



Operative Data Protection Toolbox Talk

For all GDPR Subjects

Introduction

This training is mandatory for all operatives as they will have access to service user personal data in the course of carrying out works for the Company. This training should be issued prior to the operative carrying out any works for the Company.

Objectives

1. What is data protection?
2. What personal data does the Company process?
3. What data protection obligations does the Company have?
4. What individual obligations does the operative have in relation to data protection?
5. What procedures does the Company have to ensure data protection compliance?
6. What are the consequences of non-compliance?

What is data protection?

On 25th May 2018 data protection law in the UK was updated by the Data Protection Act 2018. This Act requires that all organisations which process personal data must comply with the data protection principles.

Personal data is any data which relates to an individual.

Processing means collecting, using and storing the personal data.

What personal data does the Company process and why?

1. Employee and contractor personal data
 - Name and contact information so that work arrangements can be made
 - Bank account details so payment can be made
 - National insurance & UTR numbers so tax can be properly processed
 - Health information – in the event of an emergency and for health and safety compliance (e.g. accident reports)
 - Training and certification information to demonstrate professional competence

2. Client personal data

- Name and contact information so that we can deal with enquiries and make arrangements to carry out the work
- Some financial information for invoicing and payment purposes

What data protection obligations does the Company have?

The Company must comply with the data protection principles. The key ones are:

1. To process personal data lawfully
2. To only use the personal data for the purpose it was collected
3. To keep the data secure and confidential
4. To destroy the data securely once it is no longer needed
5. To ensure that all individuals involved in processing data are appropriately informed and trained

What individual obligations does the operative have in relation to data protection?

Any individual who has access to personal data when performing work for the Company must:

1. Comply with the instructions of management
2. Enter into any reasonable confidentiality agreement as requested by the Company
3. Take care of the data – ensure passwords are used and kept confidential, vehicles are locked etc.
4. Keep the information confidential – do not discuss a client or employee personal information other than in the course of performing the work
5. Report any data protection breaches to management

What procedures does the Company have to ensure data protection compliance?

The Company has implemented rules and procedures to keep data safe and secure. These are set out in detail in the Data Protection Policy and Information Security Policy but the key ones are:

1. All contracts of employment will include a confidentiality clause
2. Electronic data will be stored on password protected devices and systems only
3. Hard copy data will be kept in a locked cabinet or office except when it is issued to employees for off premises work
4. Employees must keep data secure and confidential when it is in their possession by keeping vehicles locked and documents hidden
5. Employees must return the data as soon as practicable once they no longer need it

What are the consequences of non-compliance?

Data protection is very important as it relates to the privacy of individuals, which is a human right. Therefore the consequences of non-compliance can be severe and include:

- The information Commissioner's Office issuing a fine of up to 20 million Euros
- Clients cancelling our contracts for non-compliance
- Damage to the reputation of the Company
- Employee or contractor contracts being terminated for breach of confidentiality

Any questions?

Quick check questions for operatives:

Question: Name a type of data we hold about clients

Answer: Contact information / financial information

Question: What must the Company do once it no longer needs personal data?

Answer: Securely destroy it

Question: How can operatives help the Company comply?

Answers: Following procedures / keeping offices, cabinets and vehicles locked / not discussing employee or client information with other people / reporting breaches

Question: What is the maximum fine for non compliance?

Answers: 20 million Euros

| | | |
|--|--|--|
| | | |
|--|--|--|