Law Society of Scotland

Guide to GDPR

Sponsored by

MITIGO CYBERSECURITY

Contents

Examples of a privacy policy and a data protection policy can be found on the GDPR section of our website at: www.lawscot.org.uk/gdpr

Data Protection law update

Since this Guide was first drafted, the UK has left the EU. The GDPR was retained with substantively the same provisions as before. It is now referred to as the UK GDPR. At the time that this Guide was published, the Data Protection Act 2018 had just been finalised. This Guide therefore is to reflect these changes and additional developments in interpretation and guidance published since 2018.

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

We have produced this 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.

Part of this guide includes a data audit we carried out with a high street firm in 2018 to look at their data processing. Many high street firms will recognise the information gathered in the audit and can use it to evaluate their own data processing.

We have also taken into account the changes that the pandemic and working from home have made which led to more technology being used by all organisations.

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 Data Protection laws lies with the Information Commissioner's Office (ICO), not the Law Society of Scotland.

September 2023

UK 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 at a level appropriate to their size and turnover.	• Law firms as data controllers
2	**Audit your data processing**	Map out how you process personal data on behalf of your clients from the moment it comes into your office through to storage and file destruction. Don't forget to map the processing of 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 data protection compliance obligations.	• What counts as personal data • Create a record of data processing • Record of processing • High street case study • Engaging with new clients • Attracting new clients
3	**Identify all the third parties you share data with**	You must have a GDPR compliant contract in place with data processors (services providers who deal with personal data on your behalf) and appropriate arrangements in place with other controllers. You may wish to consider having arrangements with other organisations that you share personal data with particularly in relation to confidentiality, security and retention.	• Contracts with data processors • Agreements with data controllers • Due diligence and monitoring • Sharing data with other controllers
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.	• See data retention • AML and data protection
5	**Have a written data protection policy**	Your data protection policy sets out your approach to data protection and privacy.	• See template

UK GDPR ten steps (cont.)

	Step	Detail	Relevant section headings (from the guide)
6	**Create privacy notices setting out how you process personal data at least for clients, staff and visitors to your website**	There is an obligation to provide anyone whose personal data you process with information about how you handle their data and which sets out their rights and how to exercise them.	• Data protection principles • awful processing • Fair processing information/privacy policies • Confidentiality and limited exemptions • AML and data protection
7	**Have a written process for dealing with data subject requests, including subject access requests**	You should have a policy detailing how you will deal with requests from clients, employees/ex-employees and others 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 or an email going to the wrong person**	Have in place written process to set out what to do in the event of a breach, which provides guidance on how to identify whether it requires to be reported and who is responsible for reporting to the ICO/data subject. Ensure that all staff can identify a personal data breach, and are aware of who to report it to.	• Reporting personal data breaches
9	**Review your approach to marketing to ensure it is compliant**	Digital marketing is regulated by the Privacy and Electronic Communications Regulations, which mandate that consent is generally required for marketing to individuals and sole traders, but not necessarily business contacts. You may be able to use the soft opt-in for clients.	• Attracting new clients • Consent • Privacy notices
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 • Data subject rights • Requests for information • Data breach reporting

Law firms as data controllers

Law firms are data controllers in relation to the personal data they hold for their employees and clients, including information about any individuals involved in the client matter. 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 or an advocate) but is generally a corporate entity such as the partnership or LLP.

All data controllers are required to register with the Information Commissioner's Office (ICO) and all data controllers are required to pay an annual Data Protection Fee. 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 10 members of staff - the fee is £40 (or £35 if you pay by direct debit).
- 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 (£55 if you pay by direct debit).
- Tier 3 – large organisations – if your organisation does not fall into the above categories then the fee is £2,900 (£2,895 if you pay by direct debit).

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.

If you have a data protection officer (DPO) you must also tell the ICO the name of that person.

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.

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 personal data on behalf of the controller but are not, as an individual, a controller or a 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 an organised paper file from which an individual can be identified or is identifiable. It includes information that can be identified as relating to an individual which is used to inform a decision that you might take about an individual. It can include:

- Name
- Contact details
- Biographical information
- Photographic images
- CCTV footage
- Passport number and copies of passport
- Personal bank account details
- Meeting notes where personal matters are discussed

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 UK GDPR. The provisions and restrictions are essentially the same but are mainly found in the Data Protection Act 2018. 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 pay a fee to 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. It has 12 staff and a turnover of £1 million and so it pays a £60 fee.

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 any cloud server storing their 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 cause individuals harm or distress knowing it is not secure.

Solicitors are generally very aware of client confidentiality but Data Protection laws require the processes to be documented a lot more than before the GDPR came into force. Working out what personal data you are processing is essential to even begin to do this effectively.

The ICO has resources about documentation including templates which can be found at www.ico.org.uk

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 UK 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 contact details of your organisation (and, where applicable, your data protection officer)
- Purposes of the processing
- The lawful basis for the processing
- Any legitimate interests relied on for processing personal data
- Description of the categories of data subjects whose data you are processing
- Categories of personal data being processed if not obtained from the person it relates to and where it was obtained from
- Recipients or categories of recipients to whom personal data will be disclosed
- Information about transfers to third countries and international organisations with information about the safeguards in place
- Time limits for erasure of personal data or information about how that will be determined
- Information about the consequences of failing to provide personal data in certain circumstances
- A description of applicable data subject rights
- Information and contact details about how to make a complaint including to the Information Commissioner

Even if you don't have 250 employees or feel your processing is occasional, it is important to work out what personal data you are processing so that you can comply with the other data protection 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 accountability is met and awareness is built into the your organisation's processes and procedures.

You may be required to make these records available to the Information Commissioner in relation to an investigation, but this is not a document that requires to be published.

Case study

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

The audit

Examples of information required for your record of data processing

Our high street firm has audited it 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

Residential 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 enquiry • From client	• Necessary to provide the legal services associated with purchasing a house	• Conveyancing department • Property centre and other third parties who advertise properties for sale • Seller's solicitor • Photographer • Planner • Person who puts up the 'For Sale' sign • Surveyors • Viewing assistant	• Practice/document management system • In a paper file • On mobile phones or laptops • Within software provided by a third party or service provider • External IT support i.e. backup server	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's client to know their address How do you secure mobile phones to ensure personal data can be deleted if lost/stolen?
National insurance number	• From client	• Only necessary for Revenue Scotland if LBTT return being made	• Revenue Scotland	• Practice/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	• Compliance team • Any software used to assist in AML checks	• Practice/document management system • Paper file • Third party software	Consider whether this documentation requires to be stored on both the paper file and digitally
Bank details for client	• From client	• To carry out financial transactions as part of service	• Conveyancing department • Cash room • Financial adviser	• Practice/document management system • Paper file	Consider security and who has access to these details and who can change them
Information about source of funds from client, including bank statements or other financial documentation	• From client	• Necessary to ensure compliance with the law	• Conveyancing department	• Practice/document management system • Paper file	Consider security and access
Information in missives	• From client • Financial adviser	• Necessary to carry out conveyancing	• Conveyancing department • Seller's solicitor • Seller	• Practice/document management system • Paper file	Are there any sensitivities around sharing address details
Information about others					
Information about source of funds coming from a third party, including bank statements or other financial documentation	• From client and/or third party	• Necessary to ensure compliance with the law	• Conveyancing department	• Practice/ document management system • Paper file	If you are processing information about a third party, then you need to provide them with a privacy notice
Information in standard security document	• Client • Bank	• To facilitate any mortgage used to purchase house	• Conveyancing department • Mortgage provider • Registers of Scotland	• Practice/ document management system • Paper file	Security and access.

The audit (cont.)

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	• Court department • Solicitor for the other party/parties • Court • Expert witnesses and advisers • Court-appointed reporters • Scottish Legal Aid Board	• Practice/document management system • Software provider • IT system support • Paper files • On mobile phone and/or laptop	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 and necessary for the establishment, exercise or defence of legal claims for any special category data	• Court department • Solicitor for the other party/parties • Court • Advocates • Expert witnesses and advisers • Court-appointed reporters • Party litigants • Scottish Legal Aid Board	• Practice/document management system • Handwritten notes on in notebook 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 Only gather the personal data you actually need Be aware of any underlying dangers to your client or client's family from sharing their location in event of potential domestic abuse
Identification documentation	• From client	• Necessary to carry out AML checks as required by law	• Any software used to assist in AML checks	• Practice/document management system • Paper file • Third party software	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	• Court department • Cash room	• Practice/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 for the client's and the firm's legitimate interests to provide legal advice to obtain and provide legal advice	• Court department • Solicitor for the other party/parties • Advocates • Court • Expert witnesses • Court-appointed reporters • Party litigants	• Practice/document management system • Handwritten notes in notebooks 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, privacy notices may be required

The audit (cont.)

Executries

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 executors	• From the will • Direct from person who contacts you to notify of death – could be executor or a family member	• Necessary to provide legal services	• Private client department • Court for confirmation • Department of Work and Pensions • HMRC • Private pension fund • Banks	• Practice/document management system • Software provider • IT system support • Paper file • On mobile phone and/or laptop	If this information did not come from the executor, then that person should be told where it came from and referred to the firm's privacy notice provided. This is still required if they decide to deal with the estate themselves
Identification documentation	• From clients/ executors	• Necessary to carry out AML checks as required by law	• Compliance team • Any software used to assist in AML checks	• Practice/document management system • Paper file • Third party software	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 the Will • From executors • From other family members • From beneficiary	• So that the instructions contained in the Will can be carried out to allow legal services to be provided	• Private Client Dept. • Cash room • Financial adviser (if beneficiary underage)	• Practice/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 be provided with a link to a privacy notice
Personal details for claimants or potential claimants, which could include bank details	• From executors • From other family members • From claimant	• In order to comply with The Succession (Scotland) Act 1964, which obliges solicitors to find and process this data	• Private client department • Cash room	• Practice/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 a way to access the firm's privacy notice

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	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	Individual clients and beneficial owners of corporate clients	Copy of passport or driver's licence, proof of address, copy of bank statements, other information from third parties to confirm identity	• Third party service provider who carries out identity checks	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 practice/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	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	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 contacts 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 and can only be accessed using multi factor authentication
Case information provided by family law client	In relation to the personal data of the client, this processing is necessary to provide legal advice under contract with the client and for others it is in the legitimate interests of the client and the firm	Client; former partner; children	Information about the legal issue about which advice is being sought	• Court department. • Solicitor for the other party. • Advocate • Court • Expert witnesses and advisers. • Court-appointed reporters. • Party litigants. • Scottish Legal Aid Board. • Cloud based server hosted by third party	5 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 Practice/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 data protection law 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

Case study

Our high street law firm's work with any personal data is underpinned by these principles and inform the content of 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).

There is an additional principle which was introduced 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.

Lawful processing

In order to process personal data lawfully, you must be able to rely on one of the following bases for processing. Under the UK GDPR, consent is not easy to obtain and maintain and therefore law firms will usually be relying on one of the other legal bases. Solicitors must process the personal data of individuals in order to provide legal services. As a regulated profession, there are legal obligations to process certain information; and sometimes because it is in the legitimate interests of the firm and/or client.

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

Special category

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 are 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

Lawful processing (cont.)

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.

Firstly, it is necessary to process the personal data of clients to provide a legal service then second legal basis can be relied upon (Art 6(b)).

Additionally, to meet anti-money laundering obligations, they will at times, rely on the third legal basis (Art6(c)). If the law firm is using any special category data, most likely biometric data, for AML purposes there is a lawful basis set out in schedule 1 part 2 of the Data Protection Act 2018 which sets out the list of substantial public interests for processing. This includes at paragraph 12, processing that is necessary for the purposes of complying with a regulatory requirement to establish whether someone has been involved in an unlawful act or act of dishonesty, such as laundering money etc.

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 their clients' legitimate interests, to process this data (Art 6(f)).

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 (Art 9(f)) from the special category list).

The processing must be **necessary** for these purposes.

The firm recorded their lawful bases in their 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 purpose you collected it for. Would the data subject be surprised or disturbed if you did something else with it? Can you explain why any unexpected processing is justified, particularly if there an adverse impact on the data subject? And would you be happy to tell the data subject what you are doing with their data?

The transparency principle requires law firms to tell people what they are doing with their personal data. The required information is set out below.

In general, law firms have an obligation to supply all data subjects whose data they are processing with the following information when they are collecting personal data obtained directly from the individual. This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is generally provided in a privacy notice or statement. If you are processing the data of a child or vulnerable person, then you must adapt your privacy information 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 (name of the law firm along with contact details which we recommend are at the start of the notice)
- Contact details of the data protection officer, if you have one
- Purposes of processing and the lawful basis of any processing
- The legitimate interests pursued by the controller or third party (where the processing is based on the legitimate interests processing condition i.e. the data of individuals who are not clients)
- The recipient or categories of recipients of the data – the organisations of type of organisations you are sharing data with i.e. courts, other solicitors, surveyors, banks etc
- Information about transfers to third countries, including information about any relevant adequacy decision or other safeguard in place and how to obtain a copy of them or where they have been made available
- The period for which the data will be stored/criteria used to determine that period
- The 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
- Where the processing is based on a statutory or contractual requirement, and the consequences of failing to provide such data for the data subject
- The existence of any automated decision making/profiling etc; how it works and the consequences of this processing for the data subject

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. A website privacy notice for clients as well as visitors to your website can be used.

There are exemptions for law firms having to comply with this principle where the personal data is subject to a duty of confidentiality. There is more on this exemption below.

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 if the data is being used to communicate with the data subject at the time of the first communication; or if the data is to be disclosed to another third party, at that time. Again that is not required if they already have the information or if the exemption applies.

Case study

Our high street firm has written a privacy notice which covers the relevant information to advise clients and others whose data they process in the course of their business what is happening to it. 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 their terms and conditions as it recognises that not all their clients access their website.

Another privacy notice has been produced for staff and this will be given to all new staff.

Marketing

Most law firms will carry out marketing to some extent. If law firms are gathering personal contact details through their websites, then they must have information describing what is happening to the contact details that they are collecting and how they will be used.

If law firms are carrying out any direct marketing activities using email addresses i.e. sending newsletters or invitations to seminars etc, then they must also comply with the Privacy and Electronic Communications Regulations 2003. These Regulations generally require that consent is in place before direct marketing emails are sent to individuals, although not in a business to business context – see below. From 25 May 2018, consent had to be GDPR compliant and this applied to marketing databases that were already in existence.

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

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

These rules do not apply to business-to-business marketing and so sending an email to named member of staff at an organisation does not require consent. You must always allow the business contact to choose to opt out of hearing from you.

Case study

The law firm in our case study does not use personal data to market its services. However, it does have a website and the website places cookies. Consent is obtained through a cookie banner for all non essential work. What cookies the website uses and how the firms deals with the information derived from cookies is covered in their cookie notice.

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

The Data Protection Act 2018 contains provisions which mean that, in some circumstances, solicitors are exempt from certain duties when dealing with personal data. This is where the personal data that the law firm is processing is subject to a duty of confidentiality to the client which could be maintained in legal proceedings. i.e. legal privilege.

If this applies, the provisions law firms are exempt from are:

- The requirement to provide fair processing information; and
- The requirement to disclose personal data in response to a subject access request and from the obligation of complying with other data subject rights; and
- all of the data protection principles in so far as they relate to the above requirements.

These exemptions exist to ensure that the obligations under the UK 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. Confidentiality can cover more information than legal privilege. The right to privilege and the right to waive privilege rests with your client. You should consider this matter carefully.

Legal professional privilege can be claimed by a client to avoid disclosure of documents and, 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 (e.g. experts and witnesses), but only applies where the overarching, dominant purpose of the communication is for use in actual, pending or reasonably contemplated litigation.

AML and Data Protection

The Money Laundering Regulations require law firms to carry out anti-money laundering checks on clients, both individuals and corporate clients which inevitably involves the processing of personal data and sometimes special category data.

Law firms have a legal obligation to carry out identification and verification checks on clients. Therefore the lawful basis for processing any personal data for this purpose is Article 6(1)(c). As stated earlier, consent is difficult to obtain and maintain and in the context of personal data that is processed for the purposes of AML checks, law firms are obliged by the regulations to retain this information for a period of time. If the individual withdraws their consent during that time then the law firm would have to delete it if requested, as it has no lawful basis under data protection law to retain this information. A data controller cannot change its lawful basis for processing and so the solution is not to rely on consent.

Increasingly law firms are using technology to carry out checks remotely. The technology supplier will be a data processor and it is important to remember that the law firm remains responsible for the processing carried out through the technology, as they remain the data controller.

Biometric data

Some of the suppliers are allowing the use of facial recognition technology which relies on the collection of biometric data. This is special category data and so must be thought about more carefully. This technology should only be used if necessary and the decision about necessity is for the law firm.

If the law firm is using biometric data, for AML purposes there is a lawful basis set out in schedule 1 part 2 of the Data Protection Act 2018 which sets out the list of substantial public interests in the UK for processing provided by Article 9(1)(g). Paragraph 12 allows processing that is necessary for the purposes of complying with a regulatory requirement.

The controller must also consider the retention of AML records and in particular the retention of biometric data. The Law Society of Scotland's supervisory position is that law firms should be able to document they have undertaken the verification check, a summary of the information on which the check was based, the result and what decisions were made following the result. Therefore it may not be necessary for the biometric data to be retained by the technology company. As it is a processor, the law firm can instruct it to delete personal data held on its behalf.

Case study

Our law firm has started using a technology company to assist it with AML checks. This allows facial recognition technology to be used and our law firm has decided that this is only necessary where the fee earner has not met the individual either face to face or through a video call. This decision was taken following the completion of a Data Protection Impact Assessment and took this approach to comply with the requirement for the processing to be necessary and the data minimisation principle.

They have also asked the technology company to delete the biometric data one month after it has been collected.

The law firm has also updated it's privacy notice for clients to explain its use of technology, including the possibility that it will process biometric data.

Data retention

Retention policy

You should decide on how long you will retain the different categories of personal data and set out your retention periods in your record of processing activities (ROPA). You should also set out how you will erase or dispose of personal data whether held electronically or in paper form.

For many firms, this issue will be challenging. Solicitors like to hold onto information. The Law Society of Scotland has Guidance on the Ownership and Destruction of Files.

This states:

A solicitor's obligations to comply with GDPR need to be considered when deciding the specific date beyond which the obligation to hold a client's own documents can be said to expire.

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 i.e. any files holding health or criminal offence data.

Then ensure that you monitor compliance with this plan and record this in your ROPA.

Retention Periods

The UK 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 privacy notice.

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.

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.

Data retention (cont.)

Law Society of Scotland guidance

In relation to the files you hold about your clients, the Law Society of Scotland has issued suggested timings for file retention as follows, although, each firm is free to use this guide or select other retention periods as they see fit.

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 Data Protection laws, although the retention period should be guided by legal requirements and professional guidelines. The ICO 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. Consideration will also have to be given to how long HR records are retained in relation to staff.

Simple debt collection	Ten years after final completion i.e. after the time for appeal has elapsed.
Divorce and consistorial matters	Ten years after final completion, e.g. after maintenance, residence and contact orders, etc, have ceased to have effect, or children have reached majority.
Civil court cases	Ten years after completion.
Criminal cases	Summary cases Files in respect of summary cases should be retained for three years following the date of conclusion of proceedings. Solemn cases In solemn cases resulting in conviction files should be retained for the duration of the custodial sentence if it is more than three years in length. If the client is acquitted or the sentence is one of less than three years in length, the files should be retained for three years from the date of conclusion of proceedings. If the case is neither indicted nor reduced to summary complaint the file should be kept for a three-year period beginning one year after the date of first appearance on petition (or three years from the date that written confirmation is received from the Crown that there are to be 'no further proceedings'). In murder cases and other cases involving disposal by way of life imprisonment (such as the imposition of an Order for Lifelong Restriction) all papers should be retained indefinitely.
Executries	The retention period may be of particular importance in cases where no clear decision has been taken to discharge legal rights. Files should be retained for the period which is the later of: (i) 20 years after the date of the approval of the 'final' accounts of the executry; or (ii) Two years from the death of the deceased's spouse or civil partner (if applicable) Relevant documents and papers may, by agreement, be sent to the Executor for safekeeping since prior rights and legal rights only prescribe if not claimed in the 20 years after becoming enforceable.
Continuing trusts	Ten years after the termination of the Trust.

Data retention (cont.)

Conveyancing transactions	The following suggested timings are primarily aimed at residential conveyancing files as we are aware that commercial firms generally have their own policies. However, these periods may be used for commercial transactions if a firm decides that they wish to do so. Purchase: Ten years after completion - although the file may be of use until the property is subsequently disposed of. Sale: One year later after completion (i.e. after implementing Letter of Obligation; dealing with any funds retained; and after Missives have ceased to have effect). Solicitors should be vigilant to the fact that there may be obligations placed upon them to retain files by other bodies, such as UK Finance, and should ensure that these obligations are complied with.
Company work	Ten years after completion
Endowment and investment business	Given the nature of this work, endowment and investment business files should be retained in line with the guidance provided by the Financial Conduct Authority.
Other correspondence files	Five years after completion of the business.
Financial records	Law firms should also be aware that "the required retention period" for accounting records is defined by Rule B6.1.1 as being, the "remainder of the financial year of the practice unit and a further six financial years". Documents containing client's tax and VAT affairs must be retained for at least the relevant statutory periods. Compliance with HMRC required retention periods or other statutory requirements for retention of certain financial documents should be borne in mind when firms are considering how long to retain documents for. If, for any reason, a situation was to arise whereby the statutory retention period conflicts with the Society's guidance on retention periods firms should comply with the statutory requirement.
Money laundering - customer due diligence records	Firms should be aware of the retention requirements of Regulation 40 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
Closing of files	In cases where the matter in which a solicitor was instructed has not come to an obvious and natural conclusion, there is a professional duty upon a solicitor to advise a client in writing that the file will be closed in the absence of their instructions within a specific, reasonable period of time. This is clearly sound common sense in the situation where the solicitor is sitting waiting for further instructions. This allows for dormant files to be closed, accounts to be rendered either to the client or SLAB and both solicitor and client know the matter has come to an end. However, there are cases such as old conveyancing transactions after the delivery of the Search and other cases where the matter is obviously concluded where the duty is not the same.
Records of Destruction	When files, papers and/or documents are destroyed a separate record should be retained of the date of destruction which should include a general description of what was destroyed.

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 processor and a controller as their obligations differ. Other controllers have the same obligations as you, but processors do not and therefore you must have a written contract in place to limit what they can do with your data. There is an obligation to have a legally binding agreement in place between a controller and a processor. Sometimes these can be found in standard terms and conditions or sometimes in the case of software providers, the data processing agreement can be found on their website. Anyone external to your firm who has access to personal data on your systems is likely to be a processor.

Data Controller	Data Subjects	Third parties you share your data with	
		Other Controllers	Processors
• Law firm	• Potential clients • Clients • Other individuals whose data is processed in order to provide legal services, i.e. witnesses, beneficiaries, executors, etc. • Employees • Partners	• 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 of Work and Pensions • Financial advisers • Law Society of Scotland	• Case management database • Your cloud-based server provider if not in house • External IT support • Confidential waste shredding company • Document storage company • Outsourced payroll provider • The company which photocopies large amounts of productions for court

Sharing data with processors

Your obligations

- Carry out due diligence on the processor
- Monitor compliance with data protection laws 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 risks 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 is an obligation to have a legally binding contract between the controller and the processor.

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 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 subject's 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 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 the law firm as a controller to ensure control over the data you hold and to advise the data subjects where their data is and what is happening to it. This helps to ensure fair and transparent processing.

The processor should have a similar contract in place with any sub-processor to ensure any personal data breaches suffered by the sub-processor should be reported to the processor immediately.

Sharing data with other controllers

There must always be a lawful basis for sharing any personal data with another controller. Recipients (or categories of recipients) of the data must be identified in your fair processing/privacy notice. It should be relatively straightforward to identify these categories and there is no requirement to name the body or individual.

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 identify why the data is being shared and what should happen to it once there is no requirement for it to be retained by that party. You should also consider security of processing and make attempts to ensure that the data will be held securely by the recipient organisation you are passing your data to. These are commonly known as Data Sharing Agreements.

The extent of this requirement will depend on the recipient organisation and it is unlikely to be required when personal data is shared with the court, for example, 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.

Name	Status	Contract	Due diligence	Monitor
• Case management system • Expert Witness	• Processor • Controller	• Yes, processor contract • Data sharing provisions in letter of instruction	• Statement from supplier • Known to us and registered	• At time of contract renewal

Data protection officers

Data protection laws provide that certain organisations must appoint a data protection officer (DPO). Every organisation should have a data protection lead/manager, 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
- Organisations whose core activities consist of processing 'special categories' of 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 may fall into this category depending on the work that they do.
- If the core activities of the organisation require regular and systematic monitoring of data subjects on a large scale. Law firms would be unlikely to fall into this category.

'Core activity' means – 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' means – 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, which 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
- The volume of data;
- The range of different type of data being processed;
- The duration, or permanence, of the data processing activity; and
- 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 it to monitor and advise on compliance and not to make decisions about the processing data as that would conflict with the role. Therefore it can be challenging to identify someone who can be independent of processing decisions to fill this role, depending on the size of your firm.

Data protection lead/manager

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 UK GDPR.

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 firm who is the lead for data protection and it has made a record of its decision.

Security

This obligation to ensure security of processing is that organisations must have appropriate technical and organisational measures in relation to personal data held in paper files and any stored digitally. Since the COVID-19 working from home restrictions, all organisations are working with digital data and online a lot more. The risk of cyber-attacks has increased as well. However the loss or misuse of paper files still attracts fines from the ICO on a regular basis and many solicitors still work with large amounts of paperwork.

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. This will assist you to identify any risks in relation to data migration and the new system and will identify how to mitigate any risks. DPIAs are not covered in any detail in this guide but more information can be found on the ICO's website.

In relation to cyber security the UK GDPR states that in deciding what security measures are appropriate, organisations should take into account the state of the art, 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 measures 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 UK 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 appropriate 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 falling into the special categories.

In 2022, a firm of solicitors was fined £98,000 by the ICO in relation to a ransomware attack which resulted in 972,191 files being encrypted. This included 24,712 court bundles. 60 were released on the dark web. These files included a significant amount of personal data and special category personal data including health records, witness statements, the addresses of witnesses and victims and allegation of criminal conduct. The fine was issued in relation to a breach of the security principles because of the following failings:

- Lack of multi factor authentication on remote desktops
- Failing to patch the system against a vulnerability that had been known for five months; and
- Failing to encrypt data in the firms archive server;

The ICO noted that given the volume and nature of the personal data held by the firm, the security contraventions created risks that were serious enough to justify enforcement action and a fine.

Security considerations set out in the UK GDPR

Article 32 provides that consideration of security measures should include the following. None of these are prescribed but should be considered when deciding on what is appropriate for your firm, given the data that you process.

There is some excellent and accessible guidance on the National Cyber Security Centre's website which is tailored to different types and sizes of organisations.

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 can reduce the risk of personal data being lost or unlawfully accessed if the additional information for attributing the data is kept separately. Anonymised data cannot be linked to any individual and if information is truly anonymised, data protection laws do not apply to it.

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 lost or stolen and may mean that there is no requirement to report the loss of such items.

Security (cont.)

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 webpage: *guide to cyber security*.

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

All organisations of any nature are vulnerable to cyber-attacks and in particular the use of ransomware attacks has increased, where any business who 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, downloading malicious files by mistake or the use or unsafe removable devices. A ransom is then sought from the business with the promise of the return of the de-encrypted data if the ransom is paid. These organisations are often involved in serious and organised crime and therefore any ransom will fund more of that and you are not guaranteed to get your data back.

The NCSC'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. Back-ups should be tested to make sure they are working as expected and that you know how to restore files. Back-ups should not be stored in a way that makes them permanently visible to the rest of the network. If they are then, they can also be encrypted by the malware or the files could be lost anyway. At least one of your back-ups should be off-site.

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 link in relation to the security and staff should be trained in relation to data protection and security in particular. 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;
- That they can be prosecuted if they deliberately give out personal details without permission;
- The use of a 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); and
- 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

GDPR introduced a new obligation for data controllers to notify the ICO of a personal data breach without undue delay and within 72 hours after having become aware of it. In practice, this means when means you have a reasonable degree of certainty that a security incident has occurred and that personal data has been compromised. 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 i.e. email to the wrong person with personal data attached.

'Availability breach'

Where there is an accidental or unauthorised loss of access to, or destruction of, personal data, which could be permanent or temporary i.e. your system is encrypted by ransomware and you cannot access your files.

'Integrity breach'

Where there is an unauthorised or accidental alteration of personal data. i.e. someone has changed information when they should not have.

Not all of these incidents require to be reported. In considering whether there is an obligation to report an incident, you should look at the likelihood for there 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 which they suffered to be reported to the 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 of 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, if applicable. This decision can change over time.

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. In some cases this may allow subjects to take precautions against their bank account being compromised, for example. The

Reporting personal data breaches (cont.)

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 and can advise how this notification 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.

Anyone affected 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. It is important to keep the data subject advised of any developments such as, the individual who received the email has deleted it and has advised that they did not read it. This will keep any distress to a minimum.

Again, an assessment will be required about whether the breach requires to be notified to data subjects. 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 as it is very unlikely that anyone will be able to access any personal data about them. 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 i.e. they owe a duty of confidentiality to the data subject over and above their obligations under data protection laws.

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

Case study

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

Contact; Joan 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/ changed made as a result of the breach**

Requests for copies of personal data

Requests for access to personal data (subject access requests, or SARs) could come from clients or third parties. Police Scotland, and other investigatory bodies, can also make requests using a power under the Data Protection Act (2018). 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 concern SARs and so it is an area of concern for members of the public and the ICO. The obligations introduced under the GDPR were greater and the timescales for compliance were shortened.

Clients and third parties – subject access requests

Under data protection laws, an individual can ask for a copy of their own personal data and information about how it is being processed. 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 if that is necessary. A copy of the personal data and the information must be provided without charge and if the request was made electronically, then it should be responded to electronically. Requests do not require to be made in writing.

You are expected to respond to the request without undue delay, and within one month of the request being made. Therefore the deadline falls on the calendar day a month after it was received. It is possible to extend this deadline if the request is complex or your receive high number of requests.

In rare cases you can either charge for sending a copy of the personal data or refuse to provide it, if the requests is manifestly unfounded or excessive. Manifestly unfounded refers to the reason for the request and if it is clear that the individual making request has no intention of exercising this right but is using it as a bargaining tool or to disrupt the business. It could also apply if the individual is making unsubstantiated accusations against you or another employee or where an employee is being targeted where there is a clear grudge. Excessive refers to related requests asking for the same information over and over.

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 as some may relate to other people and whether any other exemptions apply. See the ICO's website for a fuller summary of the exemptions.

However, dealing with requests made by third parties i.e. non-clients is likely to be more difficult. You should not disclose any information which is confidential or 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
- Even without consent, is reasonable in all the circumstances to comply with the request.

You should consider the impact on the individual if the information is disclosed and in particular if your client expects that information that they provided will remain confidential. Although there is still a balancing exercise to be made between the right to access to information and the right to privacy, client confidentiality is likely to weigh heavily in favour or withholding the information.

The ICO encourages data controllers to speak to the requester to try and identify 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."

However, if the requester asks for access to all the personal data you hold about them, you are obliged to provide it subject the exemptions mentioned here.

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 containing the information.

Other data subject rights

The UK GDPR provides other rights to data subjects as follows:

- The right to rectification: if personal data is inaccurate or incomplete then the data subject can ask for it to be changed or added to. Sometimes this involves recording that the data subject has a different opinion rather than changing another opinion.
- The right to erasure: in limited circumstances the data subject has the right to have personal data deleted, but only if the controller should not have had it in the first place or where the personal data is no longer necessary for the controller's original purpose.
- The right to object: in limited circumstances, a data subject can object to the processing of their personal data and the controller has to weigh up their interests against the objection. Individuals have an absolute right to object to direct marketing.
- In certain limited circumstances where there is a dispute about the processing, the data subject can ask that it is not further processed until the dispute is resolved.

Requests for copies of personal data (cont.)

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 help them 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. Client confidentiality must always be considered in relation to both types of request.

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 subject access requests for personal information. Part of that policy is ensuring that all staff recognise a subject access request and know who in the firm is responsible for dealing with the request. Data protection training highlighted this. 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 files and digital. The policy also includes the one month deadline 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 it 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 UK 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.

If you require to obtain consent to process the personal data of a child, then you must ensure that you have a system in place for obtaining consent from the parent/guardian. In Scotland, a child who has reached the age of 12 can generally be deemed competent to provide consent on their own behalf.

About the author

Laura Irvine is a partner at Davidson Chalmers Stewart. She has particular interest, expertise and a passion about data protection law and has been assisting clients across a wide range of sectors. Laura is also convener of the Law Society's Privacy Law Sub-committee.

Email: Laura.Irvine@DCSlegal.com

www.dcslegal.com

For further information

Law Society of Scotland

www.lawscot.org.uk/gdpr

Davidson Chalmers Stewart

About the sponsor

MITIGO CYBERSECURITY

Mitigo provides cybersecurity and cyber risk management services to the legal sector.

Mitigo will provide you with visibility of your cyber risks, and secure you against attacks and business disruption.

Cybersecurity is not the job of IT support: it requires independent advice from cyber risk management specialists.

Without adequate protection in place, victims face:

- Ransomware attacks
- Financial loss
- Reputational damage

To learn more about Mitigo and the services they offer, please visit:

www.mitigogroup.com

Law Society of Scotland

The Law Society of Scotland
Atria One
144 Morrison Street
Edinburgh
EH3 8EX
T:+44(0) 131 226 7411
F:+44(0) 131 225 2934

www.lawscot.org.uk