General data protection regulation toolkit

Introduction

This toolkit applies the main General data protection regulations (GDPR) provisions to a clinics' setting and provided links to further reading. Each clinic should consider the issues addressed throughout this toolkit so as to satisfy itself that its data processing is GDPR compliant.

GDPR in brief

Clinics are **Data Controllers** for the purpose of the GDPR.

A Data Controller means 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. The GDPR states that the Data Controller 'must be able to demonstrate compliance'. [1]

As clinics regularly deal with vulnerable individuals, including those who suffer mental and physical health problems, as well as children, the risks associated with data processing are self-evidently greater. These individuals will be entitled to greater protection under the GDPR. For example, it might not be sufficient to merely include a bald reference to a complaints procedure in letters of engagement, as this would require a complainant to contact the clinic directly, possibly even the person whom they wish to complain about, in order to establish how and to whom to complain. Clearly, for some individuals this would have the effect of dissuading them from complaining. Clear information, provided up-front in clinics' paperwork, should be the rule of thumb. Clinics' complaints procedures should generally encourage clients to address their concerns with the clinic in the first instance. Please refer to LawWorks' complaints handling resources on our website.

It is a requirement of the GDPR that everybody involved in clinics have the necessary skills and knowledge to be able to apply the law in their day-to-day work. To that end, clinic coordinators should keep a log of who has been trained and when, and build this into the induction process for any new staff, volunteers and trustees.

Reasons for processing data

Coordinators must ensure that clinics can rely on at least one of the necessary valid reasons for processing each type of data. For clinics purposes they are likely to be:[2]

- **Consent** which is demonstrably clear, recorded and is able to be withdrawn. For example, written consent is the only valid basis for processing sensitive personal data;[3]

---

[1] A **Data Processor** means '*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*'. This could be, for example, a third-party fundraiser or a data destruction company. This means clinic staff, volunteers, contractors and temporary staff are not classified as Data Processors for the purpose of the GDPR.

[2] For a comprehensive list of valid reasons see the GDPR.

- Necessity in relation to a **contract**; for the purpose of the GDPR the pro bono retainer (e.g. a Letter of Engagement) will be sufficient (or any other relevant documentation setting out the basis of acting). In the absence of any documentation the contract or retainer between clinics and clients will be oral and implied;
- In accordance with the "**legitimate interests**" condition. The 'legitimate interests' ground encompasses, for example, research and statistical analysis.

What to do next?

Using the table below, you should review clinic's processes to obtain information regarding the collection, handling, processing or storing of personal data. This will lead to a better understanding of what personal data clinics process and create a tangible overview of:

- the nature of the personal data collected by the clinic;
- the purposes for which personal data is processed;
- how such data is stored and details of any relevant policies and security measures in place;
- who the clinic shares personal data with; and
- how the clinic shares and transfers that data.

The three main areas where clinic coordinators should consider whether any remedial action should be taken are as follows:

1. **Lack of formal data protection / retention policies**
2. **Lack of compliance training/guidance for staff (including volunteers)**
3. **Inadequate security measures to protect personal data**

The table below sets out a number of suggested action points, which will help to address the risk areas listed above and further ensure that the clinic adequately protects the personal data that it collects and processes it in accordance with the law.

Personnel	Action
Clinic Coordinator	• Adopt a policy confirming the clinic's commitment to protecting the personal data of its staff (including, volunteers) and clients. Share this with staff and circulate via the clinic website (where appropriate) ["*Accountability*" Art.52, GDPR]. • Allocate responsibility for GDPR compliance to a designated individual (e.g. a Compliance Officer (CO)).

[3] 'Sensitive personal data' includes information about individuals' health, finances, as well as racial, ethnic, religious information or information concerning children.

	Clinic Coordinators may be best placed to take on this function. Generally, clinics will be **unlikely** to need to formally appoint a Data Protection Officer (DPO) under the GDPR; DPOs attract significant legal obligations of a personal nature, in which case clinics should avoid this terminology when allocating the role. • The person with responsibility should monitor and oversee compliance by the clinic with data protection laws. For convenience, throughout this toolkit the clinic person with overall responsibility is referred to as the CO.
Data audit	• The CO should gather information about the following (see the **Data Protection Questionnaire** to assist in this regard): o the personal data that the clinic collects and stores [GDPR - *data audit;* see, for example, LexisNexis' PSL online resources, using the search term, "data protection audit questionnaire". Alternatively, consult the ICO website]; o why it collects and stores this data, both factually and by relevance to the above list of valid reasons [GDPR – *purpose*]; o whether it is absolutely necessary to collect all of the data that it does [GDPR - *adequacy, relevance, necessity of data processing*]; and o how long it is absolutely necessary to retain the information for [GDPR – *necessity; clinics should adopt a retention policy: see LawWorks' template Privacy Notice*]. o Whether the data is or continues to be accurate [GDPR – *accuracy*] • The CO should then be in a position to answer the following questions about the data collected (see the data protection questionnaire in LexisNexis' online resources, using the search term, "data protection audit questionnaire" to assist with this task. Alternatively, consult the ICO website): o *Do the people I am collecting it from know what it will be used for (clients should have sight of clinic's Privacy Notice at the outset of a matter)?* o *Will the information be held safely and securely (for example, see LawWorks' guidance relating to confidentiality of client information.*

	o *Are websites or online forms used to collect data encrypted and/or password protected?* o *How can I ensure that information held is accurate and up to date?* o *Do I know how to transfer or send data securely?* o *Will the information be properly deleted or destroyed when it is no longer needed?* o *Are other people in the clinic aware of data protection rules and our policies?* o *Do they know how to handle, store and use data properly?* o *Do our marketing communications give people an easy way to opt out of receiving them?* o *If someone asked to see a copy of the information we hold on them, do I know how to handle their request (see below under the heading, "Subject Access Request")* o *If I am asked to provide personal or sensitive data, do I know what steps to follow?* o *If there has been a breach or I see something that concerns me, do I know where to report it?* • The CO should record the valid GDPR reasons for processing the data. • A data protection policy should be put in place (for a data protection policy checklist see LexisNexis' PSL online resources, using the search term "data protection policy"). For other relevant privacy notices, such as website or staff (including volunteer) privacy notices, see LexisNexis' PSL online resources, using, for example, the search terms, "website privacy policy," or "privacy notice employment". • Training of staff, including volunteers, on data protection policies is essential to ensure that they are understood and complied with. A training record should be kept by the CO. • The CO and staff/volunteers must take the necessary steps to ensure that data is stored securely and adequately protected (using password protection or encryption, where feasible (e.g. encrypted USB sticks are relatively low cost), whether on clinics' internal hard drives or external servers. • Where staff/volunteers transfer personal data to third

	parties they must ensure that this is done securely, for example using secure file transfer sites or password protected zip files where necessary, and in accordance with any clinic policy. • A data breach policy should be put in place (for information about how to respond to a breach and producing a data breach policy, see LexisNexis' PSL online resources, using the search term, "data breach policy".
Staff (including volunteers)	• Add a data protection section and/or clause into staff and volunteer handbooks and/or letters of engagement, explaining the importance of keeping personal data secure. • Keep a record of all data protection training completed by both employees and volunteers.
Marketing	• Include a link to clinics' privacy policy in any marketing material
IT	• Create Remote Working and information sharing "dos and don'ts" policy, to support and reinforce training.
Legal	• Update current privacy policies to ensure that they are clear to clients, in particular that clinics may share personal data with third parties and who those third parties are. • Monitor the ICO's guidance on forms of consent to ensure the clinic is operating in accordance with accepted practices. Review LawWorks' data protection resources, including any relevant training and webinars. • Review the data protection provisions in all key existing data processing agreements. Negotiate amendments to any existing contracts that have insufficient data protection clauses. • Include robust data protection clauses in contracts / agreements going forward (to include an obligation to notify clinics promptly of any security breaches and, preferably, a right of audit in all data protection provisions contained in third party contracts).

Subject Access Requests

On receipt of a Subject Access Request, the requested personal data must be provided within one month and free of charge.[4]

For information about responding to a Subject Access Request see LexisNexis' PSL online resources, using the search term, "Subject Access Request".

Data Protection Policy

Clinics should put in place a data protection policy. Clinics' practice and policy should match!

For a data protection policy checklist see LexisNexis' PSL online resources, using the search term "data protection policy".

Right to be forgotten

Under GDPR, the 'right to be forgotten' enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Breach management

The GDPR contains a new materiality test before the duty to report to the ICO is triggered. Breaches must be likely to pose a risk to individuals' rights and freedoms, for example identity theft, financial, reputational loss or breach of confidentiality.

Examples of a data breach include, access by an unauthorized person, sending data to the wrong person, devices containing data being lost or stolen and the loss of availability of data.

Reporting to the ICO in respect of a material breach must be made within 72 hours, unless the risk to individuals is unlikely. Reporting can be via the telephone or online: https://ico.org.uk/for-organisations/report-a-breach/.

Retention of data

Under what circumstances can personal data be retained? Your data retention policy should consider what data is destroyed and when. Allocating staff to this will ensure it is kept in focus. The potential justifications for clinics' retention of personal data include the following (non-exhaustive) list:

- to comply with any legal or regulatory requirement;
- case documents may be relevant to an appeal out of time;
- so that case documents may be used as precedents;
- case documents may contain the results of research into the law, which may be relevant to a current case;
- instructions, facts or expert opinions in a previous case may be relevant to a current case;

[4] However, a 'reasonable fee' can be charged if the request is manifestly unfounded, excessive, or repetitive

- correspondence or instructions contain contact details which may be useful;
- case documents or records may be important when carrying out a conflict search;
- case documents in the event that a complaint is made or a claim is made against the clinic's insurers;
- the need to ensure that information is accurate and up to date;
- for the purposes of research and statistical analysis, subject to consent and/or the anonymization of information;
- retention of information is exempt for the general data protection principles, such as in connection with the exercise of the 'right to be forgotten'; and,
- in order to response to a subject access request.

Further reading/guidance

There is guidance as well as the full GDPR text available via the Information Commissioner's Website or here https://gdpr-info.eu/

Other useful resources

- Preparing for the GDPR 12 steps – ICO website
- Guide to the general data protection regulation (GDPR) – ICO website
- Data Protection self-assessment – getting ready for GDPR – ICO website
- Guidance for charities – ICO website
- Cyber Security: Small Charity Guide – National Cyber Security Centre
- Good complaints handling guide – Legal Ombudsman website

Updates

- Revision 2 updated retention of data section, 25/5/18