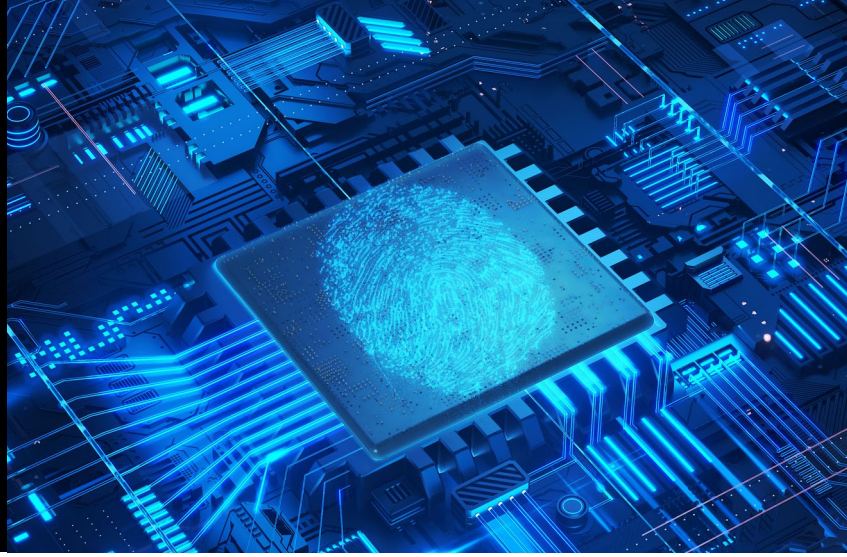
LOCKTON

Lockton Solicitors

GUIDE TO PRIVACY POLICY



INTRODUCTION

A Privacy Policy (sometimes referred to as a privacy notice or privacy statement) is a document setting out an organisation's policy on collecting and handling personal data. It contains all privacy related information that an organisation needs to make people aware of when they collect their personal data.

The main purpose of a Privacy Policy is to communicate to an individual how their data is collected and used.

The obligation to produce a Privacy Policy requires a business to consider what personal information they collect, how it is used and whether they do so in accordance with the requirements of data protection law.

THE LEGISLATIVE AND REGULATORY REQUIREMENTS

Why we need a Privacy Policy

The UK General Data Protection Regulation (UK GDPR) as supplemented and tailored by the UK Data Protection Act 2018 (DPA) forms the UK's data protection regime.

The UK GDPR requires those controlling personal data to give individuals certain information whenever you collect their personal data, this is usually done by way of a Privacy Policy.

Paragraph 2.1 of the SRA Code of Conduct for Firms (COCF) requires that you have effective governance structures, arrangements, systems and controls in place that ensure you comply with all the SRA's regulatory arrangements, as well as with other regulatory and legislative requirements which apply to law firms.

You should therefore ensure that your Privacy Policy complies with data protection law.

WHAT DOES A PRIVACY POLICY HAVE TO SAY?

Articles 13 and 14 of the UK GDPR set out the types of information that you need to provide to individuals.

The purpose of the information is to ensure fair and transparent processing of that information, so that an individual knows what you are doing with their data and why, as well as being informed of their rights in relation to that data.

Your policy should be clear, concise and easy to understand.

WHAT PRIVACY INFORMATION IS REQUIRED AND WHEN DO WE HAVE TO PROVIDE IT?

Article 13(1) of UK GDPR states that you have to provide this information "at the time when personal data are obtained".

This applies when you collect the data directly from someone (e.g. they provide you with their passport), or by observation (e.g. when you use CCTV to monitor people).

Article 13(1) sets out the information youArticle 13(1) of UK GDPR states that you have to provide this information "at the time when personal data are obtained".

This applies when you collect the data directly from someone (e.g. they provide you with their passport), or by observation (e.g. when you use CCTV to monitor people).

Article 13(1) sets out the information you have to provide:

a. The identity and the contact details of the controller and, where applicable, of the controller's representative;

b. The contact details of the data protection officer, where applicable;

c. The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d. Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

e. The recipients or categories of recipients of the personal data, if any;

f. Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Article 13(2) sets out details of further information that you must provide, again, at the time when personal data are obtained:

a. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b. The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c. Where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

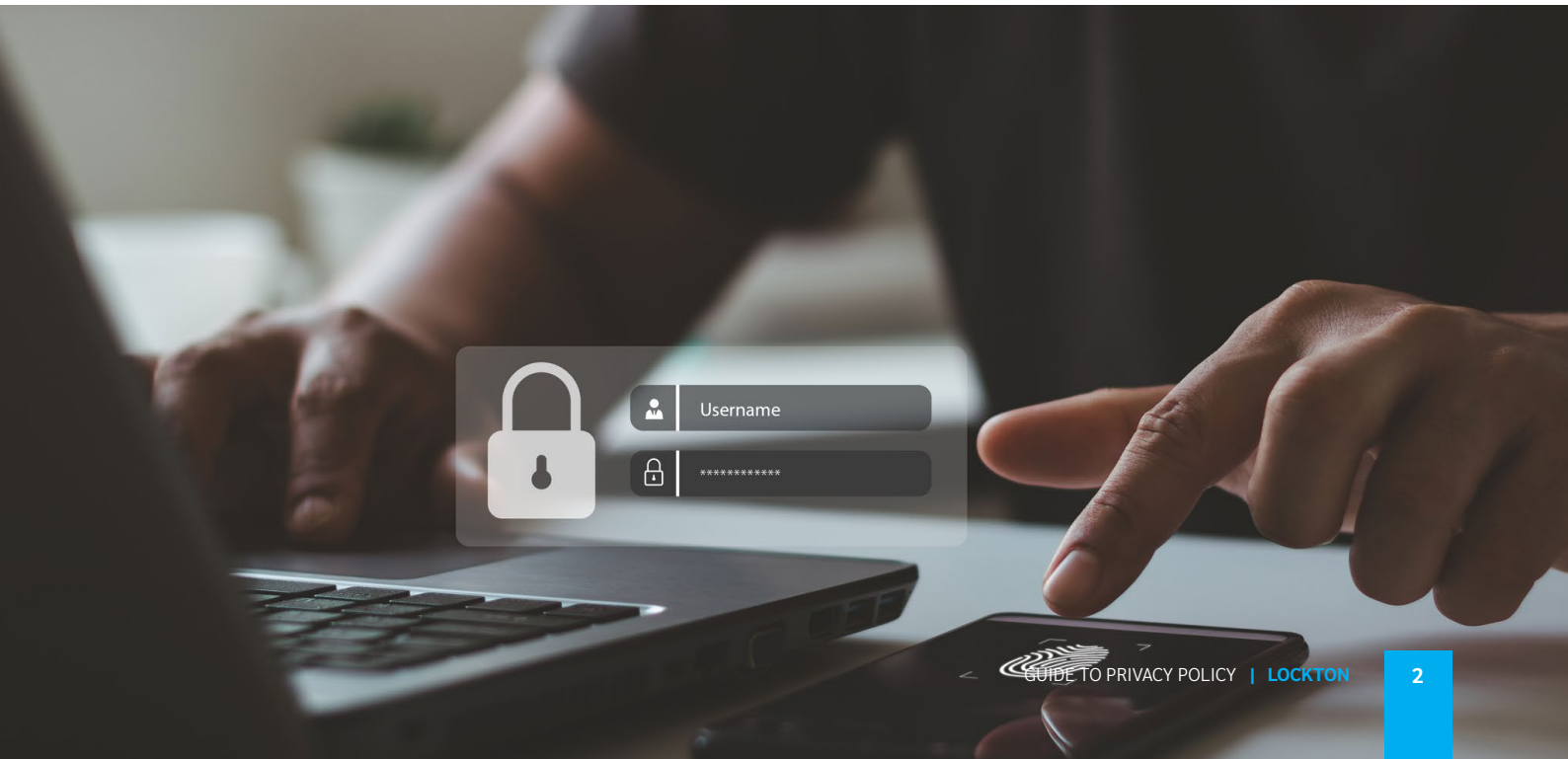
d. The right to lodge a complaint with a supervisory authority;

e. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f. The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Article 13(3) requires data controllers (i.e. the firm) to provide further information to individuals if they intend to process the data collected for other purposes than that for which it was originally collected.

Article 13(4) provides that you do not need to provide individuals with the information above (in Articles 13(1), (2) and (3) if they already have that information.



RECEIVING DATA FROM THIRD PARTIES

What do we do if we receive information from someone other than the data subject?

You must still provide privacy information to the data subject if you do not obtain information directly from them.

The information must be provided:

- Within a reasonable period of obtaining the data, but at the latest within one month, having regard to the specific circumstances in which the data are processed;
- If the personal data are to be used to communicate with the data subject, at the latest at the time of first communication to that data subject; or
- If a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

The information requirements are very similar to those listed in the above paragraph and also include the source of the information. Full details are found in Article 14.

HOW DO WE HAVE TO PROVIDE THE INFORMATION?

Whilst many organisations provide privacy information via their website, this is not mandatory and there are different ways in which you can provide this information.

The Information Commissioner's Office (ICO) has made it clear that you can provide the information in a number of ways as follows:

- Orally, face to face or when you speak to someone on the telephone - if you do use this method, you should document the process so you can evidence it if necessary.
- In writing, by way of printed media such as adverts and forms, e.g. a job application form.
- Through signage e.g. using a sign in a public area to inform people that CCTV is in operation at your offices.
- Electronically using text messages, websites, emails or mobile apps.

Some firms choose to provide their staff with privacy information via their staff handbook or a link on their firm's intranet – whatever method you use, you should make it clear to staff where they can find this information.

Organisations are also permitted to use a blended approach to provide privacy information. A popular method is a layered approach which would typically consist of providing people with an initial short notice containing key information, such as your firm's identity and the way you use personal data, and the notice may contain links that expand each section, revealing a second layer, or just a single link to more detailed information.

WHAT IF WE DON'T PROVIDE THE PRIVACY INFORMATION?

The right to be informed is considered a fundamental aspect of the UK GDPR and firms risk significant fines and reputational damage if they fail to comply with their obligations under data protection law.

What to do next

We recommend that firms take the following steps:

- Appoint an appropriate person to be responsible for producing and ensuring that your Privacy Policy is kept up to date to reflect the Firm's use of personal information.
- Any material changes to your Privacy Policy should be highlighted on your website so that clients can find this easily. Similarly, if you have a separate policy for staff, material changes should be flagged to them.
- Prepare or review your Privacy Policy. You will need to ensure that your policy contains all the information required under UK GDPR. The ICO provides useful guidance on the right to be informed and preparation of your policy (see Useful Resources below).
- Training - when you provide data protection training to staff, this should include an overview of your privacy policy (i.e. why you need it and where it can be found). This may be useful for staff if they receive enquiries asking for your firm's Privacy Policy. If you have a separate Privacy Policy for staff, you may wish to inform staff of this fact during training and remind them where they can find it.
- Annual review: Appoint an appropriate person to be responsible for reviewing and auditing your Privacy Policy to ensure that it remains compliant with data protection law. The person appointed should keep appropriate records documenting the review process.

Useful resources

ICO Guidance:

The right to be informed | ICO