THOMSON REUTERS
PRACTICAL LAW™

Data protection compliance for law firms

by Alison Deighton, Jenai Nissim and Claire Munro, HelloDPO

Status: **Law stated date 26 October 2022** | Jurisdiction: **England, Wales**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-035-1218**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

Note: this resource will be affected by the government's proposals for legislative reform of the UK data protection regime when enacted. See the UK data protection legislation tracker for details.

This practice note provides an overview of the key requirements of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (*(EU) 2016/679*) (UK GDPR) as it applies to UK-based law firms regulated by the Solicitors Regulation Authority (SRA). It also directs the reader to other relevant Practical Law resources.

This note focuses on the UK GDPR, but as this closely resembles the EU General Data Protection Regulation (*(EU) 2016/679*) as it has effect in EU law (EU GDPR), many of the same principles will apply.

Scope of this note

This resource reflects UK data protection legislation from 1 January 2021.

From the end of the UK-EU transition period, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) applies in the UK, along with the Data Protection Act 2018 (DPA 2018). For the background to UK data protection law during and after the transition period, see Practice notes, Brexit post-transition period: data protection (UK) and Brexit: implications for data protection.

As the EU GDPR will continue to have extra-territorial effect (*Article 3, EU GDPR*), the EU GDPR may continue to apply to UK controllers or processors who have an establishment in the EU or who offer goods or services to data subjects in the EU or monitor their behaviour, as far as their behaviour takes place within the EU. Such organisations may therefore find themselves subject to dual data protection regulatory regimes under the UK GDPR and the EU GDPR. For more information, see Practice note, Brexit post-transition period: data protection (UK): Determining which regimes apply.

For the purposes of this note, we have assumed that we are dealing with an organisation based solely in the UK which does not provide goods or services to EU data subjects or monitor their behaviour. For that reason, we refer to compliance with the DPA 2018 and UK GDPR only as they apply from 1 January 2021.

To view Westlaw UK's version of the UK GDPR under retained EU law, see the retained EU law version. As the government is not publishing definitive legal texts, it is not possible to publish a definitive content set of retained EU law. For more information, see Guide to identifying retained EU law in Westlaw content.

This note provides guidance to law firms regulated by the Solicitors Regulation Authority (SRA) on how to comply with data protection requirements in the UK, in particular under the UK GDPR and DPA 2018. Among other things, it explains:

- The accountability principle under Article 5(2) of the UK GDPR and what it means for law firm compliance.
- The governance structure law firms should consider adopting to ensure data protection compliance.
- The role of the data protection officer (DPO) and when a DPO should be appointed.
- The requirement for European representatives under Article 27(1) of the EU GDPR.
- The core components of a data protection compliance framework, including:
  - records of processing activities (ROPA);
  - reporting;
  - monitoring and audit;
  - data sharing protocols;

- policies and procedures;
- training and awareness;
- data protection impact assessments (DPIAs);
- data breach management; and
- data subject rights compliance.

For further general information on the UK GDPR and DPA 2018, see Practice notes, Overview of UK GDPR and Data Protection Act 2018: overview. For coverage of selected UK data protection legislation developments, see the UK data protection legislation tracker.

Accountability

Accountability is one of the key principles of the UK GDPR (Article 5(2)). There are two aspects of complying with the accountability principle:

- Controllers are responsible for complying with the UK GDPR.
- Controllers must be able to demonstrate their compliance.

In order to demonstrate compliance, a law firm must have in place:

- An effective data protection compliance framework (see Data protection compliance framework).
- Policies and procedures (see Policies and procedures).
- A staff training programme (see Training and awareness).

Senior management engagement and buy-in is also imperative, to ensure that a culture of compliance is embedded throughout the firm.

Accountability is about taking real responsibility for data protection compliance within your law firm and embedding a culture of compliance across the organisation, so that all individuals understand that they share responsibility for compliance.

Effective accountability has advantages for law firms. Senior management will understand how and why the firm uses personal data. If something does go wrong, your accountability measures will enable you to detect the problem quickly and help you to mitigate any enforcement action. You will be in a position to demonstrate that you have actively considered the risks involved with data processing and put appropriate mitigating controls in place.

Clear leadership is an essential part of accountability. Responsibility for data protection compliance should be allocated at a senior level within the firm (for example, a managing partner or at management or board level). There should be a clear governance structure to allocate roles and responsibilities for data protection compliance throughout the firm. Reporting should be set up to inform those with leadership responsibilities about what is happening with data protection compliance across the organisation. This will allow team leaders and others with leadership roles across the firm to report on the level of compliance to senior management on a regular basis.

The Information Commissioner's Office (ICO) has published guidance on accountability and governance (see ICO: Guide to the UK General Data Protection Regulation (UK GDPR): Accountability and governance).

For more information on accountability in relation to data protection, see Data protection accountability toolkit (UK).

Governance structure

Once you have identified suitable leaders to take ownership of data protection compliance, a governance structure should be put in place so that there is responsibility and accountability throughout the entire organisation (see Accountability).

Heads of department and their staff should have clearly defined responsibilities. For example, this could include understanding the data processing undertaken in their area and ensuring it is:

- Properly documented in the record of processing activities (ROPA) (see Record of processing activities (ROPA)).
- Identifying data breaches and reporting them in a timely manner (see Data breach management).
- Recognising the need for a data protection impact assessment (DPIA) when a new project is being planned (see Data protection impact assessments (DPIAs)).

These responsibilities should be documented as part of relevant role profiles.

When deciding how best to allocate these responsibilities within your firm, consider who makes decisions at present and look to build your governance structure for data protection into the existing processes of your organisation.

Data protection officer (DPO)

Some organisations are required to appoint a data protection officer (DPO) (*Article 37, UK GDPR*). Other organisations may voluntarily choose to appoint a DPO, although a DPO appointed voluntarily is subject to the same requirements as a compulsory DPO.

Law firms will need to consider their data processing activities and decide whether they need or want to

appoint a DPO. Generally speaking, a DPO will be required where a firm is carrying out data processing which requires the regular or systematic monitoring of individuals on a large scale or processing criminal conviction or special categories of personal data (special category data) on a large scale. For more information on special category data, see Practice note, Overview of UK GDPR: Special categories of personal data.

Even if you decide not to appoint a DPO, you should still allocate overall responsibility for data protection compliance to an individual within the firm. However, be careful to ensure that this individual's job title and external communications do not imply that they are the formally appointed DPO.

For guidance to help you to understand the role of the DPO and decide whether your law firm is required to appoint a DPO, see Practice note, Data protection officers (UK) and Flowchart, Do we need a data protection officer (UK)?.

Once you have made the decision to appoint or not to appoint a DPO, it is important to document your decision, so that you can show your reasoning if the decision is challenged.

EEA and EU arrangements

European representatives

Some UK law firms will need to appoint a European representative under Article 27(1) of the EU GDPR.

Law firms that are based in the UK and have no offices, branches or other establishments in the European Economic Area (EEA) but offer goods or services to, or monitor the behaviour of, individuals in the EEA must appoint a European representative (for example, when a law firm specialising in immigration law offers services to EEA citizens who want to move to the UK or a commercial firm advises the owners of a European business on compliance with UK law). An exemption applies under Article 27(2) of the EU GDPR where you are only processing personal data in these circumstances occasionally and the processing is unlikely to present a high risk to the rights and freedoms of individuals.

A European representative will act on your firm's behalf regarding your obligations under the EU GDPR and will act as a contact point for European data protection supervisory authorities for any matter in connection with your data protection compliance obligations (*recital 80, EU GDPR*). The EU GDPR itself does not provide a great deal of detail about the responsibilities of a European representative; further information can be found in the European Data Protection Board (EDPB) guidelines on territorial scope (EDPB: Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (12 November 2019)).

The European representative will facilitate communication between individual data subjects and your law firm to enable them to exercise their rights effectively. The European representative also needs to maintain a copy of the ROPA, which must be made available to the supervisory authority on request (see Record of processing activities (ROPA)). However, you will still be responsible for the main firm ROPA and for simultaneously providing the European representative with accurate and up-to-date information, so that the up-to-date ROPA is ready to provide to the supervisory authority at all times. The European representative must be appointed in writing and the appointment should detail the terms of the relationship.

Details of the European representative should be included in your privacy notices or any other information you provide to individuals before collecting their data. It is important to make this information easily accessible by supervisory authorities, for example by publishing the privacy notice on your website. However, there is no obligation to notify the ICO or supervisory authority of the appointment of your European representative.

Your European representative should be established in an EEA state where some of the individuals whose personal data you are processing are located and it is good practice to choose a representative based in a member state where a significant proportion of the relevant individuals are based. However, bear in mind that the representative must be easily accessible for data subjects in all of the EEA states in which you are offering services or monitoring behaviour.

"One stop shop" arrangement (lead supervisory authority)

Under the "one stop shop" arrangement, firms that are carrying out cross-border processing in multiple EU jurisdictions may benefit from appointing a European lead supervisory authority. The main advantage of appointing a lead supervisory authority is that, if a breach occurs in multiple jurisdictions, notification only has to be made to the lead supervisory authority and they will liaise with the other affected supervisory authorities.

Firms carrying out cross-border processing will need to identify their lead supervisory authority depending on the location of their "main establishment", which is generally the location of the headquarters or central administration base. The supervisory authority of this member state should usually be the lead supervisory authority. The situation may be different where decisions

on the purposes and means of processing are being made in other locations and then imposed on the rest of the firm including the administrative base.

When considering which lead supervisory authority to appoint in Europe, consider the primary language of your organisation. For organisations whose primary language is English, it is advisable to consider an authority who also uses English (for example the Irish, Belgian or Dutch authorities).

More information on the "one stop shop" and appointing a lead supervisory authority can be found in the Article 29 Working Party (now EDPB) guidelines (Article 29 Working Party: Guidelines for identifying a controller or processor's lead supervisory authority (adopted 5 April 2017)).

Data protection compliance framework

An effective data protection compliance framework will include and take account of the following:

- ROPA (see Record of processing activities (ROPA)).
- Reporting (see Reporting).
- Monitoring and audit (see Monitoring and audit).
- Data sharing (see Data sharing).
- Policies and procedures (see Policies and procedures).
- Training and awareness (see Training and awareness).
- Data protection impact assessments (see Data protection impact assessments (DPIAs).
- Data breach management (see Data breach management).
- Data subject rights (see Data subject rights).
- Contracting with third parties policies and procedures. These should document the due diligence that you will carry out on third parties, contract requirements and ongoing monitoring requirements.
- Legitimate impact assessments policies and procedures template documents. These should set out the circumstances in which a legitimate interests assessment must be completed, the steps involved in completing a legitimate interests assessment, and include a template document to be completed.
- Transparency information, including privacy notices, for your website, clients, employees and recruitment process and call-recording notices. Creating effective privacy notices will enable your firm to provide individuals with the information required by Articles 13 and 14 of the UK GDPR explaining how their personal data will be processed by the firm.
- Data protection programme of work. This is essential for successfully managing your data protection compliance framework and will identify and schedule key tasks to be carried out throughout the year (see Data protection compliance framework). Having a data protection programme of work in place will help the firm to manage its data protection compliance obligations effectively and proactively, by scheduling work at a manageable level throughout the year and preventing essential tasks from being overlooked. It is also a useful tool in demonstrating to an auditor or regulator the firm's commitment to its accountability obligations under the UK GDPR.

Record of processing activities (ROPA)

It is a requirement under Article 30 the UK GDPR for all controllers and processors to have a ROPA in place and the ROPA is a key part of a firm's privacy management framework. The process of completing the ROPA is an ideal starting point for your data protection compliance framework (see Data protection compliance framework). It will enable you to identify all of the data that your law firm holds and understand exactly what you do with it.

Without this information, you will be unable to assess the level of compliance within the firm or monitor your compliance with data protection requirements effectively.

A ROPA details:

- The personal data your firm holds.
- What you do with the data.
- Who you share it with.
- Overseas transfers of data.
- Data retention periods.

You can use the ROPA to document the lawful basis that you rely on to process personal data for different purposes, which helps to meet the accountability requirement (see Accountability).

You can also use the ROPA to:

- Check whether excessive data is being collected.
- Ensure that appropriate contracts are in place with those that you share personal data.
- Identify where international transfers are happening so that you can ensure that appropriate safeguards are in place.

The ROPA is also a useful tool to help identify when DPIAs and legitimate interest assessments need to be carried out (see Data protection impact assessments (DPIAs) and ICO: Guide to the UK GDPR: How do we apply legitimate interests in practice?).

You will need to consider the structure of your law firm in order to determine which records of processing activity are required. The ROPA takes a different form for controllers and processors. Your law firm may be a controller for some of its activities (for example, in relation to HR data or IT systems). Law firms are also usually controllers for the purposes of the work they do for their clients. However, there are some scenarios where a law firm could be a processor for the purposes of the UK GDPR (for example, when hosting a data room for a client). All of this means that a law firm may require multiple ROPAs taking different formats.

For more information on the ROPA, see:

- Practice note, Using data mapping to comply with Article 30 of the UK GDPR.
- Standard document, Record of processing activities under Article 30 UK GDPR (acting as controller).
- Standard document, Record of processing activities under Article 30 UK GDPR (acting as processor).

Reporting

It is important that senior management within the law firm, including partners, the management board and other relevant executive committees, are aware of the state of data protection compliance within the firm. Effective reporting will enable this.

You should ensure that the management team receives regular reports to keep them up to date with the firm's compliance with the UK GDPR. Senior management should have a good understanding of any areas that require further work or present risks.

Reports to senior management should include:

- Information about data breaches.
- Compliance with data subject rights requests.
- Updates on forthcoming regulatory changes.
- Details of significant projects involving personal data and associated risks.
- An overview of data protection compliance risks.

There is no prescribed frequency for reporting, so this can be tailored to the existing structure of management reporting within your firm. However, it is important that data protection reporting is scheduled to take place regularly and at the very least annually. If your firm has a risk register, the status of data protection risk should be recorded in it.

Monitoring and audit

It is important to continually monitor the levels of compliance with data protection legislation within your firm. If the firm has an internal audit team, you should enlist their help with carrying out audits to check compliance with data protection policies and procedures.

If you do not have an internal audit team, then self-checks should be scheduled across all areas of the firm regularly, focusing on areas handling higher risk personal data as a priority (for example HR, marketing or sensitive client data). This could involve those with responsibility for the compliance framework completing mini audits in order to determine the level of compliance with data protection legislation and identify and mitigate any risks. The results of these checks can then be used in turn to provide reporting to senior management.

For more information on monitoring and audit for data protection purposes, see Checklist, Data protection audit (UK).

Data sharing

When sharing data with third-party organisations, whether within or outside of the UK and EEA, a law firm must comply with the requirements of the UK GDPR. Some sharing (for example between controllers and processors) will require written contracts under Article 28. There is no requirement to have a written contract between independent controllers, but it is good practice to have this in place.

Article 26 requires an arrangement between joint controllers, setting out their respective responsibilities for data protection compliance (in particular, in relation to managing data subject rights requests including a contact point for individuals and providing transparency information).

For more information on data-sharing arrangements, see Practice note, Overview of data sharing arrangements: UK GDPR and DPA 2018.

Policies and procedures

Putting in place effective data protection policies and procedures is essential to your firm's ability to demonstrate compliance with the UK GDPR. It is also important to put in place a review and approval process to ensure that your policies and procedures are effective and up to date.

Training will need to be provided to ensure that staff are fully aware of the contents of policies and procedures.

Practical Law has a number of resources, including precedent policies and procedures. Not all of them will be relevant for all law firms. You should consider which policies and procedures are relevant to your firm and adapt them as appropriate for your firm's needs. See:

- Practice note, Designing Policies and Procedures: a Step-by-Step Guide.
- Practice note, Embedding Policies in your Company: a Step-by- Step Guide.
- Checklist, Policy certification process.
- Standard documents:
  - Data protection policy (UK).
  - Data retention policy (UK).
  - Cookie policy (UK).
  - Response procedures for data subject requests (UK).
  - Bring your own device to work (BYOD) policy.
  - Social media policy (UK) (short form).
  - CCTV policy.
  - IT and communication systems policy (short form).
  - Homeworking policy.

Training and awareness

Data protection training is key to embedding a culture of data protection compliance throughout the firm. All employees should be provided with basic data protection training when they join the firm and on a regular basis thereafter. A record should be maintained of the individuals who have completed the training in order to demonstrate that this has taken place. Data protection training often takes the form of online e-learning, including an end of module assessment which is used to demonstrate understanding of the subject matter.

Certain areas within the firm will require tailored, bespoke training, because of the high-risk personal data that they deal with. For example, HR (who deal with personal data that employees consider to be private, such as payroll data and special category data, such as employee sickness records). The marketing team will require bespoke training on the use of data in their day-to-day role (for example, sending email marketing, using cookies, use of social media and using online behavioural marketing).

The level of training required may also vary depending on the specialism of your law firm. For example, a law firm specialising in family law will regularly process personal data relating to children and will need to consider the particular requirements of processing children's data. This would not be relevant to a solely commercial law firm.

Data protection training cannot be a one-size-fits-all approach for all law firms or indeed all departments within the firm. By ensuring that training is tailored and relevant to the attendees' day-to-day roles, you should be able to ensure that staff receive the appropriate training for their role and in turn embed a culture of compliance with data protection legislation within the firm.

For training presentations on the UK GDPR that can be used as a starting point and adapted to a firm's specific requirements, see:

- UK GDPR key messages: presentation materials.
- UK GDPR in depth: presentation materials.

Data protection impact assessments (DPIAs)

A DPIA is an exercise intended to assist a data controller to assess the risks associated with a particular project or initiative involving the processing of personal data. Whenever your firm undertakes a new project or initiative, you should consider whether a DPIA is required.

A DPIA should be conducted at the outset of a project as it will enable you to fully understand the data protection implications of the proposal. The DPIA process will identify the risks associated with the proposed processing and identify mitigations for them. Conducting a DPIA will put you in a position to be able to explain to senior management exactly what data protection risks are involved in new initiatives or projects.

It is advisable to put in place a DPIA checklist which will enable you to identify situations where a DPIA is required. The checklist should be carried out on each individual new project or initiative. This will enable you to demonstrate that you have considered whether a DPIA is required whenever the firm is doing something new or innovative. This is important as you must document a decision not to carry out a DPIA as well as the DPIA itself.

A DPIA is required where the proposed processing is likely to result in a high risk to the rights and freedoms of the individual. The ICO advises firms to assess the level of risk by considering both the likelihood and the severity of any impact on individuals (see ICO: Guide to the UK GDPR: Data protection impact assessments). A high risk could result from either a high probability of harm or a lower probability of more serious harm.

The ICO's Guide to the GDPR provides that a DPIA should always be carried out where systematic and extensive profiling or automated decision-making is used to make significant decisions about people. This could include an automated recruitment platform which makes initial automated decisions about training contract applications.

A DPIA is also required whenever special category or criminal offence data is processed on a large scale.

Any use of an innovative technology (for example, a new document management, HR system or app) combining, comparing or matching data from multiple sources warrants a DPIA.

Invisible processing, where personal data is processed without first providing a privacy notice, is also a scenario where a DPIA should be considered.

A law firm may require a DPIA, for example, when it is:

- Looking at initiatives relating to diversity and inclusion.
- Considering implementing a new system for document management.
- Conducting pre-employment checks on applicants for roles at the firm.

For more information, see:

- Practice note, Data protection impact assessments (DPIA) (UK).
- Standard document, Data protection impact assessment (DPIA) (UK).
- Do we need a DPIA: infographic?

Data breach management

Law firms must be able to detect personal data breaches and investigate, assess risks and record them. They must also be able to report data breaches, when required, in line with the required timeline. Some data breaches will need to be notified to the regulator or the individuals affected and tight timelines apply. It is therefore important to have in place an efficient system for detection and reporting of breaches within the firm so that decisions can be made promptly.

Employees should be provided with training to enable them to recognise a data breach.

There should be clear procedures as to who a breach should be reported to internally and the breach notification mailbox should be continuously monitored.

There must be clear procedures in place for data breach management in order to contain and recover the breach, assess any ongoing risk and comply with the notification requirements. The firm must also be able to evaluate the breach effectively and consider what its response should look like.

What is a data breach?

A data breach is 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" (*Article 32, UK GDPR*).

In practice, this means there will be a personal data breach if any personal data is lost, destroyed, corrupted or accidentally disclosed to a third party. All sorts of different circumstances can constitute a personal data breach. For example:

- Losing a laptop or mobile phone on which personal data is stored.
- The corruption of data resulting from a software or equipment failure.
- Human error, such as accidentally sending personal data to an incorrect recipient.
- Deliberate attacks, such as hacking or phishing scams.
- Natural disasters, such as fire or flood damage.

For more information, see Practice note, Data breach notification (UK): What is a personal data breach?.

Notification

The ICO must be notified of a personal data breach without undue delay and, where feasible, not later than 72 hours after you have become aware of it (*Article 33(1), UK GDPR*). Notification to the ICO is only required where the personal data breach is likely to result in a risk to the rights and freedoms of individuals.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, it must be communicated to those data subjects without undue delay. The 72-hour time period does not apply to notification to data subjects; however, notification should be made without undue delay (*Article 34(1), UK GDPR*) as soon as is reasonably feasible (*recital 86, UK GDPR*).

Where a data breach involves client data, a law firm may also need to notify the SRA. The SRA Code of Conduct for Firms requires a firm to report to the SRA "any facts or matters that you reasonably believe are capable of amounting to a serious breach of regulatory requirements by any person approved by us" (*paragraph 3.9*). There are no fixed time frames for making a report to the SRA, although the SRA Enforcement strategy points out that prompt reporting is important (see SRA: SRA enforcement strategy (updated 21 January 2022)). The SRA encourages firms to engage with them at an early stage where a serious breach is indicated. For more information on SRA reporting, see Practice note, SRA Principles and Codes of Conduct: reporting obligations and whistleblowing.

For more information on data breach notification, see Practice note, Data breach notification (UK).

For template letters for use in the event of a data breach, see Standard documents:

- Letter to be sent by controller to notify data subjects of a personal data breach (UK).
- Data security breach notification: letter notifying a personal data breach to affected data subjects (UK).

Data subject rights

The UK GDPR provides individuals with a range of rights, known as data subject rights. These include:

- **Right to access (Article 15).** This provides the data subject with the right to obtain a confirmation of whether personal data concerning them is being processed and if so, where it is, access to the data and certain other information.
- **Rights to rectification, erasure and restriction of processing (Articles 16-19).** These rights allow individuals to request that inaccurate personal data is rectified, certain personal data is erased and the processing of certain personal data is restricted, so that data can only be used for limited purposes by the controller.
- **Right to portability (Article 20).** This enables data subjects to transfer personal data between data controllers.
- **Right to object to processing (Article 21).** This right allows individuals to object to specific types of processing.
- **Right not to be subject to a decision based solely on automated processing, including profiling (Article 22).** Individuals have a right not to be subject to decision based solely on automated processing (including profiling) where this would produce a legal or significant effect on them. This right provides a safeguard against the risk of a damaging decision being taken without human intervention.

For more information, see Practice note, Data subject rights (UK).

The ICO expects firms to inform individuals about their rights and ensure that all staff are trained in recognising and responding to data subject rights requests. Data subject rights requests should also be tracked and logged to demonstrate compliance and ensure the timeframes in the requirements are being met. Template response letters for data subject rights requests should be prepared to ensure that responses include all of the required information (see Handling data subject requests toolkit (UK): Controller's response letters).

Special considerations for law firms

The right to access is the most exercised right in relation to law firms. Often, a disgruntled individual involved in a client matter will attempt to exercise the right in order to obtain details of a client matter they have been involved in.

Law firms are able to take advantage of an exemption which applies in certain circumstances when an individual exercises the right to subject access. Personal data consisting of information in respect of which a claim to legal professional privilege can be maintained in legal proceedings, and information in respect of which a solicitor owes a duty of confidentiality do not need to be included in a data subject access request response (*paragraph 19, Schedule 2, DPA 2018*). In practice, this exemption will usually cover the majority of information held on a client file. Law firms may therefore find that it is unusual for them to have to provide an extensive response to a subject access request from a third party where their data is held in a client file that is subject to obligations of confidentiality and contains legally privileged information.

The right to erasure is not a blanket right and there will be certain situations where law firms will not be required to comply with requests to exercise it. The right to erasure does not apply to the extent that the processing in question is necessary to comply with a legal obligation, such as the firm's requirement to keep records under regulation 40 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (*SI 2017/692*) (MLR 2017) (*Article 17(3), UK GDPR*).

There is a further exemption (under paragraph 5 of Schedule 2 to the DPA 2018) which exempts from the right to erasure personal data which is:

- Required to be disclosed by a court or tribunal.
- Necessary for the purpose of legal proceedings or prospective legal proceedings.
- Necessary for the purpose of obtaining legal advice.
- Otherwise necessary for the purposes of establishing, exercising or defending legal rights.

These exemptions enable personal data to be used and shared in the context of providing legal advice and bringing or defending legal claims, in circumstances where the UK GDPR would otherwise prevent disclosure or use of the data.

Before relying on an exemption, it is important to check the wording of the exemption itself and document your rationale for concluding that the exemption applies in the circumstances. If an exemption does apply, the firm will still need to respond to the individual to explain why it does not need to comply with their request and inform them of their ability to complain to the ICO. For further information, see:

- Practice note, Data subject rights (UK).
- Practice note, UK GDPR and DPA 2018: profiling and automated decision-making.
- Practice note, Data subject rights under UK GDPR: compliance roadmap.
- Handling data subject requests toolkit (UK).
- Standard document, Response procedures for data subject requests (UK).