



GDPR MANAGEMENT TRAINING

An Acumenology Business Guide
Acumenology.co.uk | All rights reserved

Published 2020

Welcome to your training on an organisations obligations and management responsibilities under the GDPR

Organisations or data controllers, are responsible and accountable for compliance under the GDPR for all the processing that occurs with the internal and external data they collect.

This course provides business owners and senior management with an understanding on key areas of responsibility that will need to be addressed.

[BACK](#)

DISCLAIMER The information contained herein was prepared by Raj Tandon and the information presented was correct at the time of publication in 2018. You should not rely on the information presented as a basis for making any business, legal or other decisions.

[NEXT](#)

The Course covers



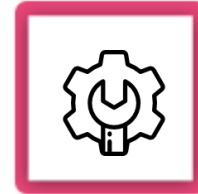
Module 1
Controller
obligations



Module 3
Lawful basis
of processing



Module 5
Subject access
requests



Module 7
Enforcement
& penalties



Module 2
Accountability



Module 4
Data
security



Module 6
Data
breaches

By the end of the course, management will be able to:

- ⚡ Understand their responsibilities under the GDPR
- ⚡ Have the knowledge to manage and implement their obligations
- ⚡ Understand the appropriate technical and organisational measures to manage personal data
- ⚡ Recognise the importance of putting in place protocols to manage Subject Access Requests and Data Breaches
- ⚡ Be aware of the consequences of failure to comply

BACK

NEXT

Module 1





Controller





Obligations

[BACK](#)

[NEXT](#)

Module 1 Covers

	Who is a Controller
	Controller obligations
	Data protection 'by design and default'
	Record of processing activity

	Appointment of processors
	Data processor agreement
	Processor obligations
	Transfer of data outside EU

BACK

NEXT

Nearly all organisations are Controllers

The Controller may be an organisation or individual that determines the purposes and means of processing personal data.

Since a company is a separate legal entity, it (the company) is normally the data controller, rather than an individual who is a part of the company.

[BACK](#)[NEXT](#)

An overview of Controller obligations



Ensure that the organisation is registered with the ICO as a data controller



Ensure data protection 'by design' & 'by default' is adhered to



Maintain a record of processing activity



Appoint processors in compliance with the legislation



Consider the legal implications of transferring data outside of the EU



Demonstrate accountability with the legislation (module 2)



Ensure a Lawful basis for processing (module 3)



Data Security (module 4)



Provide individuals access to personal information as part of SAR – Subject Access Request (module 5)



Report data breaches to the supervisory authority and individuals (module 6)

BACK

NEXT

New projects and processes must be designed to ensure data protection principles are adhered to

Organisations must ensure that when planning any new project, businesses processes are developed to ensure privacy and data protection principles are addressed and integrated into their data processing activities and that only the minimum amount of personal data is processed.

Data protection by design

Requires you to place appropriate technical and organisational measures and integrate safeguards into your processing to implement the data protection principles and protect the individual rights.

Data protection by default

Requires that you only process the data that is necessary to achieve your specific purpose.

More info - [Data protection by design and default - ICO](#)

Example

An authority responsible for courts and tribunals are building new IT systems for storing or accessing personal data. Prior to any live use, the authority is required to review their privacy and data protection compliance and perceived risks from the start of the project, rather than adding on such considerations at the end. This process could involve undertaking a Data Protection Impact Assessment (DPIA).

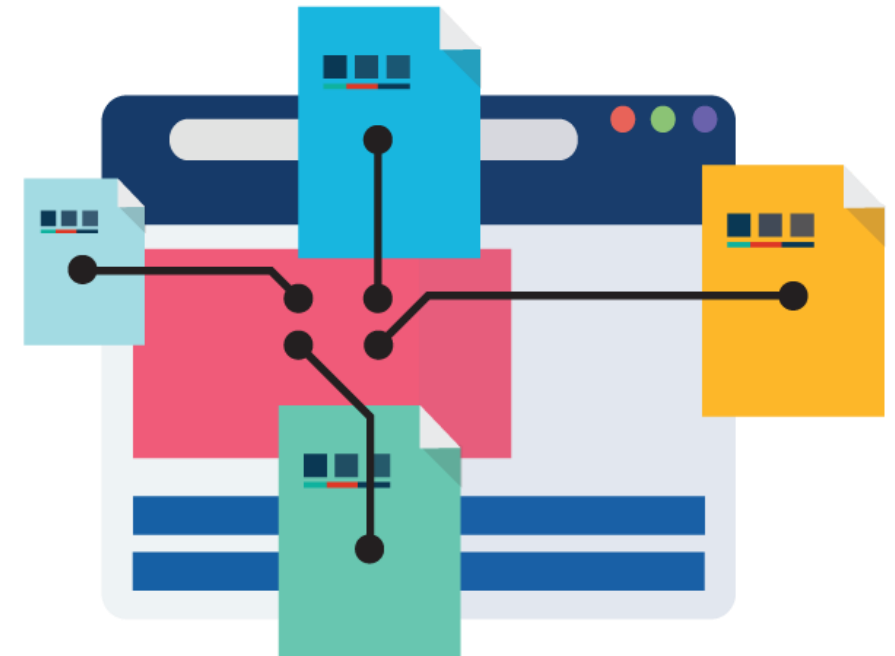
[BACK](#)[NEXT](#)

Controllers must keep a record of processing activities

The regulation requires organisations to keep records of their processing activities and, that the information be available on request by the supervisory authority.

Documenting your processing activities is important not only because it is a legal requirement, but also because it supports good data governance and helps demonstrate your compliance with certain aspects of the GDPR. The records must be kept up to date and reflect current data processing activities.

More Info - [Documentation of processing activities – ICO](#)
[Who needs to document their processing activities - ICO](#)

[BACK](#)[NEXT](#)

Controllers should only appoint processors that are compliant with the GDPR

A processor is organisation or individual who process data on behalf of the Controller e.g. third party payroll provider.

Under the GDPR the controller needs to demonstrate that any processors used are also compliant with the GDPR.

This is done by a data processing agreement or contract and is a legal guarantee that the processor will abide by the regulations at all times, upholding the rights of the data subjects.

It also sets out the terms of the work to be carried out, and the obligations of both the controller and the processor.

More info - [Contracts and liabilities between controllers and processors – ICO guidance](#)

[BACK](#)[NEXT](#)

Controllers should ensure a there is a data processing agreement

The data processing agreement is a contract between the controller and processor that sets out the rights of the data subjects, the terms of the work to be carried out, and the obligations of both the controller and the processor.

It should state that the processor must:

- Only act on the controller's documented instructions
- Impose confidentiality obligations on all personnel who process the relevant data
- Ensure the security of the personal data it processes
- Abide by the rules regarding appointment of sub-processors
- Implement measures to assist the controller in complying with the rights of data subjects
- Assist the controller in obtaining approval from the supervisory authority where required
- At the controller's instruction, either return or destroy the personal data at the end of the relationship (except as required by law)
- Provide the controller with all information necessary to demonstrate compliance with the GDPR

To implement best practice if in doubt processor – controller contracts should be reviewed by a lawyer.

More info- [Contracts and liabilities between controllers and processors – ICO guidance](#)

[BACK](#)[NEXT](#)

Processors must not deviate from the controllers instructions

If a processor deviates from the controllers instructions and processes data outside of the instructions then they are regarded by the GDPR as the Data Controller for that set of data and, assume controller obligations over it.

A processor must report any instructions to the controller if they breach the processors local legislation.

The processor also needs to comply with requirements for:



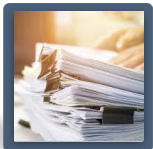
Complying with the principles



Security



Data Protection Officer appointments



Record keeping



Breach reporting



Restrictions on cross border transfers

[BACK](#)[NEXT](#)

Restrictions apply to transfer of personal data outside the EU

The controller should be aware that the GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

The GDPR states that personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in [Chapter V](#) of the GDPR.

More info - [International transfers - ICO](#)

[BACK](#)[NEXT](#)

Module 2

Accountability

[BACK](#)

[NEXT](#)

Module 2 Covers



Understanding accountability



Responsibilities under
accountability

BACK

NEXT

Accountability is key principle and compliance with the GDPR must be demonstrated

Accountability is arguably one of the most important principles of the GDPR. Not only does the GDPR make the organisation responsible for complying with the regulations, it also puts the responsibility to demonstrate it is complying. Evidence of compliance needs to be made available to the ICO if requested.

It encourages organisations to develop a culture of data privacy across all levels – from senior management to the most junior.

This includes ensuring adequate training is received and ensuring policies and procedures are understood and followed.

More info - [Accountability & Governance - ICO](#)

[BACK](#)[NEXT](#)

Key responsibilities


Responsibilities under the Accountability principle include ensuring:

- ⚡ Adherence to the GDPR principles
- ⚡ Organisations have in place appropriate technical and organisational measures – (Module 4 Data Security)
- ⚡ Data protection, privacy policy and related policies comply
- ⚡ Staff have received adequate training to ensure they understand data protection and can implement it in their day-to-day work
- ⚡ Contracts are in place with processors
- ⚡ Record of processing activities is accurate and kept up-to-date



BACK

NEXT

A group of people are seated around a white conference table in a bright, modern meeting room. They are all looking towards a large screen on the wall. The screen displays the title 'Module 3 Lawful basis for processing' in a bold, purple font. On the table, there are several green sticky notes, a yellow cup, a magnifying glass, and some pens. Two potted plants are also on the table. The room has white walls and a large window in the background.





Module 3





Lawful basis for processing

[BACK](#)

[NEXT](#)

Module 3 Covers

	Understanding lawful basis of processing
	Lawful bases of processing
	Consent
	Contract

	Legal obligation
	Vital interest
	Public Task
	Legitimate interest

BACK

NEXT

An organisation must establish a Lawful basis for processing personal data

- The first principle requires that you process all personal data lawfully, fairly and in a transparent manner. Thus, a key responsibility for an organisation is to establish a legal basis in order to process personal data and demonstrate that a lawful basis applies.
- If no lawful basis applies, your processing will be unlawful and in breach of the first principle.
- There are six lawful basis for processing – which basis is most appropriate will depend on the purpose and relationship with the individual.
- The lawful basis must be determined before you begin processing, and it should be documented.
- The privacy notice should include your lawful basis for processing as well as the purposes of the processing.

More info - [Lawful basis for processing - ICO](#)

BACK

NEXT

At least one lawful basis must apply when personal data is processed



Consent

The individual has given clear consent to process their personal data for a specific purpose.



Vital Interest

The processing is necessary to protect someone's life.



Contract

The processing is necessary for a contract with the individual.



Public Task

The processing is necessary to perform a task in the public interest or for official functions.



Legal Obligation

The processing is necessary to comply with the law.



Legitimate Interest

The processing is necessary for your legitimate interests or the legitimate interests of a third party.

BACK

NEXT

The individual has given clear consent for you to process their personal data for a specific purpose

The GDPR sets a high standard for consent, and it is the only basis allowed for obtaining and processing personal information for marketing purposes or, for processing sensitive personal data. Consent may not be necessary or be the most appropriate basis, and as it can be difficult to get, you should explore alternative options first.

The following conditions apply for consent

- Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.
- Consent should be obvious and require a positive action to opt in.
- Consent requests must be prominent, separate from other terms and conditions, concise and easy to understand, and user-friendly.
- Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.
- Keep records to evidence consent – who consented, when, how, and what they were told.
- Make it easy for people to withdraw consent at any time they choose.

You should review existing consent and your consent mechanisms to check they meet the GDPR standard. If they do not you need to obtain fresh consent.

More info – [Consent - ICO](#)

[BACK](#)[NEXT](#)

The processing is necessary for a contract you have with the individual or, because they have asked you to take specific steps before entering into a contract.

You have a lawful basis for processing if:

You have a contract with the individual and you need to process their personal data to comply with your obligations under the contract.

Example

When a data subject makes an online purchase, a controller processes the address of the individual in order to deliver the goods. This is necessary in order to perform the contract.

You do not yet have a contract with the individual but, they have asked you to do something as a first step (e.g. provide a quote) and you need to process their personal data to do what they ask.

Example

An individual shopping around for car insurance requests a quotation. The insurer needs to process certain data in order to prepare the quotation, such as the make and age of the car.

It does not apply if you need to process one person's details but the contract is with someone else.

More info – [Contract - ICO](#)

BACK

NEXT

The processing is necessary for you to comply with the law

You can rely on this lawful basis if you are obliged to process the personal data in order to comply with the law or statutory obligation but not including contractual obligations.

Example

An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC. The employer can point to the HMRC website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation.

More info – [Legal obligation - ICO](#)

BACK

NEXT

The processing is necessary to protect someone's life

This lawful basis is intended to cover only interests that are essential for someone's life. So, it is very limited in its scope, and generally only applies to matters of life and death. It is particularly relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

Example

An individual is admitted to the A & E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests.

More info – [Vital interests - ICO](#)

BACK

NEXT

The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

This lawful basis applies mainly to public organisations and can apply if you are either:

- ✿ Carrying out a specific task in the public interest which is laid down by law or
- ✿ Exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

Example

Private water companies are likely to be able to rely on the public task basis even if they do not fall within the definition of a public authority in the Data Protection Act 2018. This is because they are considered to be carrying out functions of public administration and they exercise special legal powers to carry out utility services in the public interest.

More info – [Public task - ICO](#)

[BACK](#)[NEXT](#)

It is the most flexible lawful basis for processing

Legitimate interests is most likely appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. However, you cannot assume it will always be the most appropriate.

There are three elements to the legitimate interests basis. It helps to think of this as a three-part test.



Purpose test: identify a legitimate interest



Necessity test: is the processing necessary for that purpose?



Balance test: do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits.

More info – [Legitimate interests - ICO](#)

BACK

NEXT

Module 4

Data Security

[BACK](#)

[NEXT](#)

Module 4 Covers



Understanding data security



Improving data security



Reducing human error



Improving internal systems
and processes



Strengthening IT security

BACK

NEXT

Controllers must have appropriate security measures to process and manage data securely

A key obligation under the GDPR is for controllers and processors to take 'appropriate technical and organisational measures to ensure appropriate security of the personal data they hold. This includes, protection against unauthorised or unlawful processing and, against accidental loss, destruction or damage.

Since the level of security should be 'appropriate' to the risks presented by the processing, you need to assess your information risk before deciding what measures are considered appropriate.

You should review the personal data you hold, the way you use it, assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised.

More info – [Security - ICO](#)

BACK

NEXT



Improving data security can be relatively straightforward

Since the majority of data breaches are as a result of human error, poor internal systems and processes or lack of adequate IT security, improving data security is a relatively simple and quick way to improve the security of the personal data you hold and comply with your obligation.

This can be achieved by:



Reducing
human error



Improving internal
systems and processes



Strengthening
IT security

More info – [GDPR security outcomes – National cyber security centre](#)

BACK

NEXT

Human error is the most common reason for data incidents

The majority of data incidents reported to the ICO in Q4 2017 were as a result of human error with the most common ones being:



Data posted or faxed to incorrect recipient



Loss or theft of paperwork



Data sent by email to incorrect recipient

- ✦ Train staff to take time and be more vigilant when carrying out activities involving personal data.
- ✦ Ensure all paperwork is always kept secured, especially overnight and access is restricted.
- ✦ Ensure a clear desk policy is maintained.

[BACK](#)[NEXT](#)

Strengthen internal systems and processes concerning personal data

Protect access to data

- ⚡ Ensure access to all personal data stored such as in spreadsheets, is encrypted and/or password protected
- ⚡ Removable media is encrypted
- ⚡ Access to computers is restricted, protected and screens locked

Consider carefully allowing staff to use their own devices for work

It may be easier to allow staff to login from their phone, or laptop from home. As a data controller you need to own the devices that the data is shared with and control it. Since you don't own the users' personal device you do not have right to check or remove at data stored on it. If you are to allow personal devices to be used, you will need to instigate a Bring Your Own Device (BYOD) Policy.

Working away from the office

Be aware of additional risks of working in public spaces or at home.

- Consider who may be able to look at your screen.
- Take care of looking after your devices

[BACK](#)[NEXT](#)

Strengthening IT security can reduce data incidents considerably

Do not use shared logins

Do not use shared logins (such as "accounts" or "info"). It means that multiple users know the password and what happens. When someone leaves - do you change the password? Keep logins unique to each team member and never share accounts.

Improve password protocols

**Never
make passwords
visible**

Shared accounts tend to be used by many people in an office and you can see post-it notes stuck on a PC with the password written down for the team. Don't ever do this.

**Enforce
strong
passwords**

Use combinations of upper- and lower-case letters, numbers and symbols.

**Change
Passwords
regularly**

Passwords should be changed every 90 days. You have to protect personal data so make it a habit.

**Change
passwords after
sharing**

Change your password after you have given it to a third party for access such as an outsourced IT provider .

BACK

NEXT

Strengthening IT security can considerably reduce data incidents

Identify suspect emails

Ensure staff are trained to ensure they never open an unexpected attachment, click a link that comes from an unknown sender and, how to identify spam email.

Improve password protocols

Phishing

Emails asking you to download a file or click a link. Do not click any links, delete and report.

Vishing

Voice call claiming to be from a trusted company or internal source. Treat with suspicion till verified.

Smishing

An SMS luring you into an action. Be wary of unsolicited messages, Do not respond and delete.

Get protected

Ensure you have adequate protection to guard against viruses, spyware and malware.

[BACK](#)[NEXT](#)

A group of people are seated around a white conference table in a bright, modern meeting room. They are all looking towards a large screen at the front of the room. The screen displays the title 'Module 5 Subject Access Request' in a bold, purple font. On the table, there are several green sticky notes, a yellow cup, and some pens. Two potted plants are also visible on the table. The overall atmosphere is professional and collaborative.

Module 5

Subject Access Request

[BACK](#)

[NEXT](#)

Module 5 Covers



Recognising a Subject
Access Request



Dealing with a Subject
Access Request



Information to be provided

BACK

NEXT

Controllers have a legal obligation to deal with a Subject Access Request

There is a legal obligation to allow data subjects to obtain a copy of their personal data and other supplementary information. This is known as a Subject Access Request or SAR.

Organisations need to develop systems and processes to manage these SAR's.

The Subject Access Request

- Can be made verbally, in writing or even by social media so ensure employees are trained to recognise a request.
- Consider providing a form that individuals can complete and submit electronically. This can be made available on your website.



More info – [Rights of access - ICO](#)

BACK

NEXT

Set up a system to deal with a Subject Access Request

Controllers should:

- ✿ Request proof of identity
- ✿ Record the request
- ✿ Respond within a month. In special circumstances this can be extended to three months
- ✿ Provide the information **Free of Charge**
 - A reasonable fee can be charged where the request is repetitive, unfounded or unduly excessive
- ✿ Rectify or erase inaccurate or incomplete data if requested by the data subject



More info – [Subject access code of practice - ICO](#)

BACK

NEXT

Personal data and supplementary information to be provided

Controllers are obliged to provide

- Copy of the personal data held
- Confirmation of where and how the personal data is being processed
- Information about the purpose of processing
- Information about the categories being processed
- Information about the recipients with whom the data has been or is being shared
- Information about the period of time the data will be stored and the criteria for determining this
- Details of their rights in terms of rectification, erasure, restriction of processing and to make no objections
- Details of their right to complain to the supervisory authority the ICO
- The source of the data
- Information about the logic of automated processing

If an organisation is likely to receive a significant number of SAR's you may wish to consider using appropriate software to make the task efficient and manageable.

[BACK](#)[NEXT](#)

Module 6

Data Breaches

[BACK](#)

[NEXT](#)

Module 6 Covers



Understanding a data breach



Breach response planning



What breaches should be notified?



Breach reporting obligations



Informing Individuals



Failure to notify

BACK

NEXT

A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data

What is a data breach?

A personal data breach is an incident that as a result of accidental or deliberate causes leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Example

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data.

[BACK](#)[NEXT](#)

Develop a suitable breach response plan

An organisation should understand the different aspects of data breach management to ensure they have the capabilities to respond to personal data breaches.

- What breaches do I notify?
- Breach reporting obligations. How do I notify a breach?
- What information must a breach notification contain?
- When do we tell individuals about a breach?
- What do we tell individuals about a breach?
- What are the consequences of a data breach?
- What are the consequences of failure to notify?

[BACK](#)[NEXT](#)

Obligated to report data security breaches to the ICO

Controllers are obliged to report data breaches that are likely to result in risk to peoples rights and freedoms. If this risk is unlikely, you do not have to report it. However, should you choose not to report, you need to be able to justify and record your decision.

Example

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

[BACK](#)

If a processor you use suffers a breach of the personal data they are processing on your behalf, they need to inform you as soon as they become aware, allowing you to meet your breach obligations under the GDPR.

Example

Your organisation (the controller) contracts an IT services firm (the processor) to archive and store customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the ICO.

[NEXT](#)

ICO must be notified within 72 hrs. with relevant information

When	Example	How
<p>A breach must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer you must give reasons for the delay.</p>	<p>You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.</p> <p>You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.</p>	<p>When reporting a breach, you must provide:</p> <ul style="list-style-type: none">■ A description of the nature of the personal data breach including, where possible:<ul style="list-style-type: none">• The categories and approximate number of individuals concerned• The categories and approximate number of personal data records concerned■ The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained■ A description of the likely consequences of the personal data breach■ A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

[BACK](#)[NEXT](#)

Individuals should be informed without undue delay

When	Example	How
<p>Individuals should be informed without undue delay if a breach is likely to result in a high risk to their rights and freedoms.</p> <p>The threshold for informing individuals is higher than for notifying the ICO.</p> <p>If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.</p>	<p>A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.</p> <p>A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.</p>	<p>You need to describe, the nature of the personal data breach and:</p> <ul style="list-style-type: none">■ The name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained.■ A description of the likely consequences of the personal data breach.■ A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

[BACK](#)[NEXT](#)

Failing to notify a breach when required to do so can result in:

- ✦ Range of corrective powers and sanctions from ICO
- ✦ Administrative fines

2%
Annual Global
Turnover

Tier 1 - For infringements of the organisation's obligations, including data security breaches. Up to €10 million, or 2% annual global turnover – whichever is higher.

So, it is important to make sure you have a robust breach-reporting process in place to ensure you can detect and notify a breach, on time; and to provide the necessary details.

[BACK](#)[NEXT](#)

Module 7

Enforcement and Penalties

[BACK](#)

[NEXT](#)

Module 7 Covers



Consequences of failure to comply



ICO penalties



Failure to notify

BACK

NEXT

Failure to comply can lead to sanctions, significant fines, compensation and reputational damage

It is important management are aware of the considerable risk faced by failure to comply through either administrative failures or personal data breaches.

The consequences could be:



Range of corrective powers, sanctions and fines from the ICO

Whilst a range of sanctions and significant fines are available for the most serious and persistent failures, it should be noted that not all infringements will lead to the serious fines. The ICO's commitment especially for small businesses is to guide advise and educate organisations about how to comply with the law. Issuing fines is a last resort.



Liability of material and non-material damages from individuals

Individuals have the right to compensation of any material and/or non-material damages resulting from an infringement of the GDPR. This could potentially be very damaging as it may open the door for claims from 'no win no fee lawyers'.



Reputational damage and lack of trust

[BACK](#)[NEXT](#)

Range of corrective powers, sanctions and fines from ICO

Information Notice

Requiring organisations to provide the ICO with specified information within a time period.

Compulsory Undertaking

Committing an organisation to a course of action in order to improve its compliance.

Enforcement Notice

Requiring organisations to take specified steps in order to ensure they comply with the law.

Audits

Assessing whether organisations processing in compliance with legislation

Administrative fines

2%
Annual Global
Turnover

Tier 1 - For infringements of the organisation's obligations, including data security breaches. Up to €10 million, or 2% annual global turnover – whichever is higher.

4%
Annual Global
Turnover

Tier 2 – For infringements of an individual's privacy rights. Up to €20 million, or 4% annual global turnover – whichever is higher

[BACK](#)[NEXT](#)

Next Steps

[BACK](#)

[NEXT](#)

The training has provided business owners and senior management:

- ⚡ An overview of the main responsibilities an organisation has as a controller
- ⚡ An understanding on the obligations under the Accountability principle
- ⚡ The need to establish a Lawful basis for processing
- ⚡ The requirements and processes to manage Subject Access Requests and Data Breaches
- ⚡ An understanding of the enforcement action and penalties for failure to comply

Your next steps are to:

- ⚡ Appreciate the importance of your role in managing compliance
- ⚡ Ensure your organisation has in place appropriate technical and organisational measures with a focus on data security
- ⚡ Ensure all policies are up to date and all staff have received adequate training
- ⚡ Maintain on-going compliance



END