



GDPR Staff Training Programme

Policy Number	35
Version	2.0
Policy Contact	Matthew Betteridge
Date Issued	6 th July 2018
Amended	19 th May 2019
Review Date	19 th May 2020
Target Audience	Staff and Consultants
Approved by	OneCall24 Policy Team

This Document summarises OneCall24's Staff Training Programme on the General Data Protection Regulation (GDPR) 2018.

It should be used by all staff and consultants to learn about the GDPR and keep up to date with the latest developments.

It consists of the following sections:

1. Introduction.
2. Training Activities.
3. Next Steps.

1 Introduction

The new General Data Protection Regulation (GDPR) came into force on 25th May 2018 . It strengthens the previous rules under the Data Protection Act (1998) by introducing new obligations for organisations and rights for individuals and businesses will need to comply with the GDPR from that date or face steep penalties.

OneCall24 is committed to the principles inherent in the GDPR and particularly to the concepts of privacy by design, the right to be forgotten, consent and a risk-based approach. In addition, we aim to ensure:

- transparency with regard to the use of data;
- that any processing is lawful, fair, transparent and necessary for a specific purpose;
- that data is accurate, kept up to date and removed when no longer necessary;
- that data is kept safely and securely.

The training programme explains your responsibilities and the policies and procedures OneCall24 use to operate in accordance with these principles.

Start by filling in and saving a copy of the GDPR Training Record with the title '<replace with your name> - <date>' in the 'GDPR Training Records' folder on the O:/ shared drive (e.g. if your name is Bill Smith and the date is 5th June 2018 store it as 'Bill Smith – 5th June 2018'). You can download the GDPR Training Record from the 'Policies' folder on the O:/ shared drive.

Use this to document the Training Activities you have completed and the Next Steps you plan to do.

2 Training Activities

2.1: Activity 1: Video

OneCall24 would like you to watch the following video [Data Day Hygiene | Data protection training film](#). When you have, update your training record as indicated.

The video is designed to help you manage the personal information that you store and process. You will see examples of where the data protection principles are followed and where they are not.

Use the film to reflect on your own activities and the measures that you have in place to protect personal information.

- How many of the traps that this general practice fell into would you avoid by having effective systems in place?
- What do you think needs to change in your own behaviour to conform with the data protection principles?

Here's a quick reminder of eight data protection principles:

1. **Personal information must be processed fairly and lawfully.** Data that is not personally identifiable is not covered by the Act: effective anonymisation can facilitate legitimate data sharing, watch out for this towards the end of the film.
2. **Personal information must be processed for limited purposes.** Data should only be obtained for specific and lawful purposes, and should not be further processed in any manner incompatible with that purpose or those purposes. Watch out! there are bladders about trying to breach this principle: look how Emma gets hold of information she shouldn't.
3. **Personal information must be adequate, relevant and not excessive.** Keep an eye out for this about 2 minutes in.
4. **Personal information must be accurate and up to date.** How confident are you that the information held by Blackwell Medical Practice is entirely accurate and up to date?
5. **Personal information must not be kept for longer than is necessary.** Watch out for this after about 6 minutes.
6. **Personal information must be processed in line with the rights of data subjects.** This comes up around 9 minutes in.
7. **Personal information must be secure.** Appropriate technical and organisational measures must be taken against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. This crops up throughout the film: how many can you spot?.
8. **Personal information must not be transferred to other countries without adequate protection.**

2.2: Activity 2: GDPR Compliance Statement

OneCall24's **GDPR Compliance Statement** sets out OneCall24's commitment to data privacy and can be used to answer questions from clients about OneCall24's approach to GDPR.

Read and familiarise yourself with OneCall24's GDPR Compliance Statement which can be found in the 'Policies' folder on the O:/ shared drive. When you have, update your training record as indicated.

2.3: Activity 3: Data Privacy and Data Retention Policies

OneCall24's **Data Privacy Policy for Staff and Consultants** outlines how we define, process and manage your personal data. In addition, it highlights how you should process personal data for the business, how to deal with data breaches, and subject access requests. It includes detailed policies concerning your use of IT systems (email, internet, social media, corporate infrastructure, business applications, and infrastructure monitoring) that you must comply with.

OneCall24 also has a Data Privacy policy for Agency Workers which mirrors the policy for staff and consultants. It is used to ensure that Agency Workers understand how we define, process and manage their personal data. In addition, it highlights how they should process personal data for the business, how to deal with data breaches, and subject access requests. It includes detailed policies concerning their use of IT systems (email, internet, social media, corporate infrastructure, business applications, and infrastructure monitoring) that they must comply with.

OneCall24's **Data Retention Policy** sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within OneCall24. Adherence forms part of your terms and conditions of employment and any breaches of policy may be considered a disciplinary offence and could lead to dismissal.

Read and familiarise yourself with OneCall24's Data Privacy Policy for Staff and Consultants and Data Retention Policy. Both can be found in the 'Policies' folder on the O:/ shared drive. When you have, update your training record as indicated.

2.4: Activity 4: Data Breach Policy

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. OneCall24 needs to have a robust and systematic way of responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

OneCall24's **Data Breach Policy** outlines the obligations this places on staff to report actual or suspected personal data breaches; and sets out our procedure for managing and recording actual or suspected breaches.

Read and familiarise yourself with OneCall24's Data Breach Policy which can be found in the 'Policies' folder on the O:/ shared drive. When you have, update your training record as indicated.

2.5: Activity 5: Subject Access Request (SAR) Procedure

Data Subjects have the legal right to invoke SAR's on any organisation who holds their Personal Data, and the organisation has one calendar month to respond formally to the request. Failure to respond to the

request within one calendar month entitles the Data Subject to log a complaint with the Information Commissioners Office (ICO), the GDPR's governing body.

OneCall24's **Subject Access Request (SAR) Procedure** sets out the key features regarding handling or responding to requests for access to personal data made by data subjects, their representatives or other interested parties.

Found in the 'Policies' folder on the O:/ shared drive. When you have, update your training record as indicated.

3 Next Steps

Key to our success is staff awareness and understanding and we regularly update our policies and procedures:

- when there is any change to the law, regulation or our policy;
- when significant new threats are identified;
- in the event of an incident affecting our company or a competitor.

If you have completed each of the training activities detailed in section 2 within the last 12 months, you can regard your knowledge as up to date. If you haven't, then your knowledge is out of date.

If your knowledge is out of date you should complete the training activities immediately to bring yourself up to date.

*Whatever the status of your knowledge, you should **reserve time in your calendar** to remind you to when to next do the training activities. When you have, update your training record as indicated.*

*Finally, **keep an eye on what's new on the ICO website** at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/>. When you have, update your training record as indicated.*

Prevention is always better than cure. Data security concerns may arise at any time and we encourage you to report any concerns you have to the Head of Compliance. This helps us capture risks as they emerge, protect our company from personal data breaches, and keep our processes up-to-date and effective.