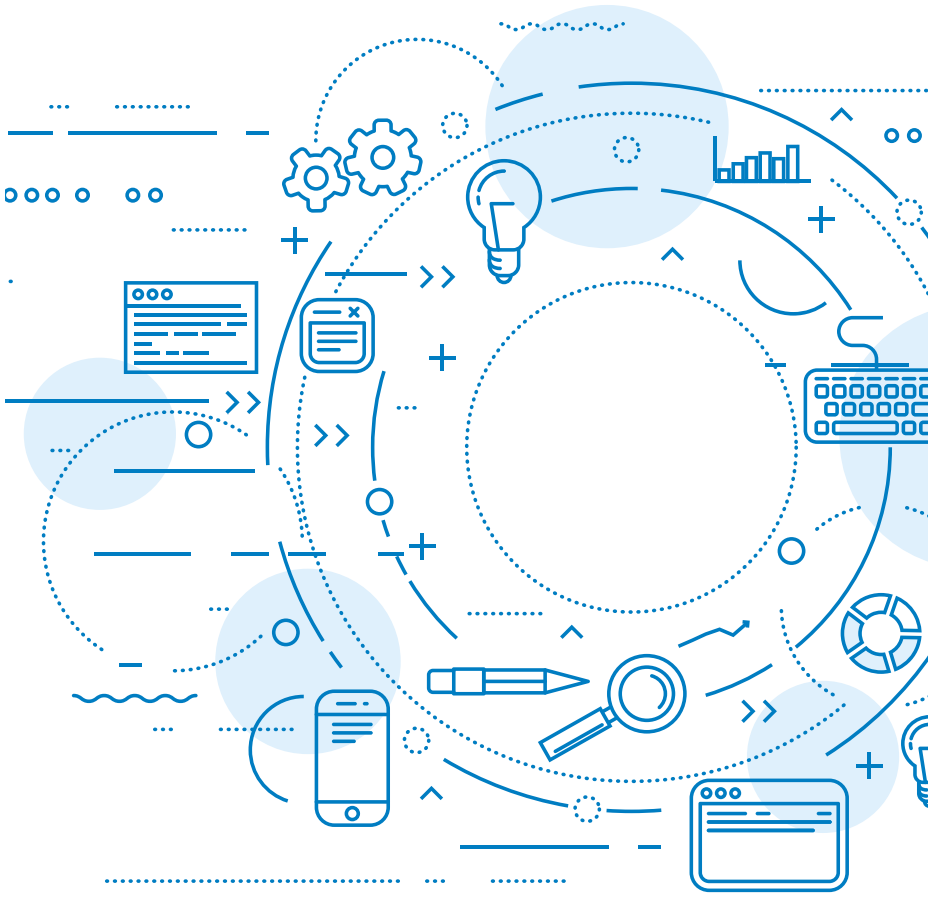
Go to www.ico.org.uk and see the section on personal data breaches for more information.

Case study

Our high street firm has created a simple incident log to record any personal data breaches, whether reported or not.

Contact: Jane Smith, Data Protection Lead at High Street Firm, joansmith@highstreet.co.uk

Nature of incident/ breach	Potential consequences of the breach	Data subject informed	ICO informed (72hrs)	Action taken/ change made as a result of the breach



Requests for client personal data

Requests for access to personal data (subject access requests, or SARs) could come from clients, third parties and investigatory bodies, particularly Police Scotland. An individual is entitled to a copy of the personal data that you hold about them but there are limits to that right. Police Scotland is entitled to request information without a warrant but if this contains personal data then you must decide whether or not you can provide them with the information.

Almost half of the complaints that the ICO receives are about SARs and so it is an area of concern for members of the public and the ICO. The obligations under the GDPR are greater and the timescales are shorter.

Clients and third parties – subject access requests

Under the GDPR, an individual can still ask for access to their own information. Before you provide that information, you should be satisfied about the identity of that individual and you can ask for verification before dealing with the request. The information must be provided without charge – previously you could request £10 payment but not under the GDPR.

You are expected to respond to the request without undue delay, and within one month of the request being made, which is on the calendar day a month after it was received.

In relation to clients, the process may be relatively straightforward, although you should consider whether they are entitled to all the personal data in their file which relates to other people and whether any other exemptions apply. See section on Requests from other organisations for personal data.

However, dealing with requests made by third parties, ie non-clients, is likely to be more difficult. You should not disclose any information which is legally privileged, but that exemption is not likely to apply to everything in your file. In relation to the other information in your file, you must consider whether it is the personal data of the requester and/or the personal data of your client or another third party. Sometimes personal data can relate to more than one person. If it is the personal data of another individual, then you must consider whether:

- The other individual has consented to the disclosure, or
- It is reasonable in all the circumstances to comply with the request even without that individual's consent

You should consider the impact on the individual if the information is disclosed – in particular, your client will expect that information that they provided, and which is in their file, remains confidential, although there is still a balancing exercise to be made between the right to access to information and the right to privacy. The ICO has further guidance on SARs (www.ico.org.uk).

The ICO encourages data controllers to speak to the requester to try to locate the information that they are actually interested in:

"We consider it good practice for you to engage with the applicant, having an open conversation about the information they require. This might help you to reduce the costs and effort that you would otherwise incur in searching for the information."

You cannot use this to try to narrow the request. Also, if the requester asks for access to all the personal data you hold about them, you are obliged to provide it subject to the exemptions mentioned here, and as will be outlined in the forthcoming Data Protection Act 2018.

It is important to note that the individual is entitled to the information held about them but not necessarily a copy of the actual document.

Other data subject rights are covered in the example of a data protection policy at www.lawscot.org.uk

Requests from other organisations for personal data

These requests are most likely to be made by the police or other investigatory bodies for the prevention and detection of crime or to apprehend or prosecute offenders. Law firms are not obliged to comply with such a request, which does not have the status of a warrant or court order.

Organisations such as other law firms may also request personal data that they believe they are entitled to. This is because they believe that the data is necessary for legal proceedings or to obtain legal advice, or to establish, exercise or defend legal rights. This can include requests from organisations seeking to recover debts. Again, law firms are not obliged to comply with such a request, which does not have the status of a warrant or court order.

Case study

Our high street firm has updated its current policy for dealing with requests for personal information. Part of that policy involves ensuring that all staff recognise a subject access request and know who in the firm is responsible for dealing with the request. The same person will deal with all requests for information.

The responsible manager determines whether that information can be shared and, if so, has clear methods for searching all the data on record – both physical and digital files. The policy also includes the new shorter timeline (one month) for providing information.

Appendix 1

Consent

It is very difficult to obtain valid consent. The result is that you should only rely on consent if there is no other legal processing condition that you can identify. You should not ask for consent if you will process data anyway as this could amount to unfair processing. Any consent that is not GDPR compliant after 25 May 2018 will not be valid and cannot be relied on as a legal basis for processing.

Definition of GDPR consent:

"Any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed. All GDPR consent must be explicit."

In order to obtain valid consent, the following conditions apply:

- The consent to the processing of personal data must be 'unbundled' and cannot be lumped in with other terms and conditions. Providing consent to the processing cannot be a prerequisite for the provision of a service unless it is necessary for the provision of that service. Requiring consent for processing that it is not necessary for the provision of the service will not produce valid consent.
- There has to be an 'active opt-in', which means that pre-ticked opt-in boxes and any mechanism that relies on silence are invalid and consent requires a positive action on the part of the individual.
- The consent should be 'granular', allowing the individual to consent separately to different types of processing and different purposes of processing.
- The data controller must be 'named' along with any third party who will be relying on the consent. This means that naming a sector or referring to generic 'third parties with similar interests' will no longer allow that third party to rely on that consent.
- Consent must be 'documented', which means that records must be kept of what the individual consented to and when, and how they were told.
- Consent must be as 'easy to withdraw' as it was to provide. There must be no detriment if an individual withdraws consent or refuses to provide consent.
- Consent will only be valid if is obtained where there is 'no imbalance in the relationship' between the data controller and the data subject. This will present difficulties for employers in relation to employees and public authorities, which will mean that they cannot rely on consent.
- Consent must be 'refreshed' at appropriate intervals, depending on the type of processing taking place.

Children's consent

In Scotland, under the UK Data Protection Bill, a child who has reached the age of 12 can generally be deemed competent to provide consent on his or her own behalf and exercise their own data subject rights.

Law Society of Scotland

About the author

Laura Irvine is partner at BTO Solicitors LLP and a solicitor advocate. She has a particular interest, expertise and passion about data protection law and has been assisting clients with the implementation of the GDPR across a wide range of sectors. Laura was co-counsel on the BTO team who successfully challenged a fine imposed by the ICO on Scottish Borders Council for a breach of the Data Protection Act 1998, which is to date the only ICO fine that has been overturned.

T: +44 (0)131 222 2939
www.bto.co.uk

For further information

Law Society of Scotland
www.lawscot.org.uk/gdpr
T:+44(0) 131 226 7411

Information Commissioner Office
www.ico.org.uk

About the sponsor

IT Governance is the leading global provider of IT governance, risk management and compliance solutions, with a special focus on cyber resilience, data protection, ISO 27001 and cyber security. We are at the forefront of helping organisations globally to address the challenges of GDPR compliance. Our GDPR experts can help your firm with a variety of best-practice solutions, including training courses, books, compliance toolkits and software, staff awareness training and consultancy services. With many years' experience in the legal sector, IT Governance can help you better understand the cyber security risks facing your firm, ensure that your defences are robust and help you through the many challenges ahead.

www.itgovernance.co.uk