GDPR Documentation and Drafting Notes

When you are using these templates it is your responsibility to understand when and how to use the templates and notes appropriately and how to tailor them as appropriate to your circumstances. Neither Lodders Solicitors LLP ("Lodders") or the BCA accept responsibility or liability in relation to the use of the templates or notes.

Mark Lewis, a Partner at Lodders, is our adviser of choice if you would like assistance to populate these documents. As the majority of the work has already been undertaken, any additional costs should be relatively limited and to be agreed directly with Mark by individual members. Please contact Mark by email: mark.lewis@lodders.co.uk.

BCA members already relying on consent for their legal basis to process data in relation to marketing

Lodders cannot provide generic advice in relation to what you need to do in relation to the current consents you have already obtained because it will depend on whether the consent you have gathered is sufficient.

One example where current consent gathered is no longer adequate is where the consent has been gathered using a pre-ticked box. In this circumstance you would need to collect new valid consents to continue marketing to those individuals.

Therefore if the current consent is not sufficient, or if you are unsure, it would be wise to send an email requesting individuals on a marketing list to opt-in to continue to receive marketing from them. Although you must be aware that if you do this then you cannot send marketing emails to those individuals again unless they have provided the new consent.

Please refer to the ICO website for more guidance in relation to consent: **www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/.**

Contracts you have with patients

The documentation is drafted on the assumption that patient data is processed on the basis of a contract and the special condition relating to health, namely that the processing is necessary for the purposes of the provision of health treatment pursuant to contract with a health professional.

Therefore, you should not need consent to process a patient's data in terms of data protection law.

In terms of referring to data protection in your contract with the patient (i.e. a new patient form) you should insert the following clause:

> ***"How we will use your personal information***
>
> *We will only use your personal information as set out in our Patient Privacy Notice, which is available on our website and behind reception if you would like to find out more information."*

Documentation

A data controller needs to be able to demonstrate compliance with the principles detailed in the GDPR, which are in summary:

1. Processing lawfully, fairly and transparently;
2. Collecting data for specified, explicit and legitimate purposes;
3. Minimising data held;
4. Ensuing data held is accurate;
5. Storing data for no longer than is necessary; and
6. Processing in a manner which ensures appropriate security of the data.

Below is a list of documents which will help you to demonstrate compliance. It would be advisable to have all of these documents in one place which is accessible to all employees should they wish to refer to them – for example in a hard copy folder or on an intranet. Some of the documents also need to be publically available and where this is necessary it is indicated in the table below.

	DOCUMENT	EXPLANATION
1	**Patient Privacy Notice** **(Public)**	The GDPR requires all controllers to notify data subjects about their personal data handling though a privacy notice. A Privacy Notice describes what how and why personal data is collected and used. This document is drafted on the assumption that patient data is processed on the basis of contract and the special condition relating to health, namely that the processing is necessary for the purposes of the provision of health treatment pursuant to contract with a health professional. You will need to consider whether this document accurately reflects how your clinic uses personal data and amend it accordingly. You will see that there are sections that you will need to populate which are written in red and also comments are made. This document should be available to the patient at the point their data is

		collected, therefore it will need to be available at the clinic and it would be advantageous to also have the document available online. The patient does not need to sign to say they have viewed/received this notice.
2	**Patient Privacy Notice Summary (Public)**	This is a summary of the Patient Privacy Notice that you could laminate and keep in a waiting area for patient to review while waiting for their treatment.
3	**Privacy Notice – under 16s** **(Public)**	The GDPR requires that where children's data is processed you need to have a separate privacy notice aimed at children. This notice is therefore a simplified version of the patient privacy notice and the website notice. Again it is drafted on the basis that a contract has been entered.
4	**Website and Marketing notice** **(Public)**	This document details how the clinic uses data it collects on its website and also explains the marketing activities of the clinic. This document is drafted on the assumption that marketing is only carried out if express consent of the individual has been received. You may need to consult with your website host to determine what technical data is used on the website and how it is used. This document should be placed on the website for individuals to view.
5	**Legitimate Interest Assessment**	When relying on legitimate interest as a basis to process data you must carry out a legitimate interest assessment. This is your evidence as to why you consider it appropriate to use this ground. It is important that you consider carefully, and amend as appropriate, the explanatory wording in the form. The privacy notices are drafted on the basis that legitimate interest basis is only used in relation to website processing and also to collect any unpaid bills. Accordingly the legitimate interest only covers these two areas. Assumptions have been made as to why you collect data on your website. Therefore if your website does not collect data for the purposes detailed you will need to amend this assessment.
6	**Employee Privacy Notice**	This notice notifies employees about the personal data that the you holds relating to them, how they can expect their personal data to be used and for what purposes This policy will need to be carefully reviewed and amended as appropriate. At the end of the document you will see an acknowledgement of receipt. The

		GDPR does not require the employee to sign to acknowledge receipt, however, as best practice, employers often request that employees sign an acknowledgment to demonstrate that they have been properly informed of their data collection and handling practices. Therefore, it is your choice whether you wish to remove this.
7	**Candidate Privacy Notice**	This policy notifies prospective employees about the personal data that you propose to hold relating to them, how they can expect their personal data to be used and for what purposes. This policy will need to be carefully reviewed and amended as appropriate. At the end of the document you will see an acknowledgement of receipt. The GDPR does not require the data subject to sign an acknowledgment of receipt, although it may be seen as good practice. However, it might be thought cumbersome to ask for this in relation to mere applicants, because of the transitory nature of the relationship. Again, it is your choice whether you wish to remove this.
8	**Privacy Standard (Internal Policy)**	This is the internal-facing policy to set out the principles and legal conditions that must be satisfied when obtaining, handling, processing, transporting or storing personal data in the course of your operations and activities, including customer, supplier and employee data. At the end of this document it gives the opportunity for employees to acknowledge receipt and review of the policy. You may feel this is unnecessary and therefore can remove it.
9	**Training handout**	This handout briefly explains the GDPR and can be used in an employee training session or circulated among employees. It would be pertinent to give a training session to all employees and get them to sign a sheet as evidence they have received training on data protection.
10	**Subject Access Request Procedure**	This document is important so that employees in your organisation know how to deal with SARs. SARs must be dealt with in a timely fashion and within 30 days of receipt. This template procedure demonstrates the necessary considerations and can be amended in any way you think is appropriate to fit in with your reporting processes.
11	**Subject Access**	Subject Access Requests do not have to be made in any standard form.

	Request Forms	However, you will need certain information from the individual to facilitate their request. This template can be sent to an individual when they make a request for personal data to ensure you gather this necessary information.
12	**Privacy Impact Assessment**	This is a standard form document designed to provide a framework for carrying out an assessment. This document is intended as a starting point for data controllers and should be amended depending on the nature and scope of the any initiative you may need to use it on. When you do have to carry out an assessment please be aware that it will be useful to complete the fact gathering section first (namely section 7). Be mindful that the assessment should be reviewed regularly and reassessed. When keeping this document on file in the event you do need to carry out an assessment it would be useful to the ICO's "Data Privacy Impact Assessments Guide available at: www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/ You may wish to consider carrying out retrospective assessments in respect of existing processing activities which may be deemed high risk.
13	**Data Breach Register**	This will be used as and when a breach occurs to keep a record of the steps taken.
14	**Data Breach Incident Response**	This document will help you to assess the risks associated with a breach when a breach occurs.
15	**Data Breach Plan**	This is put in place before a breach occurs. It details what the process is if a breach occurs and therefore should enable you to respond to any personal data breach quickly and effectively to minimise any adverse consequences of the breach.
16	**Risk register**	There is no requirement to have a risk register, however it is a useful tool for assessing risks within your organisation.

17	**Records Management Policy**	This document will demonstrate that you have considered the length of time to keep personal data and records the decisions you have come to in relation to how long you retain and then how you will dispose of the data. Appendix 2 will need to be amended to include information in relation to how your clinic retains other data not currently included, for example patient data.
18	**Data Processing Agreement**	The GDPR requires that a written contract is in place between controllers and processors to document the instructions of the controller. This document outlines the respective obligations of the parties and is drafted to be "pro-controller". Therefore you can populate this document in relation to any data processors you engage. For each processor you will have to populate the schedule to relate to that agreement and change the parties names, otherwise the document can remain the same.