GDPR Staff Training Programme

Policy Number	35
Version	5
Policy Contact	Demoiselle Chidzuu
Date Issued	6th July 2018
Reviewed	01st June 2023
Review Date	01st June 2024
Target Audience	Staff and Consultants
Approved by	ONECS Policy Team

This Document summarises ONECS 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 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.

After Brexit, the UK is no longer regulated domestically by the European General Data Protection Regulation (EU GDPR), which governs processing of personal data from individuals inside the EU. As the transition period came to an end in the UK, from 1 January 2021, a new domestic data privacy law came into effect: the UK-GDPR which, alongside the Data Protection Act (DPA) of 2018, governs data processing in the United Kingdom

ONECS 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 ONECS use to operate in accordance with these principles.

2 Training Activities

2.1 : Activity 1: Online training module

ONECS would like you to read the training material of this module and complete the relevant quiz at the end. A pass score of 90% is needed in order to be awarded a certificate.

2.2 : Activity 2: GDPR Compliance Statement

ONECS's **GDPR Compliance Statement** sets out ONECS's commitment to data privacy and can be used to answer questions from clients about ONECS's approach to GDPR. *Read and familiarise yourself with ONECS's **GDPR Compliance Statement** which can be found as part of the online training module*

2.3 : Activity 3: Data Privacy and Data Retention Policy

ONECS'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.

ONECS 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.

ONECS'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 ONECS. 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 ONECS'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. ONECS 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.

ONECS'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 ONECS'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 respond 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.

ONECS'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.

Review

This policy statement will be reviewed annually as part of our commitment to upholding professional standards. It may be altered from time to time in the light of legislative changes, operational procedures or other prevailing circumstances.