Cyber Security Tool Kit

Level 1•Guidelines & Legislation

Securing your business.

0330 174 9996
info@start-digital.co.uk
start-digital.co.uk

Start Digital

Ver. 2.1

What is This Document?

What is this document?

This **Level 1 Cyber Security Tool Kit** is a step-by-step guide to help you implement the measures and processes covered in the **Level 1 Health Check**.

Not all fields or groups of boxes will need to be filled in. We expect you to only fill in the ones you plan on implementing based on your health check audit results. You can always go back later to complete any additional modules if necessary.

The **Level 1 Cyber Security Tool Kit** is a ***living document***, which means that you will be continually editing and updating the document. Cyber security is an on-going process, and sitting still is not a position you want to be caught in. Most of this document's tasks cannot be completed in a single sitting, or a short period of time. This means you will be coming back regularly to make updates and changes.

Policy Implementation:

Certain topics within the **Level 1 Cyber Security Tool Kit** may be covered by existing policies you have implemented within your business. You may find that you can improve your existing policies with the help of the **Level 1 Health Check** and this **Level 1 Tool Kit**. If your existing policies are working as they should though, rather than repeating yourself, you can add supporting documents to the relevant policies and redirect towards the documents with the necessary information.

What you will achieve by completing this document:

The goal of this document is to support your on-going cyber security journey, no matter how small each step is. Any step you take in the right direction is an important improvement to your business's cyber security, as well as establishing your business's digital culture.

Establishing a digital culture:

Advancements and the reliance on digital technology coupled with classic business models have accelerated business disruption. In an increasingly global marketplace, the pandemic has further accelerated this trend, making the digital transformation critical for a business's success. However, it takes more than just technology and policies; the business leaders must also look at the human side of their organisations.

The culture within the business around the way your employees interact with technology is a significant factor in staying secure, and being successful. Developing a strong digital culture from the top down is an extremely important element to ensuring the policies you develop become second nature to all employees. Without the right culture of behaviour, the policies you implement have limited impact.

This is a document you will regularly refer back to before and after you've implemented your business's new cyber security policies and procedures.

Completing Task Sheets

Completing Task Sheets:

This document's task sheets are laid out in a very simple, user-friendly table format. A task sheet has 2 primary elements: the **topic table**, and the **question** and/or **task box**. Some task boxes may include a **tick box** to indicate you have completed that specific task or full topic.

Topic Table:

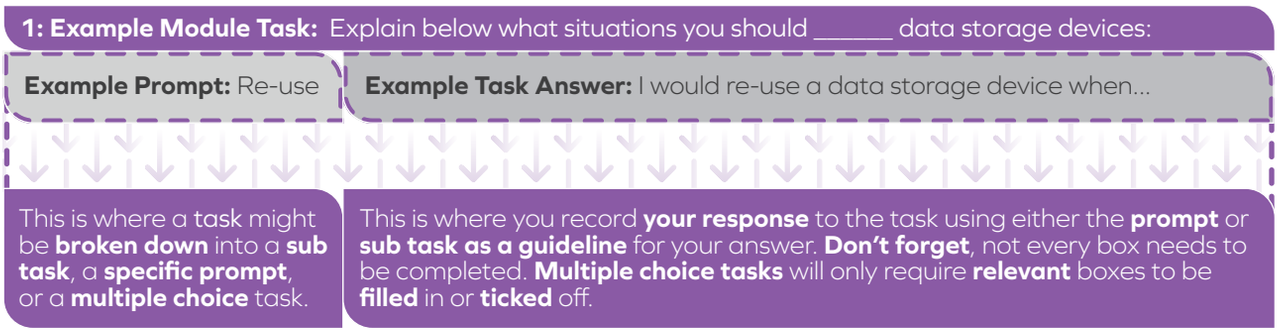
This is a table at the start of each module with each topic categorised. Once you have completed a full task, you can tick it off to keep track of the tasks you have carried out.

Answer Table:

Answer tables are set out in two different formats: **question boxes** where you are asked specific questions that require specific answers; and **task boxes** where the goal is for you to carry out a specified task, and then mark it as complete when you have finished. Some tasks will be multiple choice, where you choose one task or another.

Question Box:

Task Box:



Guidelines & Legislation

Policies and Procedure: Creating Policies for your Business.

The General Data Protection Regulation (GDPR) and the Information Commissioner's Office (ICO) are two of the most important pieces of legislation in the United Kingdom when it comes to how businesses collect and store the personal data of their customers or service users. They lay out rules that any company or individual who handles personal data must follow, and explains the serious consequences they could face if they don't.

The GDPR was introduced in May 2018, and regulates how businesses manage customer data. It also gives people more control over how their data is used. The ICO enforces GDPR compliance by handling complaints about businesses' policies and procedures, assessing fines against those who don't comply with GDPR rules, and investigating breaches of security to ensure that personal information isn't leaked or stolen, as well as what to do if it is.

Since the UK has left the EU, the EU-GDPR no longer applies to the UK, however, the UK's Data Protection Act 2018, which implements the EU General Data Protection Regulation (GDPR), has already been enacted into UK law. With effect from 1 January 2021, the Data Protection Act (Amendment) Regulations will amend the DPA 2018 to merge its requirements with the EU-GDPR, forming a new UK-specific data protection regime known as "UK-GDPR".

Businesses in the UK must prepare their GDPR documentation to reflect the requirements of the UK GDPR. Article 30 requires privacy notices and Data Protection Impact Assessments (DPIAs) to reflect the scope and wording of the UK GDPR. Data subject access requests should also be prepared for this reason.

How UK and EU GDPR Differ:

Although EU and UK data protection laws are similar, there are some notable differences for businesses to consider. To ensure full compliance with the law, GDPR training courses are a good consideration. The rest of this document will primarily cover UK-GDPR, however below we will cover the key differences between UK GDPR and EU GDPR:

- The use of personal data is monitored differently in the UK and EU. The Information Commissioner's Office (ICO) is the sole body responsible for overseeing the regulation in the UK. EU GDPR is governed by the European Data Protection Board (EDPB), member state privacy authorities, and ultimately, the European Commission.
- Data collection — In the EU and EEA, individuals must be 16 years or older to give consent for the use of their personal data (with some exceptions). In the UK, that age is 13.
- The area in which a company operates determines how it must comply with GDPR. Companies that operate wholly within the UK need to comply with both the GDPR and the Data Protection Act. If a company operates solely within the EU, the GDPR applies. If a company operates in both the UK and EU, it must comply with each jurisdictions' versions of GDPR.

UK businesses providing goods or services to, or monitoring the behaviour of, EU residents should be aware of the effects of the EU General Data Protection Regulation (GDPR) and ensure that any data processing is in compliance with the regulation. If you are handling any personal data—even if you're just a small business—you need to be aware of these rules and regulations and make sure you're following them correctly.

Guidelines & Legislation

Number	Module Topic	✓
1	General Data Protection Act (UK/EU-GDPR)	
2	GDPR: The Size of a Business and Data Collection	
3	GDPR: Becoming Compliant	
4	GDPR: The Lawful Basis for Collecting Data	
5	GDPR: Third-Party Information Processors	
6	GDPR: Individual Rights	
7	Information Commissioner's Office (ICO) Registration	

Module Notes:

You can use this box to add any notes you feel are necessary to help you work through this module.

Notes:

Guidelines & Legislation

1. Guidelines and Legislation: General Data Protection act (EU/UK-GDPR).

The General Data Protection Regulation (GDPR) is a set of laws that govern how businesses can collect, store, and use the personal information of European Union (EU) citizens. The GDPR was created in 2016, and it replaces the Data Protection Directive 95/46/EC.

GDPR's goal is to protect EU privacy rights of citizens by regulating how businesses manage personal data. It applies to any business that does business in the EU, or has an office there.

Under GDPR, businesses must be transparent about their data collection practices, and must inform individuals what they plan to do with their data before collecting it. Businesses also need to give individuals access to their own data so they can correct errors or remove information they no longer want shared with others.

Businesses that violate these rules could face fines up to €20 million, or 4% of annual global turnover, whichever is higher, and could also be banned from doing business within the EU.

There are many different sub-sections within GDPR, as it is a major part of cyber security, not all of it will be used straight away and it might not even need to be used depending on the business.

2. GDPR: The Size of a Business and Data Collection.

To follow GDPR to the best of your business's ability, you first need to take into account the questions below. After completing the table, you'll be in a better position to understand what steps you need to take to be on your way to becoming GDPR compliant.

Collecting and Processing Data: The Scope of Your Business's Data Collection.	
How many people's data do you approximately process? (Work in 10s, 100s, 1000s, etc)	
Does your business's goals require you to process personal data?	
Yes	**No**
Approximately, how many employees would require access to personal data?	
Does another business or organisation process the personal data on your business's behalf?	
Yes	**No**
Does your business's goals require you to process personal data?	
Yes	**No**
If YES, be sure to complete the external processors section	
If NO, you can skip the external processors section.	
Tick the box once you have completed this topic.	

3. Guidelines and Legislation: Becoming UK GDPR and EU GDPR Compliant.

The General Data Protection Regulation (GDPR) is a regulation in European Union law on data protection and privacy for all individuals within the EU. The GDPR replaces the Data Protection Directive 95/46/EC, which was adopted in 1995. The GDPR applies to all businesses that process or handle the personal data of EU citizens, regardless of where the business itself is located.

The objective of the GDPR is to protect all EU citizens' personal data, whether it's stored electronically, or kept on paper files. Personal data includes any information related to an identified or identifiable natural person (data subject).

The GDPR requires businesses to take the appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with processing personal data.

Businesses must inform their employees about how they process personal data, and how it impacts the employee's rights under GDPR. This can be done through training courses conducted by IT experts who have expertise in this area, as well as through written policies available for every employee to read.

Businesses should make sure that their employees have access only to the information required for carrying out their job roles. This means without being able to access any other information from other employees' systems without permission from management.

The following questions will help you become GDPR-compliant. Answer each question based on the information you provided in the table in the previous section. The amount of security you need to implement will depend on your business's size, the amount of data you process, and your industry.

Notes to help you complete the main table:

Collecting and Processing Data: Personal data - Any data that can identify an individual.

- Name
- Address
- ID card/Passport number
- Income
- Cultural profile
- Internet protocol (IP) address
- Any medical data which can be used to uniquely identify a person

Collecting and Processing Data: Special Data.

- Racial or ethnic origin
- Sexual orientation
- Political opinion
- Religious or philosophical beliefs
- Trade-union membership
- Genetic, biometric or health data except in specific cases (e.g. when you've been given explicit consent or when processing is needed for reasons of substantial public interest, on the basis of EU or national law)
- Personal data related to criminal convictions and offences unless this is authorised by EU or national law

Guidelines & Legislation

Task: Risk Assessment. Tick off when complete.
Before you start anything regarding personal data, it's good practice to complete a risk assessment, or a data protection impact assessment (DPIA) - great way to show GDPR compliance, although not required.
Complete a DPIA by using the ICO online DPIA template. Tick the box when complete.
Task: Data Accuracy and Competition. Tick off each when complete.
Ensure data is complete.
Reasonably make sure the data you hold is accurate.
Remove data that is no longer in use.
Stop collecting data when it's no longer needed.
Update data and keep data up to date if data doesn't need to be from a specified time.
Task: Technical Measures. Tick off when complete.
Types of physical security you have in place, locks, alarms, CCTV, etc. **Install physical security where necessary, though not all measures may be applicable to your business.**
Security Guards
Mechanical /Electronic Locks
Alarms
CCTV
Other types of physical security you might have or require:
Complete the Access Control task within Data & Information module of this tool kit.
Complete the Access Control Policy task within Policies & Procedure module of this tool kit.
Task: Dispose of electronics you no longer used by using specialist software or hardware to:
Physically destroy the device using an electronics waste shredder.
Wipe the data contents of the device using specialist software to "zero" out the storage multiple times.
Task: Dispose of physical/paper documentation using:
A shredder to make the contents of the documents unrecoverable. A cross-cut shredder can do this.
Contract a reputable shredding service to collect and shred the documents for you.
Keeping mobile device secure by:
Having a locked screen, a suitably secure pass code, and not leaving mobile devices unattended.
Encrypting sensitive data.
Delete unnecessary data.
Remove unnecessary apps.

Guidelines & Legislation

Task: Cyber Security Focus. Tick off when complete.

Complete the modules of the toolkit listed in the table below:
We don't expect you to be able to cover everything, so focus on what you can reasonably implement.

- Password Security.
- Social Media Security.
- Email Security.
- Website Security.
- Hardware & Software.
- Policies & Procedure.

Task: Data Security. Tick off each when complete.

Use the Data & Information module to complete this task.

- **Complete the risk assessment (DPIA) part of this module.**
- **Complete the Encryption task within Data & Information module of this tool kit.**
- **Complete the Backups task within Data & Information module of this tool kit.**

Task: Pseudonymisation of Personal Data: (can still be used to re-identify if needed)

Pseudonymisation is the practice of processing personal data in such a way that the data cannot be attributed to an identified or identifiable person without additional information. Any additional information needed to re-identify the person must be kept separately from the personal data.

Task: Organisational Measures. These are the best way to show compliance. Tick off each when complete.

- **Complete the risk assessment (DPIA) part of this module.**
- **Complete policies relevant to your business's interests in the Policies & Procedure module.**
- **Check and keep policies and systems up to date.**

Task: Restoring access and availability. Tick off when complete.

- **Complete the Backups task within Data & Information module of this tool kit.**
- **Restore systems in a 'timely manner'.** (this may change per business, or the effect on individuals)

Task: Authorisation and Control of Data. Tick off each when complete.

- **Complete the risk assessment (DPIA) part of this module.**
- **Complete the Encryption task within Data & Information module of this tool kit.**

Task: Regular Testing. Tick off each when complete.

How do you plan to carry out regular tests? Choose only one.

- Internally.
- Externally.
- Both (internally and externally.)

Guidelines & Legislation

Task: Research vulnerability scanning tools suitable for your business. There are some examples in the table below.

Vulnerability Scanning Tools:

Service:	Cost:	Pros:	Cons:	✓
Acunetix	£			
beSECURE	£			
Burp Suite	£			
GFI Landguard	£			
Intruder	£			

Other:

Task: Research vulnerability audit services suitable for your business. There are some examples in the table below.

Vulnerability Scanning Tools:

Service:	Cost:	Pros:	Cons:	✓
CYFOR Secure	£			
Redscan	£			
Jisc	£			
Khipu Networks	£			
Razorthorn	£			
Evalian	£			

Other:

Task: Research penetration testing services suitable for your business. There are some examples in the table below.

Vulnerability Scanning Tools:

Service:	Cost:	Pros:	Cons:	✓
Redscan	£			
Intruder	£			
Netsparker	£			
Dhound	£			

Other:

Keep any testing and scanning results documented for evidence/planning. Implement any of the recommendations given. You will need valid reasoning and safeguards in place if you cannot.

Guidelines & Legislation

Task: Staff Training. Tick off each when complete.
Train Staff On:
Responsibilities of a data controller in GDPR.
Staff responsibilities in protecting personal data. Staff may be committing a criminal offence by knowingly accessing or disclosing information without the proper authorisation.
Procedures to identify callers.
Mock phishing emails, or similar training to help staff be able to identify social engineering attacks.
Access control - restrictions you place on staff's personal use of devices, etc.
Update data and keep data up to date if data doesn't need to be from a specified time.
When creating a product or service, ensure that the above practices are followed during every step.
Tick the box once you've implemented the processes from the table above.
Task: Documentation. Tick off each when complete.
Create documentation that helps to keep a record of the following: **Note:** It doesn't necessarily have to be a document, it could be your preferred method.
Name/details of organisation (contact details).
Purpose of processing explained in detail.
Description of the categories of individuals.
Description of categories of personal data.
The categories of the recipients of the data.
Existence of data transfer to third countries* or international organisations including documentation of the transfer mechanism safeguards in place. ***Note:** third countries are any countries outside of the United Kingdom and European Union.
Existence of data belonging to minors.
Retention period/schedule.
Description of technical and organisational security measures.

How The Size Of Your Business Affects Documentation:	
250 Employees or More:	The above is the minimum amount of data you need to record.
249 Employees or Fewer:	Your business only needs to document processing activity that: • Is not occasional • Could result in a risk to the rights and freedoms of individuals you are recording the data of. • Involve the processing of special categories of data or criminal conviction and offence data.

Guidelines & Legislation

Task: Documentation. Tick off each when complete.	
Other data that could prove useful to have a record of: **Note:** This is optional data, however it can help show compliance to ICO, so documentation is recommended.	
Lawful basis for the processing the data.	
Legitimate interest for the processing of the data.	
Individuals' rights.	
The existence of automated decision-making, including profiling.	
The source of the personal data.	
Records of an individual's consent to gather personal data.	
Controller-processor contracts.	
The location of where personal data is stored.	
Data protection Impact assessment reports (DPIAs).	
Records of personal breaches. **(This one is highly recommended)**	
information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018 includes:	
The condition for processing in the Data protection act.	
The lawful basis for the processing in the UK GDPR.	
Your retention and erasure policy document.	
Task: Keeping on top of GDPR.	
Regularly update your systems and process to keep up-to-date with GDPR, while what you implement now might work, as your business grows, and as time passes it may no longer be enough to be following GDPR.	
Tick off when you are following the process.	
Keeping on top of GDPR Notes:	
Tick the box once you have completed this topic.	

Guidelines & Legislation

3. GDPR: The Lawful Basis for collecting data.

This section will help guide you through GDPR compliance while interacting with individuals, and ensuring you are taking the right steps to be able to collect/process their data.

When collecting data from an individual are you doing it for one of these legal bases?	
Lawful Basis:	**Individuals' Rights:**
Consent (individual consented).	The right to withdraw consent.
Legal obligation (following a law/ruling).	The right to object
Contract.	Legal obligation, the right to portability, the right to object
Vital interest (a life could be dependent on this).	The right to portability, the right to object
Public task (mainly government related organisations)	The right to withdraw consent.
Legitimate interest (needs to be expected by the individual)	The right to portability

Task: Lawful Bases for Collecting Data on Individuals. Tick off each when complete.	
What lawful basis are you collecting personal data under? - Make sure it is right the first time as it is difficult to change. Note: Follow the guide above to be understand how to use these lawful bases.	
Consent (individual consented/Allows for individual to have more control).	
Legal obligation (following a law/ruling).	
Contract.	
Vital interest (a life could be dependent on this).	
Public task (mainly government related organisations)	
Legitimate interest (needs to be expected by the individual)	
Note: If not using other legal bases than consent, don't give the individual the impression that it is a choice.	
Task: Your business's method of gaining consent: Include details, and tick off each that applies.	
Name of your organisation.	
Name of third-party controllers.	
Why you want the data.	
What you intend to do with the data.	
Explanation that the individual can withdraw at any time with directions on how to do so.	
Rules to follow when requesting consent: Tick off if you have implemented or if completed.	
No default consent allowed.	
Consent must be separated from terms and conditions.	
Consent must always be under review	
Post consent requirements:	
Keep evidence/document the gained consent.	

Guidelines & Legislation

Task: Contracts. Tick off as you go.
To be Able To use as Lawful Bases: Only tick off one here.
You have a contract with an individual that requires the processing of personal data.
Before a contract, where you need to process data for the contract and have been asked by the individual to do it.
The Below is a Requirement:
The data must be necessary, if the task can be done without gathering data, you cannot use it.
Processes for Evidence of Contract Include:
Document your decision.
Be able to justify your reasoning.
Further Considerations:
The individual is under 18, do they have necessary competence to consent?
Task: Legal Obligation. Tick off as you go.
When you can use this lawful basis to process personal data:
To comply with common law.
To comply with statuary obligations.
The Below is a Requirement:
The data processing must be necessary, if the task can be done without gathering data, you cannot use it.
Processing of Evidence for Legal Obligation: Documentation must include at least one.
Identify any legal provisions.
Appropriate source of advice.
Guidance that clearly sets out your obligations.
Further Considerations:
Add your purpose and lawful basis to your privacy notice.
Task: Vital Interest. Tick off as you go.
When you can use this lawful basis to process personal data: All must be ticked.
Protect life.
Require there to be no other option (that is less intrusive).
They cannot legally consent.

Guidelines & Legislation

Task: Public Tasks. Unlikely to be applicable to businesses.

When you can use this lawful basis to process personal data:

Following public functions and powers set out in law.

Perform specific task in the public interest set out by law.

The Below is a Requirement:

Must have a clear basis in law.

The processing must be necessary. It's recommended to use the least intrusive way possible.

Processing of Evidence of Public Tasks Must Include:

You must specify one of the following:

- Relevant Task
- Relevant Function
- Relevant Power

Then the common law basis that allows the specified task, function or power.

Further Considerations:

include basic information about your purposes and lawful basis in your privacy notice.

Task: Legitimate Interest. Tick off as you go.

When you can use This Lawful Basis to Process Personal Data:

Use people's data in ways they would reasonably expect, and which have a minimal privacy impact.

The Below is a Requirement:

Identify a legitimate interest, it doesn't need to be your own.

Show that the processing is necessary to achieve it.

Balance it against the individual's interests, rights, and freedoms.

The processing must be necessary, use the least intrusive way possible.

Use the ICO's template for a **legitimate interest assessment** (LIA) and complete it.

Processing of Evidence for Legal Obligation: Documentation must include at least one.

Keep a copy of a completed legitimate interest assessment.

Further Considerations:

You must include details of your legitimate interests in your privacy information.

Note:

You should avoid using legitimate interests as reasoning if you are using an individual's personal data in ways people generally do not understand and would not reasonably expect, or if you think some people would object if you explained it to them.

Guidelines & Legislation

Task: Collecting Data. Tick off as you go.
Informing Users.
Inform users when collecting data at the time the data is collected.
Information to include when informing users you are collecting their data: (privacy information)
Name and contact detail of your organisation, and representative and DPO if you have one.
Purpose for processing their data.
Lawful basis reasoning/rights (right to withdraw, obligations due to law, etc).
What categories of personal data obtained.
Who will receive the personal data (third parties).
The details of transferring data across to third party countries (if any).
Your retention periods.
The rights of the individual in regard to the data.
Information in regard auto-mated decision making, including profiling.
When obtaining information on individuals from other sources you must: (including publicly accessible sources)
Provide the individuals with the privacy information within a reasonable period (28 days).
Unless the following exemptions apply: • The individual already has the information; or, • It would involve or require a disproportionate amount of effort to provide it (DPIA required). • Required not to by law.
When providing information to an individual, the information must be:
Concise.
Transparent.
Intelligible.
Easily accessible.
Clear and plain unambiguous language used.
Privacy information must be regularly reviewed and updated.
Any new uses of information should be brought to the individuals' attention before processing.
Tick this box once implemented.
Collecting Data Notes:

4. GDPR: Third-Party Information Processors.

Third-party data processors are businesses that offer services to other businesses, but do not retain any personal data themselves. This means that they are not responsible for EU and UK-GDPR compliance on their own, but adhering to the requirements of their clients.

This can lead to a situation where a third-party processor does not comply with EU/UK-GDPR regulations. For example, if you use an advertising agency to run your ads, and they have not completed EU/UK-GDPR-required training on your behalf (they are only required to do so on their own behalf), then they may fail to meet the requirements of the GDPR and cause your business serious problems with compliance.

The significance for businesses who use third parties to perform services related to their data processing activities (such as hosting websites or running advertising campaigns) is to ensure that those third parties have been properly trained in how best to comply with EU/UK-GDPR regulations.

Task: Checking for EU/UK-GDPR Compliance. Tick off as you go.	
Audit your data processor, make sure they have sufficient guarantees about security, to do this you can:	
Check business qualification/certificates.	
Audit reports.	
Other:	

Task: Sub-processors. These are not allowed without the explicit permission of the data controller Tick off as you go.	
Check whether your data processor uses sub-processors.	
Check business qualification/certificates.	
Ensure that your processor has suitable contract with their sub-processor.	
Tick this box when completed.	
Contracts with data processors must contain clauses relating to:	
Responsibilities.	
Liabilities.	
Subject matter of the processing.	
Duration of processing.	
Nature and purpose of processing.	
Types of personal data involved.	
The categories of data subjects.	
The data controller's obligation/rights (this will be your business).	
Individual rights (how they will be handled).	

Guidelines & Legislation

Specific terms or clauses must include:	
Processing only on the data controller's documented instructions.	
The duty of confidence.	
Appropriate security measures that follow article 32 of GDPR.	
The terms of using sub-processors.	
Data subjects' rights.	
Assisting the data controller.	
End-of-contract provisions.	
Audits and inspections.	

Contract Notes:

Tick the box once you have completed this topic.

4. GDPR: Individual Rights.

The EU/UK-GDPR grant individuals the right to access, rectify, erase, and restrict personal data.

The right to be informed. This includes being told what personal data is collected and how it will be used. In addition, information must be provided on how long the data will be stored and its source.

The right of access. Individuals have the right to request copies of their personal data from any organisation that holds it. They can also request an explanation for why their information is being held and how it's being used.

The right to rectification. If a company has collected incorrect or incomplete information about an individual, they can compel them to correct it.

The right to erasure (or "the right of deletion"). This allows an individual to request that companies delete all their personal information from their systems, unless they have a legitimate reason not to do so (such as needing it for legal reasons).

There are however exceptions to the individual rights:

- Crime and taxation: general
- Crime and taxation: risk assessment
- Legal professional privilege
- Functions designed to protect the public
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Judicial appointments, independence and proceedings
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest
- Health, education and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks
- Other exemptions

Guidelines & Legislation

GDPR: Right of Access.

The right to access is one of the most important rights granted by GDPR. It allows an individual to ask a business for copies of all the personal data they have on them, as well as information about how they use it, and where it came from.

Individuals also have the right to know what data is being collected about them, and how long it will be kept. This can be helpful in a variety of situations, for example: if they want to dispute something, such as data contained within a credit report.

You also have the right to request an electronic copy of your personal data in a machine readable format, such as: CSV or JSON.

You may receive a subject access request (SAR) in the following forms:	
Verbally.	
In writing (in a letter by post.)	
Electronically (email, online contact form, etc.)	
Responding to a subject access request.	
As soon as possible.	
A maximum of 28 days.	
Conditions of a subject access request:	
Situation	**Your possible actions**
SAR from a minor.	Are they mature enough to respond to the request?
SAR from a minor's guardian.	Allow if the minor authorises it or is for the best of the child.
A large request.	Ask for more specific information to make fulfilling the request easier. You should still work on getting the information while waiting for response.
Unsure of identity of person.	Request ID (The time period of your response pauses till you get ID).
Contains information about another individual.	Try to complete the response without the data of the other individual included. If you can't, you don't have to comply unless the other individual gives consent or it is reasonable. Either action requires you to respond to the requester, with justification of action. **Keep a record of justification.**
The time to respond can be increased in cases where: (2 months extension only)	
Complex request.	
Number of requests from a single individual.	
You cannot charge a fee unless the subject access request is excessive: (in most cases)	
Subject Access Request Fulfilment: Data Formats.	
Fulfil the request in the format the individual requests.	
If the individual does not specify a format, return it in the same format the request was made.	
Use a secure method to transfer the information using encryption or other secure methodologies.	

Guidelines & Legislation

You can only refuse a subject access request if:

An exemption applies.

Restrictions apply.

If the request is manifestly unfounded and or excessive.

If you have grounds to refuse a subject access request, you must inform the requestee of:

- The reason why.
- Their right to make a complaint to the relevant authority (ICO for individuals residing within the UK.)
- Their right to enforce their request rights through the courts.

Record Keeping: Keep a record of the following information from subject access requests.

The date of the request.

The date of response.

Who responded to the request.

What information was provided to fulfil the request.

Right of Access Notes:

Tick the box once you have completed this topic.

Guidelines & Legislation

GDPR: Right of Rectification.

Individuals have the right to have information rectified or completed if it is currently incomplete. This section of GDPR will guide you in case you get a request to complete this. Anyone within the business can be asked to fulfil this request so knowing about this right is an important part of GDPR.

You may receive a right to rectification request in the following forms:

Verbally.

In writing (in a letter by post.)

Electronically (email, online contact form, etc.)

How to recognise a right to rectification a request.

Create a policy or plan of action for when an employee receives a request of this nature.

Responding to a subject access request.

As soon as possible.

A maximum of 28 days.

You request ID. An ID request pauses your time to respond until received.

The time to respond can be increased in cases where: (2 months extension only)

Complex request.

Number of requests from a single individual.

While verifying the accuracy of a request:

Restrict the processing of the relevant data.

When you receive a request, you should:

Fix or change the relevant data.

If you believe that the data is accurate, you should:

You must inform the requestee of:

- Your decision
- Their right to make a complaint to the relevant authority (ICO for individuals residing within the UK.)
- Their right to enforce their request rights through the courts.

You can refuse to comply if:

If the request is manifestly unfounded (demonstrate to requestee, and explain your reason to the ICO.)

You cannot charge a fee unless the subject access request is excessive: (in most cases)

Keep a record of:

Past information, for example if the incorrect information was a mistake your business made.

Inform third-parties that use the data that there has been an update.

Tick the box once you have completed this topic.

Guidelines & Legislation

GDPR: Right of Erasure.

The right of erasure is an EU/UK-GDPR-specific right that allows an individual to request the removal of their personal data from any databases or systems where it's stored. This means that if someone requests their data be erased, the business must remove it from their records and systems—and not just keep it in a backup location.

This right of erasure is intended to protect citizens' privacy rights by allowing them to erase their personal information from the databases of businesses that have collected and stored it without consent. It also covers situations where an individual's personal information has been collected under false pretences—for example, if they provided it to a business during the job application process and then later decided they didn't want their information shared with other businesses.

You may receive a right of erasure request in the following forms:

- Verbally.
- In writing (in a letter by post.)
- Electronically (email, online contact form, etc.)

The right of erasure does not exist:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation.
- For the performance of a task carried out in the public interest, or in the exercise of official authority.
- For archival purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
- For the establishment, exercise or defence of legal claims.
- For certain special category data including (2 cases):
  - **Case 1**: The processing is necessary for public health purposes in the public interest.

  Or:
  - **Case 2:** If the processing is necessary for the purposes of preventative or occupational medicine
  - **Case 2:** For the working capacity of an employee.
  - **Case 2:** For medical diagnosis.
  - **Case 2:** For the provision of health or social care.
  - **Case 2:** For the management of health or social care systems or services.

  Case 2 only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy

Guidelines & Legislation

The right to erasure applies if:

The data is no longer necessary for the purpose for which you originally collected or processed it for.

You rely on consent as your lawful basis for holding the data, and the individual withdraws their consent.

You rely on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.

You're processing the data for direct marketing purposes and the individual objects to that processing.

You've processed the data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle.)

You have to do it to comply with a legal obligation.

You have processed the personal data to offer information society services to a minor.
Note: Give it some weight if permission was given as a minor even if they are no longer a minor, as at the time they may not have fully understood the risks of any data collecting consent they gave.

Recognising a right to erasure request: Create a plan of action for when you receive a request of this nature.

Responding to a right to erasure request.

As soon as possible.

A maximum of 28 days, or you request ID. An ID request pauses your time to respond until it's received.

The time to respond can be increased in cases where: (2 months extension only)

The request is complex.

Number of requests from a single individual.

While verifying the accuracy of a request, restrict the processing of the relevant data.

When you receive a request, you should:

Erase the data from current systems and any backups. Once fulfilled, explain all parts that have been erased to the individual who requested. Make sure to include the mention of data that was erased in a backup.
Note: Circumstances may require erasure for live system data, but kept on backups until overwritten.

You can refuse to comply if:

If the request is manifestly unfounded (demonstrate to requestee, and explain your reason to the ICO.)

Excessive. This only applies as a legitimate reason to refuse if it's purposefully excessive.

If you refuse:

You must inform the requestee of:

- The reason why.
- Their right to make a complaint to the relevant authority (ICO for individuals residing within the UK.)
- Their right to enforce their request rights through the courts.

You cannot charge a fee unless the right of erasure request is excessive: Any fee can only cover admin costs.

You must inform third-parties of the erasure under the following circumstances:

The personal data has been disclosed to others.

The personal data has been made public in an online environment.

Tick the box once you have completed this topic.

Guidelines & Legislation

GDPR: Right to Restrict - Sometimes referred to as "the right to be forgotten."

The right to restrict is the right to prevent others from processing an individual's personal data.

Individuals have this right if a business is processing their data unlawfully, if they are in dispute with that business and have objected to the processing, and if the controller has no overriding legitimate grounds for continuing the processing.

If someone want to exercise this right, they must contact the controller directly and tell them that they are objecting to the processing. They can also request that they stop processing their personal data and delete any copies of it.

You may receive a right to restrict request in the following forms:
Verbally.
In writing (in a letter by post.)
Electronically (email, online contact form, etc.)
The right of restriction can apply when:
The individual contests the accuracy of their personal data and you are verifying the data's accuracy.
The data hasn't been lawfully processed and the individual opposes erasure and requests restriction.
You no longer need the data but the individual needs you to keep it to establish, exercise or defend a legal claim.
The individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.
Recognising a right to erasure request: Create a plan of action for when you receive a request of this nature.
Responding to a right to erasure request.
As soon as possible.
A maximum of 28 days, or you request ID. An ID request pauses your time to respond until it's received.
The time to respond can be increased in cases where: (2 months extension only)
The request is complex.
Number of requests from a single individual.
While verifying the accuracy of a request, restrict the processing of the relevant data.
When you receive a request, you should:
Stop processing the data of the individual for an amount of time that coincides with their reason for requesting. You must let them know before unrestricting the data, including the reasons based on article 16 and 21 – follow the section on the table regarding if you refuse. **Processing of Data Includes:** collection, structuring, dissemination and erasure. **Examples of restriction:** • temporarily moving the data to another processing system • making the data unavailable to users • temporarily removing published data from a website • other

Guidelines & Legislation

What can be done with restricted data - You can process the data when:

You have the individual's consent.

It's for the establishment, exercise, or defence of legal claim.

It's for the protection of the rights of another person (natural or legal).

It's for reasons of important public interest.

You can refuse to comply if:

If the request is manifestly unfounded
(demonstrate to requestee, and explain your reason to the ICO.)
Manifestly unfounded typically refers to acts of:

- Blackmail
- Malicious intent (disruption, individual stated a malicious statement in regards to request.)

Excessive. This only applies as a legitimate reason to refuse if it's purposefully excessive.
Purposefully excessive typically refers to:

- Repeated requests.
- Overlapping requests.

If you refuse to comply:

If you have grounds to refuse a right to restrict request, you must inform the requestee of:

- The reason why.
- Their right to make a complaint to the relevant authority (ICO for individuals residing within the UK.)
- Their right to enforce their request rights through the courts.

You cannot charge a fee unless the right to restrict request is excessive: Any fee can only cover admin costs.

You must inform third-parties of the restriction under the following circumstances:

The personal data has been disclosed to others.

The personal data has been made public in an online environment.

Right to Restrict Notes:

Tick the box once you have completed this topic.

Guidelines & Legislation

GDPR: Right to Data Portability.

The right to data portability is a privacy right that UK-GDPR introduced. It allows individuals to obtain a copy of their personal data in a machine-readable format, which they can use to move it to another service provider. This has the potential to be very useful for consumers, as it gives them more control over their information and better tools for managing their own data.

The right is limited by several restrictions: it does not apply to processing that is necessary for the performance of a contract between the individual and the controller, or when there is a legal obligation to respond to a request. Additionally, the right will not apply if there are grounds for believing that disclosure would harm the vital interests of an individual or the legitimate interests of a third party.

You may receive a right to portability request in the following forms:
Verbally.
In writing (in a letter by post.)
Electronically (email, online contact form, etc.)
Recognising a right to portability request: Create a plan of action for when you receive a request of this nature.
Responding to a right to portability request.
As soon as possible.
A maximum of 28 days, or you request ID. An ID request pauses your time to respond until it's received.
The time to respond can be increased in cases where: (2 months extension only)
The request is complex.
Number of requests from a single individual.
Types of information that can be provided to an individual making a right to portability request: **Note:** this only has to be the original data they provided, not data that you have created based on the data given. Exclusions: • Created data by you about the individual. • Anonymous data. • Other individuals' data that will impede on rights of individuals (both parties generally have to agree.)
History of website usage or search activities.
Traffic and location data.
'Raw' data processed by connected objects, such as smart meters and wearable devices.
Email.
Address.
Username.
Name.
Age.
Other:

Guidelines & Legislation

Right of Portability Request Fulfilment:

Option 1: Give them a copy of their data (in a readable format)

Option 2: Transfer data across to another controller (without hindrance/unnecessary road blocks.)

Use a secure method to transfer the information using encryption or other secure methodologies.

Transferring Right of Portability Request Data:

Directly transmitting the requested data to the individual using a secure method of transfer.

Providing access to an automated tool that allows the extraction of the requested data themselves.

The data should be formatted to adhere to the concepts below:

Structured.

In a commonly used format.

In a machine readable format.

Note: Machine-readable format means a structured format that can automatically be read and processed by a computer such as comma-separated values (CSV), JavaScript Object Notation (JSON) or Extensible Markup Language (XML).

Common Formats:

JSON.

CSV.

XML.

You can refuse to comply if:

If the request is manifestly unfounded
(demonstrate to requestee, and explain your reason to the ICO.)
Manifestly unfounded typically refers to acts of:

- Blackmail
- Malicious intent (disruption, individual stated a malicious statement in regards to request.)

Excessive. This only applies as a legitimate reason to refuse if it's purposefully excessive.
Purposefully excessive typically refers to:

- Repeated requests.
- Overlapping requests.

If you refuse to comply:

If you have grounds to refuse a right to restrict request, you must inform the requestee of:

- The reason why.
- Their right to make a complaint to the relevant authority (ICO for individuals residing within the UK.)
- Their right to enforce their request rights through the courts.

You cannot charge a fee unless the right to restrict request is excessive: Any fee can only cover admin costs.

Guidelines & Legislation

Receiving data from a portability request:

- Sort the incoming data to allow you to follow GDPR.
- Delete data that you have no reason to keep you should delete it as soon as possible.
- Keep the third-party data under the control of the individual and only use it for their purposes

Right to Portability Notes:

Tick the box once you have completed this topic.

Guidelines & Legislation

GDPR: Right to Object.

The right to object is a UK-GDPR requirement that allows individuals to object to their data being processed. This means that they can ask the company processing their data to stop doing so, or at least limit the number of people who have access to it.

People have this right if they are under 16 years old, or if they have mental health issues, or disabilities that make them unable to consent. Additionally, individuals have this right if they believe that the data in question was collected illegally. If an individual believes their data has been mishandled in any way, they can opt out of having it used by contacting the company that is handling it for them.

Before you Receive a Right to Object Request:

Inform individuals about the right to object in your first communication where:

You process personal data for direct marketing purposes.

your lawful basis for processing is for:

- A public task (for the performance of a task carried out in the public interest),
- A public task (for the exercise of official authority vested in you), or
- Legitimate interests.

After receiving a request: You may receive a right to object request in the following forms:

Verbally.

In writing (in a letter by post.)

Electronically (email, online contact form, etc.)

A Right to Object Request Applies When: This list isn't exhaustive, it's the most common situations.

A task carried out in the public interest (specific reason needed.)

The exercise of official authority vested in you (specific reason needed.)

Your legitimate interests (or those of a third party) (specific reason needed.)

Direct marketing purposes (an absolute right – you cannot refuse.)

Recognising a right to object request: Create a plan of action for when you receive a request of this nature.

Responding to a right to portability request.

As soon as possible.

A maximum of 28 days, or you request ID. An ID request pauses your time to respond until it's received.

The time to respond can be increased in cases where: (2 months extension only)

The request is complex.

Number of requests from a single individual.

While verifying the accuracy of a request, restrict the processing of the relevant data.

Guidelines & Legislation

When you receive a request, you should:

Make a decision in which you balance the individual's interests, rights, and freedoms with your own legitimate grounds. This can lead your decision to a refusal)

Stop processing the data of the individual for an amount of time that coincides with their reason for requesting. You must let them know before unrestricting the data, including the reasons based on article 16 and 21 – follow the section on the table regarding if you refuse.

You can refuse to comply if:

If the request is manifestly unfounded
(demonstrate to requestee, and explain your reason to the ICO.)
Manifestly unfounded typically refers to acts of:

- Blackmail
- Malicious intent (disruption, individual stated a malicious statement in regards to request.)

Excessive. This only applies as a legitimate reason to refuse if it's purposefully excessive.
Purposefully excessive typically refers to:

- Repeated requests.
- Overlapping requests.

If you refuse to comply:

If you have grounds to refuse a right to restrict request, you must inform the requestee of:

- The reason why.
- Their right to make a complaint to the relevant authority (ICO for individuals residing within the UK.)
- Their right to enforce their request rights through the courts.

You cannot charge a fee unless the right to Object request is excessive: Any fee can only cover admin costs.

Right to Object Notes:

Tick the box once you have completed this topic.

Guidelines & Legislation

GDPR: Rights related to automated decision-making, including profiling.

As systems are getting more sophisticated ,a lot more of data processing is being done by computers and algorithms. This right is a way to make sure that the algorithms are not over used for every possible type of data.

Automated decision-making, including profiling, can only be carried out when:

- Necessary for entering into or performance of a contract between an organisation and the individual.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decision-making including profiling can only be carried out when:

Special Category Data:

- You have the individual's explicit consent.
- The processing is necessary for reasons of substantial public interest.

Before carrying out automated decision-making including profiling, you must first:

- Complete a data protection impact assessment (DPIA.)
- Give individuals specific information about the processing.
- Take steps to prevent errors, bias, and discrimination.
- Individuals' rights to challenge and request a review of the decision.
- Provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual.
- Use appropriate mathematical or statistical procedures.
- Ensure that individuals can:
  - Obtain human intervention;
  - Express their point of view; and
  - Obtain an explanation of the decision and challenge it;
- Put appropriate technical and organisational measures in place, so that you can correct any inaccuracies and minimise the risk of further errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that also prevents discriminatory effects.

Rights Related to Automated Decision-Making Notes:

Tick the box once you have completed this topic.