1 Introduction

This procedure is intended to be used when a new or changed business process is put in place which requires the collection of personal data from data subjects that fall within the scope of the European Union General Data Protection Regulation (GDPR).

The GDPR, mainly in articles 13 and 14, requires that specific information is provided at the point of data collection or receipt which informs the data subject about the use that the data will be put to, and their rights over that data. This information will vary according to the specific circumstances and this procedure should be used to ensure that the correct information is given in the correct format so that Mighton Products remains compliant with the GDPR at all times.

Whereas in the past, information regarding privacy has tended to be provided in a single [illegible] individual privacy notices are used according to the transaction involved. For example, one privacy notice may be displayed when an order is taken on a website, and a different privacy notice is displayed when a user signs up to receive a newsletter. This allows the privacy information provided to be more transparent and less confusing for the data subject.

Such privacy notices may be used in conjunction with a more traditional privacy policy if desired.

This procedure should be considered in conjunction with the following related documents:

- Privacy notice planning form – Data subject
- Privacy notice planning form – Other source
- Data protection impact assessment process
- Records Retention and Protection Policy
- Data protection policy
- Legitimate interest assessment procedure

2 Privacy notice procedure

The purpose of this procedure is to create an appropriate privacy notice which provides the data subject with the information they are required to receive, in as fair and transparent a way as possible.

There are two main ways of obtaining personal data which are covered by the GDPR. These are:

1. Where personal data are collected from the data subject *(*GDPR Article 13*)*
2. Where personal data have not been obtained from the data subject *(*GDPR Article 14*)*

In both cases, the GDPR specifies the information that must be provided to the data subject. This procedure describes that information and explains how to create a privacy notice that meets the requirements.

2.1 Does the data subject already have the information?

The GDPR requires the data subject to be provided with the listed information **unless the data subject already has the information**. It is therefore important to determine whether it is reasonable to believe that the data subject is already aware of all of the information that would otherwise be required to be provided.

Where this is the case, the rationale for this belief must be documented and retained as evidence of GDPR compliance. Care should be taken to ensure that this applies to **all** of the information required and **all** of the data subjects affected, otherwise steps should be taken to address any gaps.

2.2 Where personal data are collected from the data subject

In the event that the data subject does not have the information required, the following must be provided at the time when personal data are obtained:

1. Identity and contact details of the controller and, where applicable, of the controller's representative
2. Contact details of the data protection officer, where applicable
3. The purposes and legal basis of the processing (e.g. consent, legal obligation, legitimate interest)
4. The legitimate interests pursued by the controller, or by a third party (if legitimate interest is defined as the lawful basis of the processing)

5. The recipients, or categories of recipients, of the data, if any
6. Details of any planned transfers of personal data to a third country or international organisation
7. The length of time that the personal data will be stored for (or the criteria used to determine that period)
8. The data subject's rights to access, rectification, erasure and portability of the personal data (depending on the lawful basis used, see below)
9. The data subject's rights to restriction of, or objection to, processing of their personal data
10. The data subject's rights to withdraw consent at any time (if consent is used as the lawful basis of the processing)
11. The data subject's right to lodge a complaint with a supervisory authority
12. Whether the collection of the personal data is a statutory or contractual requirement and whether they are they obliged to provide it
13. Whether the personal data will be subject to automated processing, including profiling and, if so, the logic and potential consequences involved

Care must be taken to explain the data subject's rights in the context of the lawful basis of the processing. For example, if the lawful basis is contractual then the right to withdraw consent does not apply (see the Data Subject Request Procedure for more information).

2.3 Where personal data have not been obtained from the data subject

If the personal data are not obtained directly from the data subject, there are a number of additional circumstances (i.e. in addition to the case where the data subject already has the information) allowable by the GDPR that mean that the information does not have to be provided. These are:

- If the provision of the information proves impossible or would involve a disproportionate effort
- Where it is covered by other applicable law(s) which provide appropriate measures to protect the data subject's legitimate interests (GDPR Article 14)
- Where the data is confidential under law

Where any of the conditions apply, the rationale for this belief must be documented and retained as evidence of GDPR compliance. Care should be taken to ensure that this applies to **all** of the information required and **all** of the data subjects affected, otherwise steps should be taken to address any gaps.

In the event that none of these conditions apply, the information must be provided to the data subject:

- within a reasonable time, at the latest one month after obtaining it
- if used for communication (eg email addresses), at the latest when the first communication takes place
- at the point where the data are disclosed to another recipient (if applicable)

The information to be provided is as follows:

1. Identity and contact details of the controller and, where applicable, of the controller's representative
2. Contact details of the data protection officer, where applicable
3. The purposes and legal basis of the processing (e.g. consent, legal obligation, legitimate interest)
4. The categories of personal data concerned
5. The recipients, or categories of recipients, of the data, if any
6. Details of any planned transfers of personal data to a third country or international organisation
7. The length of time that the personal data will be stored for (or the criteria used to determine that period)
8. The data subject's rights to access, rectification, erasure and portability of the personal data (depending on the lawful basis used, see below)
9. The data subject's rights to restriction of, or objection to, processing of their personal data
10. The data subject's rights to withdraw consent at any time (if consent is used as the lawful basis of the processing)
11. The data subject's right to lodge a complaint with a supervisory authority
12. The origin of the personal data
13. Whether the personal data will be subject to automated processing, including profiling and, if so, the logic and potential consequences involved

As for when the personal data is obtained directly from the data subject, the data subject's rights will depend on the lawful basis of the processing.

2.4 Informing the Data Subject

There are two Privacy notice planning forms available; one to be used where the personal data are collected directly from the data subject, and the other where the personal data are obtained from another source. Use the relevant form to ensure that all of the required information has been captured before it is put into the appropriate format for communication to the data subject.

As with all information provided to data subjects in accordance with the GDPR, the information must be in an intelligible and easily-accessible form, using clear and plain language. The best method of providing the information to the data subject will depend upon the specifics of the business process and may include one or more of:

- As a notice on a website
- Via email
- Via physical post
- By telephone
- Face to face

The approach to privacy notices needs to be carefully planned so that the relevant information is presented to the data subject at the appropriate time. This will tend to mean that a coherent set of privacy notices is required, rather than a single document that covers all processing. Each privacy notice should be designed to be displayed at the appropriate point in the business process and be specific to the information being collected, the purpose for which it will be put and the lawful basis of the processing involved. This is often referred to as a "just in time approach" to privacy notices.

Equally, the best way to present the information should be carefully considered. Presenting a link to the relevant privacy notice document may meet the requirements of GDPR on a website, but alternative methods of screen design may allow a smoother user experience.

2.5 Further Processing

However it is obtained, if it is decided to use the personal data for a purpose other than that for which the data were obtained or collected, further information about that purpose, and the basis on which it is deemed lawful, must be provided to the data subject before the processing happens.