Chapter 3:
Data protection

By Nigel Miller, founding partner, Fox Williams LLP

Introduction

Compliance with data protection laws is a key regulatory risk for law firms, just as it is for clients. Law firms manage huge volumes of data relating to their clients, which can be both sensitive and confidential. Law firms are subject to a general duty of confidentiality to keep the affairs of clients confidential unless disclosure is required or permitted by law or the client consents. In addition to this, law firms must comply with data protection laws.

The risk of getting it wrong can be severe. Aside from substantial fines, more damaging can be the adverse publicity, damage to reputation, and loss of goodwill that can flow from a data breach or regulatory action. This chapter sets out a high-level summary of applicable data protection laws, with a focus on areas that have specific application to law firms, and provides some best practice points for risk management.

Overview

Applicable law

The GDPR applies to all UK organizations that handle personal data. Since Brexit, we refer to the EU GDPR[1] and the UK GDPR.[2] In the UK, the Data Protection Act 2018 (DPA) applies alongside UK GDPR. In this chapter we refer generically to the GDPR.

While the GDPR applies only to "personal data", law firms handle considerable volumes of information that may not fall within the definition of personal data (for example, confidential corporate information). Some of the disciplines imposed by the GDPR in respect of personal data (for example, data security) can also be helpful in terms of protection of such other information.

In the UK, the Information Commissioner's Office (ICO) is the national data protection authority.

Awareness

It is important to ensure that the firm's decision-makers and personnel who handle personal data are aware of the extensive obligations imposed by the data protection regime. The firm should adopt a data protection compliance policy to make sure all staff are aware of their obligations. Compliance with data protection laws should be recorded as a risk in the firm's risk register.

Many data breaches arise as a result of human error. Crucially, therefore, all staff should receive training to ensure awareness of data protection laws and cyber risks. This can be done remotely using elearning programs.

Law firms as controller or processor

The GDPR distinguishes between "controllers" and "processors". In any transaction involving personal data, it is essential to identify the roles correctly (e.g., processor, independent controller, or joint controller) as this determines the obligations of each party under data protection laws.

The controller is the party *"which, alone or jointly with others, determines the purposes and means of the processing of personal data"*.[3] The ICO describes this as the party that decides what data to process and why.[4]

A processor is a body *"which processes personal data on behalf of the controller"*.[5] Typically, a processor is a service provider for the controller.

The main obligations under GDPR fall on the controller. However, a processor also has some standalone obligations (such as record keeping and data security).

Some clients assume that their law firm is a processor and request that the firm enters into a data processing agreement as they would with other service providers. Generally, this is not appropriate as it is considered that law firms process personal data on behalf of their clients as independent controller and not as processor. This is because law firms provide independent advice and have their own professional and regulatory responsibilities that can impact on their processing of the data. The Law Society has also cautioned that contractual obligations imposed upon a law firm in a data processor agreement could put the firm in conflict with its professional duties.[6]

Registration

In the UK, controllers need to register with the ICO and pay the data protection fee.[7] You are at risk of receiving a fine and attracting adverse publicity if you fail to register. Registration is a relatively straightforward step. On the other hand, failure to pay the fee is publicly visible – because

firms that have registered are on the searchable register on the ICO website – and could also betray a failure to comply with data protection requirements more generally.

There is no need to register if you only carry out "exempt processing"[8] of personal data, such as staff administration, advertising, marketing and PR, and accounts and record keeping. Even if you are exempt from registration, you must still comply with the requirements of data protection law and best practice is to register voluntarily for public transparency and in case any of your processing extends beyond the scope of the limited exemptions (so as to avoid receiving a fine).

It's good practice to have a process in place to pay the data protection fee on an annual basis. This can be done by setting up a direct debit with the ICO so that the registration is auto-renewed.

Data protection principles

There are seven data protection principles that form the core of the GDPR regime.[9] These are:

1. The lawfulness, fairness and transparency principle – see further below, under "Transparency".
2. The purpose limitation principle – data should be collected only "*for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".
3. The data minimization principle – you should hold only the minimum amount of personal data you need to fulfil your purpose.
4. The accuracy principle – "*personal data must be 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*".
5. The storage limitation principle – see further below.
6. The integrity and confidentiality (data security) principle – see further below.
7. The accountability principle – see further below.

Transparency

Providing privacy information is a fundamental requirement of the GDPR. In practice this means providing a privacy notice to anyone whose personal data you collect. Law firms will typically require privacy notices for clients and prospective clients, for partners and other members of staff, for

candidates, for marketing contacts such as users of the website or people you meet at networking events, for visitors to the office and for suppliers.

Under the GDPR, a privacy notice also has to be provided to individuals whose personal data you receive from someone else; for example, information you receive from the client. This may include family members, or people on the other side of a transaction or dispute. In this case, however, there are exemptions that are helpful for law firms. Privacy information does not need to be provided where:

- *"[T]he provision of … information proves impossible or would involve a disproportionate effort, … or in so far as … is likely to render impossible or seriously impair the achievement of the objectives of that processing"*;[10] or
- A claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings in respect of the personal data;[11] or
- The personal data is subject to a duty of confidentiality owed by a professional legal adviser to a client of the adviser.[12]

In practice, the professional duty of confidentiality will make the exemption available.

Storage limitation

The "storage limitation" principle means that personal data must be kept *"for no longer than is necessary"* for the purposes for which the personal data are processed.[13]

As such, each firm needs to establish and document its data retention policy. It is for each firm to decide how long personal data should be retained, taking into account legal and tax requirements, data protection laws, liability limitation periods, business needs, and professional obligations.

Once a retention period has expired, the data or record should be reviewed and securely destroyed if it is no longer needed. Keeping data for longer than is necessary, aside from breaching this principle, unnecessarily exposes the firm to continuing risk (e.g., in the event of a data breach) in relation to the data which it is holding.

Data security

The security of the data (both personal data and confidential corporate

data) that law firms process will be an ongoing concern for the management of the firm. A breach of data security can lead to substantial reputational damage, as well as potential loss of business, liabilities, costs, and regulatory action.

Under the GDPR, controllers and processors are required to implement *"appropriate technical and organizational measures to ensure a level of security appropriate to the risk"*.[14] The GDPR takes a risk-based approach such that there is no "one size fits all" requirement for data security. You can take into account the state of the art, costs of implementation, and the nature of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of the data subjects.

The "state of the art" will be determined by reference to relevant industry standards of good practice including the ISO 27000 series, the National Institutes of Standards and Technology (NIST), the various guidance from the ICO, the National Cyber Security Centre (NCSC), the Solicitors Regulatory Authority (SRA), Lexcel, and "NCSC Cyber Essentials".

Organizational measures will include development and regular review of the firm's IT security policy, including physical and digital access controls, strong password policies, staff training, and a process for regularly testing and evaluating the effectiveness of the measures put in place.

Technical measures can include implementing encryption of personal data when personal data is in transit (including on storage devices and laptops) and multi-factor authentication. In the event of the loss or theft of the device, the risk of the data being compromised is much reduced and as such there may be no need to report the loss or theft to the ICO as a personal data breach (see below). In addition, ensuring systems are kept up to date with virus protection, timely implementation of software security patches, and maintaining robust data back-up processes are essential.

In March 2022, the ICO fined Tuckers Solicitors LLP £98,000 for contravention of the data security principle following a personal data breach that resulted from a ransomware attack involving the encryption by the attacker of 972,191 files, some of which were then released on the dark web. The ICO identified a number of areas where Tuckers had failed to comply with the data security principle, including use of single factor authentication when multi-factor authentication should have been applied, failing to implement a free patch for four months after it was released (thus allowing a software vulnerability to be exploited), and failing to encrypt data stored on the firm's archive server.[15]

Lawful ground for processing

You can only process personal data if you have a lawful ground for doing so under Article 6 of GDPR. The main lawful grounds for processing are:

- Consent;
- Performance of a contract;
- Compliance with a legal obligation; and
- Necessary for the purpose of legitimate interests.

Under the GDPR, consent must be freely given, specific, informed, and unambiguous. Consent also has to be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes, or inactivity. A separate distinct (granular) consent is needed for different purposes and types of processing. Because of the high bar for obtaining a valid consent, and because consent can always be refused or revoked, it is not normally the preferred ground. Furthermore, consent of employees in the HR context is not normally considered to be valid because of the imbalance in the relationship such that employees may not have an effective free choice.

Where you rely on "legitimate interests", you need to document a legitimate interests assessment (LIA). The ICO provides a template to assist with this.[16]

You have to explain your lawful ground for processing in any privacy notice and when you answer a data subject request.

Special category personal data

If you are processing special category personal data, you will need to identify an additional ground under Article 9. Special category data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic or biometric data processed for the purpose of uniquely identifying a natural person; and personal data concerning health, sex life or sexual orientation.

There are a number of potential grounds for processing special category data, including:

- The data subject has given explicit consent to the processing;
- The processing is necessary for the purposes of compliance with the obligations of an employer under employment law;

- The processing is necessary for the establishment, exercise or defense of legal claims; and/or
- The processing is necessary for reasons of substantial public interest (with a basis in law).

In respect of the substantial public interest condition, there are a number of particular circumstances. The following may be particularly relevant:

- Equality of opportunity or treatment;
- Racial and ethnic diversity at senior levels;
- Preventing or detecting unlawful acts;
- Protecting the public;
- Regulatory requirements;
- Preventing fraud; and/or
- Suspicion of terrorist financing or money laundering.[17]

If you rely on one of the substantial public interest conditions, you will also need an "appropriate policy document".[18] This is a document outlining your compliance measures and retention policies for special category and criminal offence data.

It's good practice to review all the data you process (see below, data mapping) and identify your lawful ground for doing so for each category of data, paying particular attention to special category personal data.

Criminal convictions and offences

The GDPR gives extra protection to personal data relating to criminal convictions and offences. This covers a wide range of information about criminal activity, allegations, investigations, and proceedings. You can only process criminal offence data if you meet one of the 28 possible conditions19 that are available for the processing of criminal offence data similar to those that apply in relation to special category data. As with special category data, you will need an "appropriate policy document".

Accountability

The concept of accountability is central to the GDPR. The controller is responsible for, and must also be able to demonstrate, compliance with the data protection principles.

In practice, this involves implementing policies, keeping good records and documentation, and having appropriate contracts in place with data processors and other parties with whom you share personal data. It also involves the following specific elements.

Data mapping

You must create a record of your personal data processing, including the information set out in Article 30 of the GDPR. In the event of any issue arising, you may need to make this record available to the ICO on request.

As part of this, it's good practice to create a data map. There is no particular form for this but the ICO offers a template.20

There is an exemption from the obligation to keep a record of data processing for organizations employing fewer than 250 people. However, the exemption does not apply in wide-ranging circumstances (for example, where the processing is "not occasional" (not just a one-off occurrence or something you do rarely) or includes special categories of data).[21] As such, the exemption is unlikely to apply to most law firms and, in any event, irrespective of the size of the firm, it is good practice to keep a record of data processing.

Data Protection Officer (DPO)

You must appoint a DPO[22] if your core activities consist of:

- Large-scale processing of special categories of data or data relating to criminal convictions and offences; or
- Processing operations that require the regular or systematic monitoring of data subjects on a large scale.

Law firms, therefore, need to make a determination as to whether the firm is required to appoint a statutory DPO. When considering if processing is on "a large scale", regulator guidelines[23] say you should take into consideration the number of data subjects concerned as well as the volume of personal data being processed.

Even if you are not required to appoint a DPO, it's good practice to appoint someone to take responsibility within the firm for data protection matters and so you may choose to appoint one voluntarily. But if you appoint a DPO on a voluntary basis, that individual becomes subject to the same requirements of the GDPR as a compulsorily appointed DPO. Therefore, if you do not need or want to appoint a formal DPO, consider appointing a data privacy manager or similar alternatively titled role.

Data protection impact assessments (DPIA)

You must carry out a DPIA[24] in respect of certain higher risk processing, especially when implementing new technologies.

Generally, a DPIA should be conducted at the start of a project that could have significant data protection or privacy implications, e.g., rolling out a customer relationship management (CRM) or human resources system. The ICO provides a sample DPIA template.[25]

Data protection by design and by default

"Data protection by design" is an approach to ensure privacy and data protection issues are considered at the design phase of any system, service, product, or process and then throughout the lifecycle. "Data protection by default" requires controllers to implement appropriate technical and organizational measures to ensure that, by default, personal data is only processed as necessary to achieve a specific purpose.[26]

Data processors

Law firms may engage with a range of providers to obtain services that may include processing of personal data on their behalf. Such services could include use of software as a service (SaaS), outsourced IT services, payroll, or hosting of data. The GDPR[27] requires that such processing must be governed by a written contract containing certain minimum obligations on the processor (and requiring that the processor flows down such obligations to any sub-processors it may have). It is, therefore, necessary to keep under review the list of processors that the firm engages and ensure that the appropriate compliant contracts are in force.

Individual rights

The individuals (data subjects) whose personal data you process have a range of rights – known as data subject rights. The main data subject rights that will be applicable to law firm data processing are:

- Access (data subject access request (DSAR)) – the right to access and receive a copy of their personal data.[28]
- Rectification – the right to have inaccuracies corrected.[29]
- Erasure – the right to have information erased, also known as the "right to be forgotten".[30]
- Objection to direct marketing – individuals have the absolute right to object to the processing of their personal data for direct marketing purposes.[31]

- Objection based on legitimate interests – an individual can also object to the processing where you rely on "legitimate interests". This is not an absolute right, and you can refuse to comply if you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual, or if the processing is for the establishment, exercise, or defense of legal claims.[32]
- To prevent automated decision-making and profiling, individuals have the right not to be subject to a decision based solely on automated processing (without human involvement in the decision-making process) which produces legal effects or similarly significantly affects him or her. This could apply, for example, to online recruitment tests that may use defined criteria to filter out certain applications.[33]

In practice, the DSAR is the right most exercised. If a controller receives a DSAR, they must provide the information requested *"without undue delay and in any event within one month of receipt of the request"*.[34] Exceptionally, that period may be extended by two further months where necessary, taking into account the complexity and number of the requests.[35]

There are a number of exemptions to the right of access to information. Importantly, one person's right of access has to be balanced against another person's rights to protection of their personal information. Under the DPA, a controller is not obliged to disclose information to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information, unless: *"(a) the other individual has consented to the disclosure of the information to the data subject, or (b) it is reasonable to disclose the information without the consent of the other individual"*.[36]

A further exemption that will be helpful to law firms and their clients provides that the right of access does not apply to personal data that consists of: *"(a) information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings, or (b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser"*.[37]

It is good practice, therefore, to review your internal processes for dealing with DSARs and implement a policy to enable staff to recognize a DSAR and define how you will handle requests within the timescales specified by the GDPR and apply the various exemptions.

Personal data breach

The GDPR imposes a requirement to notify a personal data breach to the ICO.[38] Not all breaches have to be notified – only those where data subjects are likely to suffer some form of damage, e.g., through identity theft or a confidentiality breach.

When notification to the ICO is required, it must be done *"without undue delay and, where feasible, not later than 72 hours after having become aware of it"*.[39] A justification must be provided if this timeframe is not met.

In addition, if the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must also communicate the personal data breach to the data subject *"without undue delay"*.[40]

Law firms suffering a personal data breach may also need to report the matter to the Solicitors Regulation Authority and, in appropriate cases, to their insurers.

It is essential, therefore, both for compliance and to mitigate liability, to implement and maintain a data breach incident response plan to detect, investigate, and report, and manage the consequences of, a personal data breach.

Whether or not a personal data breach is reportable, it needs to be documented in a personal data breach register, including the facts relating to the breach, its effects, and the remedial action taken.[41]

International data transfers

The EU GDPR restricts[42] transfers of personal data to a separate organization located outside of the European Economic Area,[43] unless the rights of the individuals in respect of their personal data are protected. The UK GDPR similarly restricts transfers outside of the UK. Transfers are permitted where:

The receiver is located in a third country covered by an "adequacy decision". Currently, following Brexit, the UK is covered by an adequacy decision of the EU, and UK adequacy regulations include the EEA and all countries covered by EU "adequacy decisions";[44]

Appropriate safeguards are in place – such as the standard contractual clauses for international data transfers as approved by the EU or the UK;[45] or

A derogation is in place, such as the individual has given explicit consent to the transfer, or (for occasional transfers) the transfer is necessary for the establishment, exercise, or defense of legal claims.[46]

Reliance on standard contract clauses is commonplace in transactions involving data transfers. However, this has become more complex following

the case of *Schrems II*.[47] It is now necessary to carry out and document a transfer impact assessment and, if the assessment is that the appropriate safeguard does not provide the required level of protection, you may need to include supplemental measures.

In the context of the data mapping (see above), it is good practice as a first step to map your international data flows and identify any transfers of personal data outside the UK/EEA, the parties involved, and the purposes of the transfers.

Marketing and cookies

Email marketing

In addition to the GDPR, under the ePrivacy Directive/ePrivacy Regulations (PECR),[48] firms must comply with PECR when sending unsolicited texts or emails to generate marketing. What is permitted by PECR depends on whether the direct marketing is aimed at a business or an individual. Generally, it is not permitted to send unsolicited texts or emails to individuals without their specific consent, save in limited situations when marketing similar products or services to existing clients or contacts who have expressed an interest in your products or services, and who have not objected. Marketing emails to corporate email addresses do not require prior consent.

As referred to above (Individual rights), data subjects have the right to object at any time to their personal data being processed for direct marketing purposes. Every marketing email should include an email address or web link where individuals can easily unsubscribe from future emails. Firms need to have a process in place to ensure that opt-outs are respected.

Websites and cookies

PECR also provides that website owners that set cookies or access information on their users' equipment are required to:

- Provide users with clear and comprehensive information about the purposes for which cookies are stored and accessed; and
- Obtain users' consent.[49]

There are limited exemptions for cookies that are "strictly necessary" for the provision of the service requested by the user.[50]

It is good practice to carry out a cookie audit to determine what cookies are used on your website and the purposes of each. Details should then be set out in a Cookie policy published on the website and a mechanism included on the site to ensure that cookies that are not "strictly necessary" are not set unless and until the user has specifically opted-in.

Conclusion

Good data protection practices and policies are essential for compliance and risk management. However, there are many other sound business reasons why they are important, including to maintain the confidence of clients and others with whom you deal that you will secure and respect the sensitive personal data that they entrust to you.

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
2. The version of the GDPR transposed into UK law pursuant to the European Union (Withdrawal) Act 2018.
3. Article 4(7) GDPR.
4. See www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/#3.
5. Article 4(8) GDPR.
6. Law Society Guidance for solicitors in law firms (GDPR and the Data Protection Act), September 2019.
7. Under the Data Protection (Charges and Information) Regulations 2018.
8. As defined in the Schedule to The Data Protection (Charges and Information) Regulations 2018.
9. Article 5 GDPR.
10. Article 14(5)(b) GDPR.
11. DPA Schedule 2 Part 4 paragraph 19(a).
12. DPA Schedule 2 Part 4 paragraph 19(b).
13. Article 5(1)(e) GDPR.
14. Article 32 GDPR.
15. www.ico.org.uk/action-weve-taken/enforcement/tuckers-solicitors-llp-mpn/
16. www.ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx
17. DPA, Schedule 1, Part 2.

18. Data Protection Act 2018, Schedule 1, Part 2, Paragraph 5.
19. DPA, Schedule 1, Part 1, 2 and 3.
20. www.ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx
21. Article 30(5) GDPR.
22. Article 37 GDPR.
23. Guidelines on Data Protection Officers (DPOs) WP 243 rev.01, as last revised and adopted on 5 April 2017.
24. Article 35 GDPR.
25. www.ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx
26. Recital 78 and Article 25 GDPR.
27. Article 28 GDPR.
28. Article 15 GDPR.
29. Article 16 GDPR.
30. Article 17 GDPR.
31. Article 21(2) GDPR.
32. Article 21(1) GDPR.
33. Article 22 GDPR.
34. Article 12(3) GDPR.
35. Article 12(3).
36. DPA Schedule 2, Part 3, Paragraph 16.
37. DPA Schedule 2, Part 4, Paragraph 19.
38. Article 33 GDPR.
39. *Ibid*.
40. Article 34 GDPR.
41. Article 33(5) GDPR.
42. Article 44 GDPR.
43. EU countries and also Iceland, Liechtenstein, and Norway.
44. Article 45 GDPR.
45. Article 46 GDPR.
46. Article 49 GDPR.
47. Data Protection Commission v. Facebook Ireland and Maximillian Schrems, 16 July 2020, Case C-311/18.
48. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended).
49. *Ibid*, Regulation 6.
50. *Ibid*, Regulation 6(4)(b).