



# Guide to GDPR

Commercial team  
Data protection and GDPR

 **Paris Smith**  
LEGAL EXCELLENCE



## Introduction

The General Data Protection Regulation requires all organisations to demonstrate compliance with the data protection principles and to provide further information to data subjects about their processing activities.

Managing compliance policies effectively whilst running a business can be challenging. Our guide covers key steps and offers advice so that you and your business can effectively demonstrate compliance.



Chapter 1	<b>Common terms</b>	<a href="#">01</a>
Chapter 2	<b>Key principles</b>	<a href="#">02</a>
Chapter 3	<b>FAQs for marketing</b>	<a href="#">04</a>
Chapter 4	<b>10 steps to compliance</b>	<a href="#">09</a>
Chapter 5	<b>Role of the DPO</b>	<a href="#">11</a>
Chapter 6	<b>Speak to an expert</b>	<a href="#">13</a>



## Common terms

### Personal data

Simply, personal data is 'any information relating to an identified or identifiable natural living person'. Therefore any data held on a living individual who can be identified is personal data. This usually encompasses names and addresses of staff, customers, clients, suppliers and professional contacts, but it can also include more general information about the physical, genetic, cultural or social identity of a person. Remember - it can also include data which appears to be anonymised such as job titles - 'Head of IP at Paris Smith' identifies Laura Trapnell personally if you type it into google or look on our firm website.

### Special category data

Special category data is personal data that needs more protection because it is sensitive. The GDPR defines special category data as:

- Personal data revealing racial or ethnic origin;
- Personal data revealing political opinions;
- Personal data revealing religious or philosophical beliefs;
- Personal data revealing trade union membership;
- Genetic data;
- Biometric data (where used for identification purposes);
- Personal data concerning health;
- Personal data concerning a person's sex life; and
- Personal data concerning a person's sexual orientation.

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9.

### Data controller

A data controller is an individual or legal entity which controls how and why the personal data is collected and processed. This is most commonly the employer/business. GDPR requires data controllers to comply with a set of principles for processing personal data which we set out below. A data controller must ensure that it can meet at least one of a number of gateway conditions providing the legal basis for processing and in doing so, it must give data subjects information on its processing.

### Data processor

A data processor is the individual or legal entity which processes the personal data on behalf of the data controller – sometimes this can be the same entity but is often an independent legal entity to whom the processing function is outsourced.

### Data subject

The data subject is the individual to whom the personal data relates.

### Data subject rights

Data subjects have always had the right to be informed as to what data is held about them. They have always had the right to access this information and to object to the use of this data for direct marketing purposes. GDPR introduced additional rights for data subjects including (1) the right to be forgotten – which might be exercised where for example the processing of data is no longer necessary in relation to the purposes for which it was collected or processed, where the processing is either unlawful, or where a data subject has objected to processing based on the 'legitimate interest' condition, and (2) the right to rectification – where for example the data is inaccurate or incomplete and the right to restriction of processing (Article 18).

### Data protection officer (DPO)

Although some businesses will appoint DPO's voluntarily, there is only a requirement to have a DPO under the GDPR if your core activities involve systematic monitoring, large-scale processing of sensitive data (for example, health data or criminal records), or if you are a public body. A DPO will be independent, with a position in some ways analogous to an auditor although it is perfectly permissible for the DPO to be an employee, provided that the employee cannot be prejudiced by his/her role as DPO.

### Data breach notifications

The definition of a personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data". Organisations discovering a personal data breach must notify the regulator promptly and within 72 hours, if feasible. If the notification is not made within this time, the employer must provide a "reasoned justification" explaining the delay. Affected data subjects must be informed of any breach which is likely to result in harm to their rights and freedoms.

## Key principles

Our data protection laws set out fundamental principles which should form the foundation of your approach to processing data protection.

### Article 5

Personal data must be:

- Processed fairly and lawfully
- Processed for limited, specified, legitimate purposes and not in any manner incompatible with those purposes
- Accurate and kept up to date
- Adequate, relevant and not excessive
- Not kept for longer than is necessary for the processing purpose.
- 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.

These principles lie at the heart of the GDPR. They are set out right at the start of the legislation, and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions. Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the GDPR.

### Lawful basis for processing

## You must have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others - which basis is most appropriate to use will depend on your purpose and relationship with the individual data subject.

You must determine your lawful basis before you begin processing, and you should document it:

- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

### What are the lawful bases for processing?

The lawful bases for processing non-special category personal data are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

## You must determine your lawful basis before starting to process personal data. It is important to get this right first time.



If you find at a later date that your chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

### Processing special category data

If you are processing special category data, you need to identify both a lawful basis for processing under Article 6 and a special category condition for processing in compliance with Article 9.

You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

There are 10 conditions for processing special category data in Article 9 of the GDPR. Five of these require you to meet additional conditions and safeguards set out in UK law, in schedule 1 of the DPA 2018.

You must determine your condition for processing special category data before you begin this processing under the GDPR, and you should document it.

---

## Article 9 lists the conditions for processing special category data:

---

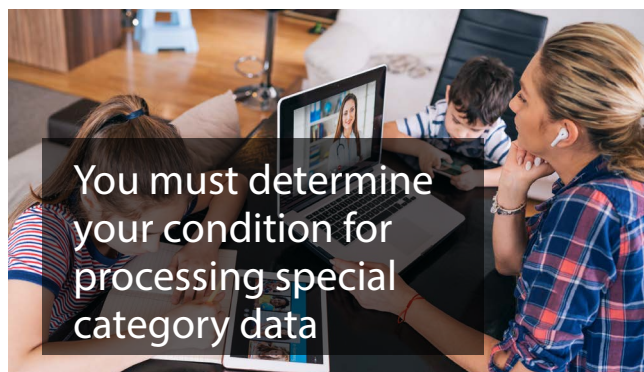
1. Explicit consent
2. Employment, social security and social protection (if authorised by law)
3. Vital interests
4. Not-for-profit bodies
5. Made public by the data subject
6. Legal claims or judicial acts
7. Reasons of substantial public interest (with a basis in law)

8. Health or social care (with a basis in law)
9. Public health (with a basis in law)
10. Archiving, research and statistics (with a basis in law)

If you are relying on conditions (2), (8), (9) or (10), you also need to meet the associated condition in UK law, set out in Part 1 of schedule 1 of the DPA 2018. If you are relying on the substantial public interest condition in Article 9 (2) (g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

### Processing criminal offence data

If you are processing data about criminal convictions, criminal offences or related security measures, you need both a lawful basis for processing, and either 'official authority' or a separate condition for processing this data in compliance with Article 10. You should document both your lawful basis for processing and your criminal offence data condition so that you can demonstrate compliance and accountability.



You must determine your condition for processing special category data



## FAQs for marketing

If your organisation carries out direct marketing activities, then in addition to the GDPR and our Data Protection Act 2018, you must also ensure compliance with the Privacy and Electronic Communications Regs (PECR) where your direct marketing activities are carried out by electronic means – i.e., sent between particular parties over a phone line or internet connection. This includes phone calls, faxes, text messages, video messages, emails and internet messaging. It does not include generally available information such as the content of web pages or broadcast programming.

### PECR will apply to you if you:

- market by phone, email, text or fax;
- use cookies or a similar technology on your website; or
- compile a telephone directory (or a similar public directory)

PECR restrict unsolicited marketing by phone, fax, email, text, or other electronic message. There are different rules for different types of communication. The rules are generally stricter for marketing to individuals than for marketing to companies.

You will often need specific consent to send unsolicited direct marketing. The best way to obtain valid consent is to ask customers to tick opt-in boxes confirming they are happy to receive marketing calls, texts or emails from you.

Direct marketing is defined in section 122(5) of the Data Protection Act 2018 as: “the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”. This covers all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations – for example, it covers a charity or political party campaigning for support or funds.

The marketing must be directed to particular individuals. In practice, all relevant electronic messages (e.g. calls, faxes, texts and emails) are directed to someone, so they fall within this definition.

---

## Genuine market research does not count as direct marketing.

---

However, if a survey includes any promotional material or collects details to use in future marketing campaigns, the survey is for direct marketing purposes and the rules apply.

Routine customer service messages do not count as direct marketing. In other words, correspondence with customers to provide information they need about a current contract or past purchase (e.g. information about service interruptions, delivery arrangements, product safety, changes to terms and conditions, or tariffs). General branding, logos or strap lines in these messages do not count as marketing. However, if the message includes any significant promotional material aimed at getting customers to buy extra products or services or to renew contracts that are coming to an end, that message includes marketing material and the rules apply.

### When is marketing ‘solicited’ and when is it ‘unsolicited’?

Most of the rules in PECR only apply to unsolicited marketing messages. They do not restrict solicited marketing.

Put simply, a solicited message is one that is actively requested. So if someone specifically asks you to send them some information, you can do so without worrying about PECR (although you must still say who you are, display your number when making calls, and provide a contact address).

An unsolicited message is any message that has not been specifically requested. So even if the customer has ‘opted in’ to receiving marketing from you, it still counts as unsolicited marketing. An opt-in means the customer agrees to future messages (and is likely to mean that the marketing complies with PECR). But this is not the same as someone specifically contacting you to ask for particular information.

This does not make all unsolicited marketing unlawful. You can still send unsolicited marketing messages – as long as you comply with PECR.



## What counts as consent?

You will often need a person's consent before you can send them a marketing message. If you do need consent, then – to be valid – consent must be knowingly and freely given, clear and specific. It must cover both your particular organisation and the type of communication you want to use (e.g. call, automated call, fax, email, text). It must involve some form of very clear positive action – for example, ticking a box, clicking an icon, or sending an email – and the person must fully understand that they are giving you consent. You cannot show consent if you only provide information about marketing as part of a privacy policy that is hard to find, difficult to understand, or rarely read.

The clearest way to obtain consent is to ask the customer to tick an opt-in box confirming they are happy to receive your marketing calls, faxes, texts or emails. You should keep clear records of what a person has consented to, and when and how you got this consent, so that you can demonstrate compliance in the event of a complaint.

---

## You should be very careful when relying on consent obtained indirectly (consent originally given to a third party).

---

You must make checks to ensure that the consent is valid and specifically identifies you. Generic consent covering any third party is not enough.

Remember that the customer is entitled to withdraw their consent at any time. You must make it easy for people to withdraw consent, and tell them how.

## What is the difference between 'opt in' and 'opt out'?

'Opt in' means a person has to take a specific positive step (e.g. tick a box, send an email, or click a button) to say they want marketing. 'Opt out' means a person must take a positive step to refuse or unsubscribe from marketing.

Some organisations provide opt-in boxes that are automatically pre-ticked. However, the GDPR is clear that pre-ticked boxes do not give valid consent.

You must use an 'affirmative' method of getting consent. We recommend you use un-ticked opt-in boxes wherever possible.

## Do the rules apply to business-to-business marketing

Yes, but there are different rules for marketing to companies and marketing to individuals (which includes sole traders and some partnerships). In general, the rules on marketing to companies are not as strict.

## What are the rules on making live calls?

The rules on live marketing calls are in regulation 21, 21A and 21B. In short, you must not make unsolicited live calls:

- To anyone who has told you they don't want your calls;
- To any number registered with the TPS or CTPS, unless the person has specifically consented to your calls – even if they are an existing customer (unless the call is in relation to pension schemes and you meet a strict criteria, see below);
- For the purpose of claims management services, unless the person has specifically consented to your calls; or
- In relation to pension schemes unless you are a trustee or manager of a pension scheme or a firm authorised by the Financial Conduct Authority, and the person you are calling has specifically consented to your calls or your relationship with the individual meets a strict criteria.

You must always say who is calling, allow your number (or an alternative contact number) to be displayed to the person receiving the call, and provide a contact address or free phone number if asked.

## What are the rules on automated calls?

The rules on automated calls are in regulation 19, and are stricter. You must not make an automated marketing call – that is, a call made by an automated dialling system that plays a recorded message – unless the person has specifically consented to receive this type of call from you. General consent for marketing, or even consent for live calls, is not enough – it must specifically cover automated calls.

All automated calls must include your name and a contact address or free phone number. You must also allow your number (or an alternative contact number) to be displayed to the person receiving the call.



## When can we make marketing calls to individuals?

You can call any individual who has specifically consented to receive marketing calls from you – for example, by ticking an opt-in box. You can also make live calls without consent to a number if it is not listed on the TPS – but only if that person hasn't objected to your calls in the past and you are not marketing claims management services.

---

## In practice, this means you will need to screen most call lists against the TPS register.

---

You will also need to keep your own 'do not call' list of people who object or opt out, and screen against that as well.

In general you cannot make live marketing calls in relation to pension schemes. However there is an exception to this but you must be a trustee or manager of the scheme, or authorised by the Financial Conduct Authority. You must also have either the individual's consent for the calls or your relationship with the individual must meet a strict criteria. The criteria that you must meet if you want to make such a call without consent is as follows:

- you have an existing customer relationship with the person you are calling;
- they might reasonably expect such a call from you; and
- you gave them a chance to opt-out of such calls when you collected their details and in every message you send them.

## When can we make marketing calls to businesses?

The rules are the same as for calls to individuals. So, you can call any business that has specifically consented to your calls – for example, by ticking an opt-in box.

You can also make live calls to any business number that is not registered on the TPS or the CTPS, but only if they haven't objected to your calls in the past and you are not marketing claims management services.

You should remember that some businesses (sole traders and some partnerships) register with the TPS, and others (companies, some partnerships and government bodies) register with the CTPS. For business-to-business (B2B) calls, you will therefore need to screen against both the TPS and the CTPS registers, as well as your own 'do not call' list.

## What are the rules on electronic mail marketing?

The rules on electronic mail marketing are in regulation 22. In short, you must not send electronic mail marketing to individuals, unless:

- They have specifically consented to electronic mail from you; or
- They are an existing customer who bought (or negotiated to buy) a similar product or service from you in the past, and you gave them a simple way to opt out both when you first collected their details and in every message you have sent.
- You must not disguise or conceal your identity, and you must provide a valid contact address so they can opt out or unsubscribe.

This same rule applies to emails, texts, picture messages, video messages, voice mails, direct messages via social media or any similar message that is stored electronically.

## When can we email or text individuals?

You can email or text an individual if they have specifically consented to receiving emails or texts from you – for example, by ticking an opt-in box.

You can also email or text an existing customer who has bought (or discussed buying) a similar product or service from you in the past – but only if you gave them a clear chance to opt out of getting marketing emails or texts when you collected their details, and in every message.





## What is a 'soft opt-in'?

The term 'soft opt-in' is sometimes used to describe the rule about existing customers. The idea is that if an individual bought something from you recently, gave you their details, and did not opt out of marketing messages, they are probably happy to receive marketing from you about similar products or services even if they haven't specifically consented. However, you must have given them a clear chance to opt out – both when you first collected their details, and in every message you send.

The soft opt-in rule means you may be able to email or text your own customers, but it does not apply to prospective customers or new contacts (e.g. from bought-in lists). It also does not apply to non-commercial promotions (e.g. charity fundraising or political campaigning).

## When can we email or text businesses?

Sole traders and some partnerships are treated as individuals – so you can only email or text them if they have specifically consented, or if they bought a similar product from you in the past and didn't opt out from marketing messages when you gave them that chance.

You can email or text any corporate body (a company, Scottish partnership, limited liability partnership or government body). However, it is good practice – and good business sense – to keep a 'do not email or text' list of any businesses that object or opt out, and screen any new marketing lists against that.

You may also need to consider data protection implications if you are emailing employees at a corporate body who have personal corporate email addresses (e.g. firstname.lastname@org.co.uk).

## Can we use bought-in marketing lists?

You can use bought-in lists to make live marketing calls, but you should screen against both the TPS and your own 'do-not-call' list of people who have previously objected to or opted out of your calls.

---

**You must be very careful before using bought-in lists for recorded calls, texts or emails.**

---

You can only use them if all the people on the list specifically consented to receive that type of message from you. Generic consent covering any third party will not be enough.

If you are using bought-in B2B fax lists, you must screen against both the FPS and your own 'do-not-fax' list of people who have previously objected to or opted out of your faxes. You may only fax individuals (including sole traders and some partnerships) if they have specifically consented to receiving faxes from you.

You must make checks to satisfy yourself that any list is accurate and the details were collected fairly, and that the consent is specific and recent enough to cover your marketing.

## What's the best way to compile our own marketing list?

You may want to compile your own in-house marketing list using details of people who have bought goods or services in the past, or who have registered on your website or made an enquiry. However, you should not assume that everyone is happy to receive marketing just because they have provided their contact details.

You should make it clear upfront that you intend to use their details for marketing purposes. The best way to get clear consent for your marketing is to provide opt-in boxes that specify the type of messages you plan to send (e.g. by email, by text, by phone, by fax, by recorded call).

You should record when and how you got consent, and what type of messages it covers. If possible, you should also record whether the customer is an individual or a company, as different rules apply. If this is not clear, assume they are an individual.



### Can we share our list with other companies in our group?

The same rules apply as for other third parties. If you intend to share the list within your group, you must have each individual's specific consent to marketing from your group companies.

As always, the best way to get consent is to provide an opt-in box. You should list the group companies (you could do this online by providing a link). You may even want to consider offering separate opt-ins for each company, to give the individual greater choice and to target your group's marketing more effectively. You cannot show consent if you only provide information about marketing from your group companies as part of a privacy policy that is hard to find, difficult to understand, or rarely read.

### How should we respond to objections or opt-outs?

As soon as someone objects to or opts out of your marketing, you should add them to a 'do not contact' list.

You should screen all your marketing against this list to make sure you don't contact anyone who has opted out. You can send an immediate reply confirming they have unsubscribed, but you must not contact them at a later date even if this is just to ask if they want to opt back in.

You must not simply delete their details altogether, as you need to ensure they are not later put back on your marketing list by mistake (for example if you buy more leads that include the same details). If someone asks you to delete their details, you should explain that you will need to keep them on a 'do not contact' list to make sure you comply with their right to opt out.

### Can we send marketing by post?

PECR do not cover marketing by post, but if you are sending post to named individuals you must comply with the Data Protection Act and the GDPR.





# 10 steps to compliance

The trick to ensure effective compliance with data protection is to adopt a logical 'keep it logical and straight forward' approach. Look at it as an opportunity to benefit and add value to your organisation, rather than being a box ticking exercise. Here are 10 top tips on what is essential for data protection compliance:

## 1. Data audit

Ask yourself -

- whose/what personal or sensitive personal data do you hold (this includes staff and customers);
- how/where is it stored and who has access to it?
- for how long is it stored and for what purpose?
- who are the data controllers and/or processors?
- Record your answers for future reference.

## 2. Risk assessment

What are the risks associated with the data storage and what are you going to do to eliminate those risks or reduce them to the lowest level possible? Risks might include a lack of understanding of what is meant by personal (or sensitive personal) data, loss of personal data, home working, disclosing personal data in error, failing to identify a request for access to personal data, retaining data for longer than is permitted or for a non-specific or irrelevant purpose, a change in personnel, new projects, a failure to register with the Information Commissioners Office or personal data being held by third parties (for instance, in the cloud).

---

**You need to record your findings and feed them into your risk register and training sessions.**

---

## 3. Privacy policy

Set out what the organisation intends to do about protecting individuals' personal data and the key personnel with responsibility for data protection - this does not need to be War and Peace!

## 4. Procedures

What practical steps are you as the data controller going to take? You will need to have in place procedures to deal with issues identified in the risk assessment such as:

- Data security
- Data access requests - covering in particular, to whom any (or any suspected) requests should be directed, ensuring the identity of the person making the request is clear, how to deal with third party information held with the personal data requested (this can be particularly tricky), reasons for denying access to personal data and how you record relevant deadlines and decisions (for instance to deny or permit access to personal data)
- Taking of/use of photographs or CCTV
- Disposal of data
- What to do in the event of a breach or suspected breach of the Data Protection Act - covering who will conduct the investigation, who should be contacted (this might include the individuals concerned, Information Commissioner's Office, your lawyers and insurers), whether internal disciplinary action is required and dealing with any adverse media coverage (you will no doubt find there are cross references to other documents, such as your social media policy, staff handbook/employment contracts and so on)

It might seem like a long list but with a little thought, procedures can be kept concise and manageable. It is often a good idea to involve staff who either already have or are likely to have hands on experience of data protection issues as this often leads to the development of more relevant and robust procedures as well as better buy-in from staff.



## 5. Training

Ensure anyone who handles or is likely to handle personal data is fully conversant with what the organisation and their colleagues expect from them.

## 6. Standard templates and documents

Draft and use these for subject access requests (if you want to put it on your website) and responses to subject access requests.

## 7. Communication

Ensure prompt and transparent communication with staff and customers about data protection issues, including 'plain English' privacy notices.

## 8. Contractual arrangements

Have in place proper contractual arrangements with third parties holding or disposing of personal data - to ensure clarity of the identity of the data controller/processor and who has responsibility for what as well as inclusion of appropriate confidentiality and liability/indemnity clauses.


## 9. Keep everything under review

As a benchmark, an annual review is sensible, although if there are any significant changes during the year, you should revisit your policy and procedures to ensure they remain relevant. Monitoring can help with improving and streamlining processes.

## 10. Keep up to date

Think about signing up to a regular update to save time. This is especially important with the EU Data Protection Regulation on the horizon.

Once established, data protection policies and procedures will become an integral part of the day to day running of the organisation rather a burden. As well as the benefits already alluded to, you will have staff that are confident of what they can and can't do, it will help build trust with customers and the reputation and financial position of the organisation will be protected.



Once established, data protection policies and procedures will become an integral part of the day to day running of the organisation rather a burden.





# Role of the Data Protection Officer

Under the GDPR, you must appoint a data protection officer (DPO) if you are a public authority (except for courts acting in their judicial capacity), carry out large scale systematic monitoring of individuals (for example, online behaviour tracking), or carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size. Any organisation is able to appoint a DPO - regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

## DPO Responsibilities:

### Policies and procedures

The DPO needs to implement policies and procedures to manage the outsourcing of data processing activities including the use of third party vendors for HR, IT and marketing.

### Information security

The DPO needs to maintain close relationships with the person responsible for information security in order to manage not only the contractual issues and compliance issues relating to the processing of personal data but also the information security policies and procedures relating to that processing and cyber security planning.

In terms of the development of policies, procedures and practices the DPO needs to:

- provide guidelines to the Board of Directors as well as all members of staff;
- provide guidelines to joiners or new members of staff;
- provide guidelines to contractors and third parties that are using company facilities and company information;
- liaise with HR in relation to the development of policies, procedures and practices and for particularly members of staff, interviewees and job applicants;

- liaise with the IT department in relation to the development of policies, procedures and practices for information security, data handling, outsourcing, BYOD and monitoring in the work place; and
- liaise with sales and marketing to ensure compliance with applicable laws and regulations for marketing, advertising, profiling and publicity.

## Training

Another important aspect of the role of the DPO is that of training. Apart from the fact that training is an essential element of implementing compliance it is also in the eyes of the data protection authorities an intrinsic part of compliance with the law. There have been a number of instances where when an investigation has been carried out by a DPA, the lack of training on policies and procedures has increased the fines and/or settlement.

---

**The DPO therefore must provide facilities for training in order to raise awareness of policies and procedures amongst existing staff, new staff and the board.**

---

In addition the DPO needs to advise and co-ordinate in-house training tailored to specific departments and teams and produce regular information as changes in laws and regulations emerge. This is a significant role as the global privacy frameworks change almost daily and the DPO needs access to as much information and updates as possible from external sources in order to keep fully abreast of laws, regulations and regulatory guidance.



## Subject Access Requests

In many jurisdictions in Europe data subjects have the right to know from the data controller what personal information that data controller is processing about them. This right is often called a Subject Access Request ('SAR') and when a SAR is received by the data controller there is often a fixed mandatory period for the data controller to properly respond to the SAR and therefore the DPO needs to implement a SAR policy and procedure as well as internal training on how a SAR is to be properly managed.

When a data subject issues a SAR it is usually in circumstances where the individual is unhappy or concerned about personal data being processed by the data controller and the SAR policy needs to anticipate the complexity of responding to a SAR particularly where large volumes of personal information are processed by the data controller in respect of that individual whether they are an employee or a customer.

The DPO needs to ensure that there is a records management policy that enables searches for personal records to be made in electronic databases as well as manual records since both are caught by the requirements of a SAR. This will mean understanding what personal information is held within the data controller's network as well as on personal devices on members of staff or on manual files. The SAR process means that attention also needs to be given to document retention and document destruction policies as well as home working and BYOD policies.

## Compliance audits and impact assessments

Under the GDPR, organisations are required to conduct routine impact assessments in order to assess the risk to individuals of a data breach. Organisational measures will be required to be implemented in the event of a data breach to ensure that such impact is minimised.

### The future role of the DPO

The DPO has to balance the role of a trusted advisor to the company as well as the internal policeman. This will require the DPO to carry out a number of tasks, including:

- raising privacy awareness;
- monitoring implementation and applicability of policies and procedures, and of the regulation
- ensuring that mandatory documentation is maintained;

- monitoring the documentation, notification and communication of data incidents and breaches;
- implementing and monitoring privacy impact assessments;
- liaison with data protection authorities and liaison with works councils and employees representatives.

### A protected position?

Article 38(3) requires that DPOs should 'not be dismissed or penalised by the controller or the processor for performing [their] tasks'. This requirement also strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.

---

**Businesses are not allowed to penalise a DPO (in terms of delay of promotion, prevention of career advancement, denial of benefits) if they are imposed as a result of the DPO carrying out his or her duties.**

---

It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to his/her DPO activities. As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct). However, the more stable a DPO's contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent manner.



# Speak to an expert

## GDPR & Data Compliance team

Our team has extensive experience of guiding clients through the complex requirements of GDPR, and have delivered multiple training sessions. Contact our team for bespoke advice and guidance on your compliance procedures.



Crispin Dick  
Partner  
m: **07958 165440** t: **023 8048 2107**  
[crispin.dick@parissmith.co.uk](mailto:crispin.dick@parissmith.co.uk)



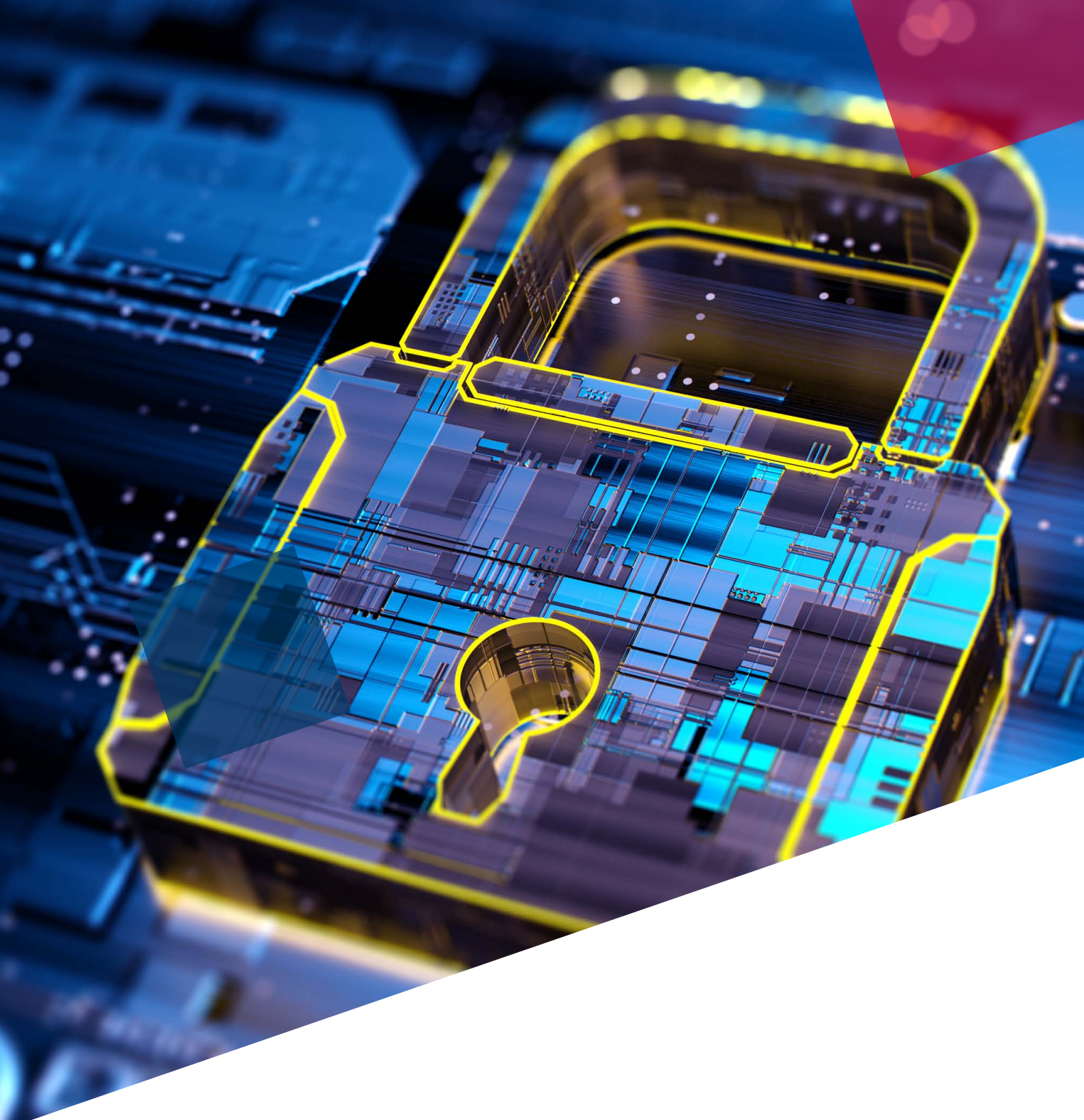
Laura Trapnell  
Partner  
m: **07825 250201** t: **023 8048 2114**  
[laura.trapnell@parissmith.co.uk](mailto:laura.trapnell@parissmith.co.uk)



Emily Sadler  
Associate  
m: **07771 643060** t: **023 8048 2102**  
[emily.sadler@parissmith.co.uk](mailto:emily.sadler@parissmith.co.uk)



Ryan Mitchell  
Solicitor  
m: **07741 906841** t: **023 8048 2316**  
[ryan.mitchell@parissmith.co.uk](mailto:ryan.mitchell@parissmith.co.uk)



1 London Road, Southampton  
Hampshire SO15 2AE  
t: 023 8048 2482  
e: [info@parissmith.co.uk](mailto:info@parissmith.co.uk)  
[www.parissmith.co.uk](http://www.parissmith.co.uk)

9 Parchment Street, Winchester  
Hampshire SO23 8AT  
t: 01962 679 777  
e: [info@parissmith.co.uk](mailto:info@parissmith.co.uk)  
[www.parissmith.co.uk](http://www.parissmith.co.uk)