Security

You might have noticed we've made some changes to our website. This includes changes to the Guide to the UK GDPR, which has been broken down into smaller guides such as this one.

■ Latest updates

> **19 May 2023** - we have broken the Guide to the UK GDPR down into smaller guides. All the content stays the same.

At a glance

- A key principle of the UK GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.
- We have worked closely with the National Cyber Security Centre (NCSC) to develop an approach that you can use when assessing the measures that will be appropriate for you.

Checklists

☐ We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.

☐ When deciding what measures to implement, we take account of the state of the art and costs of implementation.

☐ We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.

☐ Where necessary, we have additional policies and ensure that controls are in place to enforce them.

☐ We make sure that we regularly review our information security policies and measures and, where necessary, improve them.

☐ We have assessed what we need to do by considering the security outcomes we want to achieve.

☐ We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

☐ We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.

☐ We use encryption and/or pseudonymisation where it is appropriate to do so.

☐ We understand the requirements of confidentiality, integrity and availability for the personal data we process.

☐ We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

☐ We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.

☐ Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

☐ We ensure that any data processor we use also implements appropriate technical and organisational measures.

In brief

What does the UK GDPR say about security?

Article 5(1)(f) of the UK GDPR concerns the ‘integrity and confidentiality’ of personal data. It says that personal data shall be:

> 'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

You can refer to this as the UK GDPR’s ‘security principle’. It concerns the broad concept of **information security**.

This means that you must have appropriate security in place to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

You need to consider the security principle alongside Article 32 of the UK GDPR, which provides more specifics on the security of your processing. Article 32(1) states:

> ‘Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk’

Further Reading

Relevant provisions in the UK GDPR - See Articles 5(1)(f) and 32, and Recitals 39 and 83
External link

Why should we worry about information security?

Poor information security leaves your systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases.

Some examples of the harm caused by the loss or abuse of personal data include:

- identity fraud;
- fake credit card transactions;
- targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
- witnesses put at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Although these consequences do not always happen, you should recognise that individuals are still entitled to be protected from less serious kinds of harm, for example embarrassment or inconvenience.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the UK GDPR.

The ICO is also required to consider the technical and organisational measures you had in place when considering an administrative fine.

What do our security measures need to protect?

The security principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as 'confidentiality, integrity and availability' and under the UK GDPR, they form part of your obligations.

What level of security is required?

The UK GDPR does not define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

This reflects both the UK GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:

- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf.

Further Reading

Relevant provisions in the UK GDPR - See See Article 32(2) and Recital 83

External link

We cannot provide a complete guide to all aspects of security in all circumstances for all organisations, but this guidance is intended to identify the main points for you to consider.

What organisational measures do we need to consider?

Carrying out an information risk assessment is one example of an organisational measure, but you will need to take other measures as well. You should aim to build a culture of security awareness within your organisation. You should identify a person with day-to-day responsibility for information security within your organisation and make sure this person has the appropriate resources and authority to do their job effectively.

Example

The Chief Executive of a medium-sized organisation asks the Director of Resources to ensure that appropriate security measures are in place, and that regular reports are made to the board.

The Resources Department takes responsibility for designing and implementing the organisation's security policy, writing procedures for staff to follow, organising staff training, checking whether security measures are actually being adhered to and investigating security incidents.

Clear accountability for security will ensure that you do not overlook these issues, and that your overall security posture does not become flawed or out of date.

Although an information security policy is an example of an appropriate organisational measure, you may not need a 'formal' policy document or an associated set of policies in specific areas. It depends on your size and the amount and nature of the personal data you process, and the way you use that data. However, having a policy does enable you to demonstrate how you are taking steps to comply with the security principle.

Whether or not you have such a policy, you still need to consider security and other related matters such as:

- co-ordination between key people in your organisation (eg the security manager will need to know about commissioning and disposing of any IT equipment);
- access to premises or equipment given to anyone outside your organisation (eg for computer maintenance) and the additional security considerations this will generate;
- business continuity arrangements that identify how you will protect and recover any personal data you hold; and
- periodic checks to ensure that your security measures remain appropriate and up to date.

What technical measures do we need to consider?

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering physical security, you should look at factors such as:

- the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
- how you control access to your premises, and how visitors are supervised;
- how you dispose of any paper and electronic waste; and
- how you keep IT equipment, particularly mobile devices, secure.

In the IT context, technical measures may sometimes be referred to as ‘cybersecurity’. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them.

When considering cybersecurity, you should look at factors such as:

- system security – the security of your network and information systems, including those which process personal data;
- data security – the security of the data you hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely;
- online security – eg the security of your website and any other online service or application that you use; and
- device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

Depending on the sophistication of your systems, your usage requirements and the technical expertise of your staff, you may need to obtain specialist information security advice that goes beyond the scope of this guidance. However, it’s also the case that you may not need a great deal of time and resources to secure your systems and the personal data they process.

Whatever you do, you should remember the following:

- your cybersecurity measures need to be appropriate to the size and use of your network and information systems;

- you should take into account the state of technological development, but you are also able to consider the costs of implementation;
- your security must be appropriate to your business practices. For example, if you offer staff the ability to work from home, you need to put measures in place to ensure that this does not compromise your security; and
- your measures must be appropriate to the nature of the personal data you hold and the harm that might result from any compromise.

A good starting point is to make sure that you're in line with the requirements of Cyber Essentials – a government scheme that includes a set of basic technical controls you can put in place relatively easily.

You should however be aware that you may have to go beyond these requirements, depending on your processing activities. Cyber Essentials is only intended to provide a 'base' set of controls, and won't address the circumstances of every organisation or the risks posed by every processing operation.

A list of helpful sources of information about cybersecurity is provided below.

Further reading – ICO/NCSC security outcomes

We have worked closely with the NCSC to develop a set of security outcomes that you can use to determine the measures appropriate for your circumstances.

The Accountability Framework looks at the ICO's expectations in relation to security.

Further reading – ICO guidance

Under the 1998 Act, the ICO published a number of more detailed guidance pieces on different aspects of IT security. Where appropriate, we will be updating each of these to reflect the UK GDPR's requirements in due course. However, until that time they may still provide you with assistance or things to consider.

- IT asset disposal for organisations (pdf) – guidance to help organisations securely dispose of old computers and other IT equipment;
- A practical guide to IT security – ideal for the small business (pdf);
- Protecting personal data in online services – learning from the mistakes of others (pdf) – detailed technical guidance on common technical errors the ICO has seen in its casework;
- Bring your own device (BYOD) (pdf) – guidance for organisations who want to allow staff to use personal devices to process personal data;
- Cloud computing (pdf) – guidance covering how security requirements apply to personal data processed in the cloud; and
- Detailed guidance on encryption – advice on the use of encryption to protect personal data.

Other resources

Homepage of the Cyber Essentials scheme

What if we operate in a sector that has its own security requirements?

Some industries have specific security requirements or require you to adhere to certain frameworks or standards. These may be set collectively, for example by industry bodies or trade associations, or could be set by other regulators. If you operate in these sectors, you need to be aware of their requirements, particularly if specific technical measures are specified.

Although following these requirements will not necessarily equate to compliance with the UK GDPR's security principle, the ICO will nevertheless consider these carefully in any considerations of regulatory action. It can be the case that they specify certain measures that you should have, and that those measures contribute to your overall security posture.

Example

If you are processing payment card data, you are obliged to comply with the Payment Card Industry Data Security Standard. The PCI-DSS outlines a number of specific technical and organisational measures that the payment card industry considers applicable whenever such data is being processed.

Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the UK GDPR's security principle, if you process card data and suffer a personal data breach, the ICO will consider the extent to which you have put in place measures that PCI-DSS requires particularly if the breach related to a lack of a particular control or process mandated by the standard.

What do we do when a processor is involved?

If one or more organisations process personal data on your behalf, then these are data processors under the UK GDPR. This can have the potential to cause security problems – as a data controller you are responsible for ensuring compliance with the UK GDPR and this includes what the processor does with the data. However, in addition to this, the UK GDPR's security requirements also apply to any processor you use.

This means that:

- you must choose a data processor that provides sufficient guarantees about its security measures;
- your written contract must stipulate that the processor takes all measures required under Article 32 – basically, the contract has to require the processor to undertake the same security measures that you would have to take if you were doing the processing yourself; and
- you should ensure that your contract includes a requirement that the processor makes available all information necessary to demonstrate compliance. This may include allowing for you to audit and

inspect the processor, either yourself or an authorised third party.

At the same time, your processor can assist you in ensuring compliance with your security obligations. For example, if you lack the resource or technical expertise to implement certain measures, engaging a processor that has these resources can assist you in making sure personal data is processed securely, provided that your contractual arrangements are appropriate.

Further Reading

Relevant provisions in the UK GDPR - See Articles 28 and 32, and Recitals 81 and 83

External link

Further reading

Controllers and processors

Contracts

Should we use pseudonymisation and encryption?

Pseudonymisation and encryption are specified in the UK GDPR as two examples of measures that may be appropriate for you to implement. This does not mean that you are obliged to use these measures. It depends on the nature, scope, context and purposes of your processing, and the risks posed to individuals.

However, there are a wide range of solutions that allow you to implement both without great cost or difficulty. For example, for a number of years the ICO has considered encryption to be an appropriate technical measure given its widespread availability and relatively low cost of implementation. This position has not altered due to the UK GDPR — if you are storing personal data, or transmitting it over the internet, we recommend that you use encryption and have a suitable policy in place, taking account of the residual risks involved.

When considering what to put in place, you should undertake a risk analysis and document your findings.

Further Reading

Relevant provisions in the UK GDPR - See Article 32(1)(a) and Recital 83

External link

In more detail – ICO guidance

Detailed guidance on encryption

What are ‘confidentiality, integrity, availability’ and ‘resilience’?

Collectively known as the ‘CIA triad’, confidentiality, integrity and availability are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for you as a data controller, and for the individuals whose data you process.

The information security measures you implement should seek to guarantee all three both for the systems themselves and any data they process.

The CIA triad has existed for a number of years and its concepts are well-known to security professionals.

You are also required to have the ability to ensure the ‘resilience’ of your processing systems and services. Resilience refers to:

- whether your systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident; and
- your ability to restore them to an effective state.

This refers to things like business continuity plans, disaster recovery, and cyber resilience. Again, there is a wide range of solutions available here, and what is appropriate for you depends on your circumstances.

Further Reading

Relevant provisions in the UK GDPR - See Article 32(1)(b) and Recital 83

External link

What are the requirements for restoring availability and access to personal data?

You must have the ability to restore the availability and access to personal data in the event of a physical or technical incident in a ‘timely manner’.

The UK GDPR does not define what a ‘timely manner’ should be. This therefore depends on:

- who you are;
- what systems you have; and
- the risk that may be posed to individuals if the personal data you process is unavailable for a period of time.

The key point is that you have taken this into account during your information risk assessment and selection of security measures. For example, by ensuring that you have an appropriate backup process in place you will have some level of assurance that if your systems do suffer a physical or technical incident you can restore them, and therefore the personal data they hold, as soon as reasonably possible.

Example

An organisation takes regular backups of its systems and the personal data held within them. It follows the well-known ‘3-2-1’ backup strategy: three copies, with two stored on different devices and one stored off-site.

The organisation is targeted by a ransomware attack that results in the data being encrypted. This means that it is no longer able to access the personal data it holds.

Depending on the nature of the organisation and the data it processes, this lack of availability can have significant consequences on individuals – and would therefore be a personal data breach under the UK GDPR.

The ransomware has spread throughout the organisation's systems, meaning that two of the backups are also unavailable. However, the third backup, being stored off-site, allows the organisation to restore its systems in a timely manner. There may still be a loss of personal data depending on when the off-site backup was taken, but having the ability to restore the systems means that whilst there will be some disruption to the service, the organisation are nevertheless able to comply with this requirement of the UK GDPR.

Further Reading

Relevant provisions in the UK GDPR - See Article 32(1)(c) and Recital 83

External link

Are we required to ensure our security measures are effective?

Yes, the UK GDPR specifically requires you to have a process for regularly testing, assessing and evaluating the effectiveness of any measures you put in place. What these tests look like, and how regularly you do them, will depend on your own circumstances. However, it's important to note that the requirement in the UK GDPR concerns your measures in their entirety, therefore whatever 'scope' you choose for this testing should be appropriate to what you are doing, how you are doing it, and the data that you are processing.

Technically, you can undertake this through a number of techniques, such as vulnerability scanning and penetration testing. These are essentially 'stress tests' of your network and information systems, which are designed to reveal areas of potential risk and things that you can improve.

In some industries, you are required to undertake tests of security measures on a regular basis. The UK GDPR now makes this an obligation for all organisations. Importantly, it does not specify the type of testing, nor how regularly you should undertake it. It depends on your organisation and the personal data you are processing.

You can undertake testing internally or externally. In some cases it is recommended that both take place.

Whatever form of testing you undertake, you should document the results and make sure that you act upon any recommendations, or have a valid reason for not doing so, and implement appropriate safeguards. This is particularly important if your testing reveals potential critical flaws that could result in a personal data breach.

Further Reading

Relevant provisions in the UK GDPR - See Article 32(1)(d) and Recital 83

External link

What about codes of conduct and certification?

If your security measures include a product or service that adheres to a UK GDPR code of conduct or certification scheme, you may be able to use this as an element to demonstrate your compliance with the security principle. It is important that you check carefully that the code or certification scheme has been approved by the ICO.

Further Reading

Relevant provisions in the UK GDPR - See Article 32(3) and Recital 83

External link

Further reading

Codes of conduct

Certification

What about our staff?

The GDPR requires you to ensure that anyone acting under your authority with access to personal data does not process that data unless you have instructed them to do so. It is therefore vital that your staff understand the importance of protecting personal data, are familiar with your security policy and put its procedures into practice.

You should provide appropriate initial and refresher training, including:

- your responsibilities as a data controller under the UK GDPR;
- staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- the proper procedures to identify callers;
- the dangers of people trying to obtain personal data by deception (eg by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading your staff to alter information when they should not do so; and
- any restrictions you place on the personal use of your systems by staff (eg to avoid virus infection or spam).

Your staff training will only be effective if the individuals delivering it are themselves reliable and knowledgeable.

Further Reading

Relevant provisions in the UK GDPR - See Article 32(4) and Recital 83

External link

Other resources

The NCSC has detailed technical guidance in a number of areas that will be relevant to you whenever you process personal data. Some examples include:

- 10 Steps to Cyber Security– The 10 Steps define and communicate an Information Risk Management Regime which can provide protection against cyber-attacks.
- The Cyber Essentials scheme – this provides a set of basic technical controls that you can implement to guard against common cyber threats.
- Risk management collection – a collection of guidance on how to assess cyber risk.

The government has produced relevant guidance on cybersecurity:

- CyberAware – a cross-government awareness campaign developed by the Home Office, the Department for Digital, Culture, Media and Sport (‘DCMS’) and the NCSC.
- NCSC small business guide – cyber security guidance for small businesses.

Technical guidance produced by the European Union Agency for Network and Information Security (ENISA) may also assist you:

- Data protection section at ENISA’s website

Encryption

At a glance

- The UK GDPR requires you to implement appropriate technical and organisational measures to ensure you process personal data securely.
- Article 32 of the UK GDPR includes encryption as an example of an appropriate technical measure, depending on the nature and risks of your processing activities.
- Encryption is a widely-available measure with relatively low costs of implementation. There is a large variety of solutions available.
- You should have an encryption policy in place that governs how and when you implement encryption, and you should also train your staff in the use and importance of encryption.
- When storing or transmitting personal data, you should use encryption and ensure that your encryption solution meets current standards.
  You should be aware of the residual risks of encryption, and have steps in place to address these.

Checklists

☐ We understand that encryption can be an appropriate technical measure to ensure that we process personal data securely.

☐ We have an appropriate policy in place governing our use of encryption.

☐ We ensure that we educate our staff on the use and importance of encryption.

☐ We have assessed the nature and scope of our processing activities and have implemented encryption solution(s) to protect the personal data we store and/or transmit.

☐ We understand the residual risks that remain, even after we have implemented our encryption solution(s).

☐ Our encryption solution(s) meet current standards such as FIPS 140-2 and FIPS 197.

☐ We ensure that we keep our encryption solution(s) under review in the light of technological developments.

☐ We have considered the types of processing we undertake, and whether encryption can be used in this processing.

In brief

- What does the UK GDPR say about encryption?

What does the UK GDPR say about encryption?

- The UK GDPR's security principle requires to you put in place appropriate technical and organisational measures to ensure you process personal data securely.
- Article 32 provides further considerations for the security of your processing. This includes specifying encryption as an example of an appropriate technical measure, depending on the risks involved and the specific circumstances of your processing. The ICO has seen numerous incidents of personal data being subject to unauthorised or unlawful processing, loss, damage or destruction. In many cases, the damage and distress caused by these incidents may have been reduced or even avoided had the personal data been encrypted.
- It is also the case that encryption solutions are widely available and can be deployed at relatively low cost.
- It is possible that, where data is lost or destroyed and it was not encrypted, regulatory action may be pursued (depending on the context of each incident).

What is encryption?

- Encryption is a mathematical function that encodes data in such a way that only authorised users can access it.
- It is a way of safeguarding against unauthorised or unlawful processing of personal data, and is one way in which you can demonstrate compliance with the security principle.
- Encryption protects information stored on mobile and static devices and in transmission, and there are a number of different encryption options available.
- You should consider encryption alongside other technical and organisational measures, taking into account the benefits it can offer and the risks it can pose.
- You should have a policy in place governing the use of encryption, including appropriate staff education.
- You should also be aware of any sector-specific guidance that applies to you, as this may require you to use encryption.

Encryption and data storage

- Encrypting data whilst it is being stored provides effective protection against unauthorised or unlawful processing.
- Most modern operating systems have full-disk encryption built-in.
- You can also encrypt individual files or create encrypted containers.

- Some applications and databases can be configured to store data in encrypted form.
- Storing encrypted data still poses residual risks. You will need to address these depending on the context of your processing, such as by means of an organisational policy and staff training

Encryption and data transfer

- Encrypting personal data whilst it is being transferred provides effective protection against interception by a third party.
  You should use encrypted communications channels when transmitting any personal data over an untrusted network.
- You can encrypt data prior to transmission over an insecure channel and ensure it is still protected. However, a secure channel provides assurance that the content cannot be understood if it is intercepted. Without additional encryption methods, such as encrypting the data itself prior to transmission, the data will only be encrypted whilst in transit.
- You should look to use HTTPS across your entire site. While there are some circumstances that can make this difficult you still need to take appropriate steps such as ensuring that all areas of user input are protected.
- Encrypted data transfer still poses residual risks. You will need to address these depending on the context, such as by means of an organisational policy and staff training.

What types of encryption are there?

- The two types of encryption in widespread use today are symmetric and asymmetric encryption.
- With symmetric encryption, the same key is used for encryption and decryption. Conversely, with asymmetric encryption, different keys are used for encryption and decryption.
- When using symmetric encryption, it is critical to ensure that the key is transferred securely.
- The technique of cryptographic hashing is sometimes equated to encryption, but it is important to understand that encryption and hashing are not identical concepts, and are used for different purposes.

How should we implement encryption?

- When implementing encryption it is important to consider four things: choosing the right algorithm, choosing the right key size, choosing the right software, and keeping the key secure.
- Over time, vulnerabilities may be discovered in encryption algorithms that can eventually make them insecure. You should regularly assess whether your encryption method remains appropriate.
- It is important to ensure that the key size is sufficiently large to protect against an attack over the lifetime of the data. You should therefore assess whether your key sizes remain appropriate.
- The encryption software you use is also crucial. You should ensure that any solution you implement meets current standards such as FIPS 140-2 and FIPS 197.
- Advice on appropriate encryption solutions is available from a number of organisations, including the National Cyber Security Centre (NCSC).
- You should also ensure that you keep your keys secure, and have processes in place to generate new keys when necessary to do so.

Encryption scenarios

There are a number of typical data processing activities where you should consider the use of encryption. These are outlined in our detailed guidance which includes a section on common scenarios.

In each case, it is important that you consider the residual risks that remain even after you put the encryption in place.

Further reading

Security

Security outcomes

Data protection by design and default

We have published detailed guidance on encryption including a number of common scenarios and risks.

Ransomware and data protection compliance

At a glance

- Personal data breaches from the ICO’s caseload during 2020/2021 have seen a steady increase in the number and severity caused by ransomware. This is a type of malicious software or “malware” designed to block access to computer systems, and the data held within them, using encryption.
- Ransomware is a type of malware that attempts to unlawfully encrypt files on a host computer system.
- This guidance presents eight scenarios about the most common ransomware compliance issues we have seen.

Checklist

Governance

☐ We establish and communicate a set of suitable security policies that provide direction to appropriate levels of security.

Asset identification

☐ We identify, document and classify the personal data we process and the assets that process it. Examples of personal data that typically require a higher classification level include large volumes of data, children's data and special category data.

Technical control selection

☐ We determine and document appropriate controls to protect the personal data we process. We use the NCSC Mitigating Malware and Ransomware guidance to give us a set of practical controls we can implement to prevent ransomware.

Access controls

☐ We implement appropriately strong access controls for systems that process personal data. For internet facing services, such as remote access solutions, we enable multi-factor authentication or other alternatively strong access controls.

Vulnerability management

☐ We implement a policy that defines our approach to patch management. We prioritise patches relating to internet-facing services, as well as critical and high risk patches. We use the NCSC Vulnerability management guidance to support us further.

Staff education and awareness

☐ We ensure all relevant staff have a baseline awareness of attacks such as phishing. We consider providing additional and specific security training for staff with responsibility for IT Infrastructure and security services.

Detection

☐ We implement appropriate controls to be able to detect and respond to an attack before it can exploit the personal data we process. If we are a smaller organisations, we use the NCSC Logging Made Easy solution to support us in developing basic enterprise logging capability.

Incident response

☐ We define an incident response plan that guides us in the event of a ransomware attack. We include thresholds for ICO and affected individual notifications.

☐ We perform regular tests of our plan, for example, the NCSC Exercise in a Box helps us practise our response in a safe environment.

Disaster recovery

☐ We have disaster recovery and business continuity plans to support us in restoring personal data in a timely manner. Measures such as offline backups or those described in the NCSC "Offline backups in an online world" blog are important to ensure we can restore personal data.

Assurance

☐ We test, assess and evaluate our control environment using measures such as audits, vulnerability scanning, penetration testing and accreditation against proven security standards such as NCSC Cyber Essentials and other relevant standards of good practice.

In brief

What is ransomware?

Ransomware is a type of malware that attempts to unlawfully encrypt files on a host computer system.

A ransomware attack occurs when an attacker gains access to an organisation's computer systems and delivers malicious software into the network. This software, or 'payload,' then makes the data unavailable through encryption or deletion. Ransomware is often designed to spread from device to device to maximise the number of files it can encrypt.

The 'ransom' element comes from the ransom note left by the attacker requesting payment in return for restoring the data. This is usually done by a decryption key that only the attacker can access.

Where personal data is encrypted as the result of a ransomware attack, that constitutes a personal data breach because you have lost timely access to the data.

Unless you have a backup of the data, you will not usually be able to recover it unless you decide to comply with the attacker's demand for payment. Even if you decide to pay the ransom fee, there is no guarantee that the attacker will supply the key to allow you to decrypt the files.

Why is ransomware an important data protection topic?

In recent years, ransomware attacks are one of the most common cyber incidents affecting personal data. The attack can lead to the loss of timely access to personal data. Permanent data loss can also occur, if appropriate backups are not in place.

The National Cyber Security Centre (NCSC) recognises ransomware as the biggest cyber threat facing the United Kingdom. The most recent threat landscape report from the European Union Agency for Cyber Security (ENISA) has also assessed ransomware as the prime threat with cybercriminals increasingly motivated by monetisation.

The attacks are becoming increasingly damaging and this trend is likely to continue. Malicious and criminal actors are finding new ways to pressure organisations to pay. For example, through uploading a copy of your data and threatening to publish it.

As criminal actors look for additional ways to exploit the captured data, the risks to individuals have increased, including:

- potential permanent personal data loss;
- potential loss of control over their personal data;
- being further targeted in social engineering style attacks using the breached data (eg phishing emails); and
- their personal data being further maliciously used by criminal actors (eg to facilitate identify and financial fraud).

Sectors such as education, health, legal services and business are amongst the most targeted. However, all UK businesses that process personal data are at risk. This is due to the low barriers to entry, such as by using ransomware-as-a-service and opportunistic attacks.

What can we do to prevent ransomware?

You should review our checklist above, as well as the following eight scenarios. These are the eight most common ransomware compliance issues we have identified, based on past personal data breaches.

Scenario 1: Attacker sophistication

> I am a small organisation that is aware of the growing threat of ransomware. However, I don't think attackers will be interested in targeting me. If they do, how can I protect the personal data I process?

'Scatter gun' style attacks are a common attack method. This is a type of attack that is indiscriminate and does not have a specific target. For example, the attacker may send thousands of phishing emails attempting to deliver ransomware to at least one victim, whoever that may be.

The NCSC Cyber Essentials is designed to support you in preventing basic and common types of attacks. The measures they describe will help you apply appropriate security measures, which are a requirement of the UK GDPR.

For medium and larger organisations, maintaining good cyber security practices is essential to defend against ransomware attacks. Assessing your cyber security arrangements and capabilities against relevant good practice models can support you protect personal data from the threat of ransomware, such as:

- NCSC 10 Steps to Cyber Security;
- ISO27001 for Information Security; and
- NIST Cyber Security Framework.

The NCSC Mitigating Malware and Ransomware attacks also provides specific guidance that can support you in preventing such attacks.

Scenario 2: Personal data breach

> We have been subjected to a ransomware attack, but personal data has not been uploaded from our systems to the attacker. If the data has not been removed does this mean a personal data breach has not occurred?

If you are subject to a cyber-attack, such as ransomware, you are responsible for determining if the incident has led to a personal data breach. This is your first step in deciding if you should notify the ICO about the incident.

The UK GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Where personal data is taken it typically results in unauthorised disclosure or access to personal data and therefore is a type of personal data breach. However, it is not the only consideration you should make when determining if a personal data breach has occurred.

You may have lost timely access to the personal data, for example because the data has been encrypted. This is a type of personal data breach because you have lost "access to" personal data. Temporary loss of access is also a type of personal data breach. For example, if there is a period of time before you restore from backup.

Therefore, loss of access to personal data is as much of a personal data breach as a loss of confidentiality.

However, just because a personal data breach has occurred does not automatically mean you should notify the ICO. Scenario 3 deals with a common breach notification scenario.

Scenario 3: Breach notification

We have established a personal data breach has occurred, but data has not been exfiltrated, therefore there are no risk to individuals. Do we still need to notify the ICO?

You are required to notify the ICO of a personal data breach without undue delay and no later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

This means once you have established a personal data breach has occurred, you should undertake a formal risk assessment. This is to determine the risks to individuals and the likelihood of such risks occurring. If you determine the risks to be unlikely, you do not need to notify the ICO. However, you must keep a record of any personal data breaches, regardless of whether you are required to notify, together with the risk assessment undertaken.

Where data is uploaded from your systems to the attacker it can increase the risks to individuals. Therefore, you should take data exfiltration into account as part of your risk considerations. Appropriate logging can support you in determining if personal data is likely to have been exfiltrated. The NCSC blog post "What exactly should we be logging" can support you in deciding what logs to collect and retain.

Without appropriate logs you may not generate the evidence to allow you to make an informed decision. If you determine there is no evidence of data exfiltration, the ICO may ask you to demonstrate what logs and measures you used to make this decision.

However, whilst exfiltration is an important consideration it is not the only one you should make. You should consider the rights and freedoms of individuals in totality. For example:

- Does the lack of availability impact on any individual rights, such as right of access to the personal data?
- Have individuals lost control of their personal data?
- Can you restore the personal data in a timely manner? If not, what does this mean for individuals?
- To what degree was the personal data exposed to unauthorised actors and what are their likely motivations?
- How confident are you in your detection and monitoring controls – could you have detected personal data being uploaded if it had occurred? If you do not have appropriate logs to make an informed decision, it may be helpful to determine if the attacker had the means, motivation and opportunity to

exfiltrate the data. You can then use this assessment to make a risk-based decision.

Further reading

The ICO’s Personal data breach assessment tool can support you in identifying reportable personal data breaches.

Our guidance on personal data breaches can also further support you in assessing reportable personal data breaches.

Scenario 4: Law enforcement

A ransomware attack has breached the personal data we process. We are planning to notify individuals, however, law enforcement are currently collecting evidence as this was a criminal attack. They have requested we delay notifying individuals until they has completed this. How do I comply with my GDPR obligations whilst also cooperating with law enforcement?

If you have been subjected to a ransomware attack it is recommended you should contact law enforcement.

Law enforcement play a fundamental role in protecting individuals and the ICO work closely with these agencies in providing a multi-agency response to ransomware. Recitals 86 and 88 of the UK GDPR provide direction should law enforcement recommend delaying data subject notification:

Recital 86:

> Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities

Recital 88:

> Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach

However, law enforcement involvement does not automatically mean you should delay notifying individuals. Should law enforcement request a delay in a public notification, you should work closely with the ICO. This will allow us to work with you and law enforcement to assess the risk to the individuals under respective legislation.

Scenario 5: Attacker tactics, techniques and procedures

> We have recently seen an increase in phishing emails coming into our organisation and are looking at what measures we can put in place to mitigate this risk. Are there any other specific attacker tactics that the ICO commonly see in ransomware attacks?

Tactics, techniques and procedures (TTPs) describe the methods attackers use to compromise data. Different attacks will use different types of TTPs, for example phishing is a common TTP to trick someone into giving up their credentials.

However, attacker TTPs are constantly evolving, as described within scenario one of this report. A good baseline of controls will reduce the likelihood of being exploited by basic levels of attack, such as those described in the NCSC Cyber Essentials.

Frameworks are available, such as the Mitre ATT&CK that provide a knowledgebase of TTP based on real world observations. The framework outlines each stage of an attack and the common TTPs that are used. These are a great resource to support you in identifying if your controls are appropriate to resist known TTPs.

During 2020/2021, we identified four of the most common TTPs from ransomware casework. The following practical advice for each example will support you in implementing appropriate measures.

Phishing: Attackers typically use social engineering techniques to trick you into doing something. Phishing is a common method we've seen to either deliver ransomware by email or to trick you into revealing your username and password.

Your security strategy should include ensuring all relevant staff receive basic awareness training in identifying social engineering attacks. In addition, you should consider tailoring the measures in the NCSC Phishing Attack guidance to your own organisation.

Remote access: The most common entry point into a network was by the exploitation of remote access solutions. Attackers often scan the internet for open ports such as remote desktop protocol and use this as an initial entry point. If they can capture valid credentials (eg by phishing, password database dumps or password guessing through brute force), they can authenticate by the remote access solution.

You should risk assess and document your remote access solution and identify appropriate measures in response to the risks. An access control policy that directs you to the minimum levels of controls required will support you in applying appropriate measures.

You should not use single-factor authentication on internet facing services, such as remote access, if it can lead to access to personal data. Use multi-factor authentication, or other comparably secure access controls.

The NCSC device security guidance provides further advice on designing a remote access architecture for enterprise services.

Privileged account compromise: Once an attacker has a foothold in the network it is common that they compromise a privileged account, such as a domain administrator account. This is typically done by either

- compromising weak passwords of privileged accounts;
- compromising service accounts that do not belong to a particular user;
- using well known tools to extract plain text domain administrator passwords, password hashes or Kerberos tickets from the host; or
- exploiting a known software or application vulnerability which has a patch available to fix it.

Once an attacker can elevate their privileges to a domain administrative level account they are typically in a commanding position and will usually deploy the ransomware through the domain controller.

The security of privileged accounts should be a high priority for you. Basic account hygiene can support you in protecting these accounts, such as:

- regular reviews of permissions;
- following the principle of least privilege;
- risk assessments of membership into privileged groups; and
- senior level approval of privileged group membership.

Further reading

The NCSC has a selection of guidance available that can further support you in identifying appropriate measures to protect privileged accounts.

- How to do secure system administration
- Protecting system administration with PAM

Known software or application vulnerabilities: The exploitation of known vulnerabilities where patches were available to fix the issue is a common method used by attackers. This was much more common than zero-day attacks where the vulnerability exploited is not yet publicly known and is typically crafted by advanced levels of attackers. In particular, attackers often scan, sometimes indiscriminately, for known vulnerabilities present in internet-facing device and services.

The NCSC vulnerability management guidance will support you in managing vulnerabilities within your estate.

Considering the following will also support you in managing known vulnerabilities:

- Identify the assets within your organisation, including the software and application you use.
- Define and direct your approach to the patch management lifecycle, including the process of identifying, assessing, acquiring, testing, deploying and validating patches.
- Maintain software and applications that are in support by the vendor.

- Identify vulnerabilities within your estate for both internal and external hardware and software (eg vulnerability scanning).

Scenario 6: Disaster recovery

> We understand the UK GDPR requires appropriate controls to be able to restore personal data in the event of a disaster. We currently backup our data so we are able to restore it in the event of a ransomware attack. Is there anything else we should consider?

A ransomware attack can be amongst the most stressful times for an organisation. Planning for such an event is critical in ensuring you have the measures in place to be able to appropriately respond to it.

For smaller and medium sized organisations the NCSC Small Business Guide Response and Recovery gives you practical advice that will help you plan for dealing with an incident such as a ransomware attack.

For larger organisations the NCSC Incident Management guidance within its 10 steps to cyber security can support you in implementing appropriate controls.

A backup of your personal data is one of the most important controls in mitigating the risk of ransomware. However, it is common that attackers will attempt to either delete or encrypt your backup. You should therefore consider if your current backup strategy could be at risk. Performing a threat analysis against your backup solution and considering how an attacker could delete or encrypt the data is recommended. The questions below will help you get started in your threat assessment:

- Is your backup segregated or offline?
- What would an attacker need to compromise to gain access to the backup? For example, what accounts can access the backup? What accounts can perform deletion or edit the backups? How could an attacker compromise these accounts? How do you protect accounts that can access the backups?
- Are you able to detect changes to your backup? For example, if an attacker initiated a deletion of your backup, could you detect this?
- What device or IP address or both can access the backup repository? Can this be spoofed? Can an attacker access the device or repository that stores the backup?
- How would you respond if an attacker deleted or encrypted your backup?

Using your threat analyses will help you identify controls to mitigate the risks. Offline backups that are completely offline from the main network are one of the most secure ways to prevent attackers from accessing it. If you are using cloud backups, you should read the NCSC blog posts about protecting these backups Offline Backups in on online world and Cloud Backup options for mitigating the risk of ransomware.

Scenario 7: Ransomware payment

> The attacker has provided a ransomware note saying it can restore the data if we pay the ransom fee. The attacker has also stated that if we pay they will not publish the data, so we are also considering if this would further reduce risk to individuals.
>
> Does the ICO recommend the payment of the ransom to restore the data and mitigate risks to individuals?

Before paying the ransom, you should take into account that you are dealing with criminal and malicious actors. Even if you pay, there is no guarantee that they will provide you with the decryption key. “Double extortion” is also common, where you pay for the decryption key and the attacker then requires an additional payment to stop the publication of the data. Attack groups may also target you again in the future if you have shown willingness to pay.

Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. The ICO supports this position.

You should also consider the terminology within the UK GDPR. It requires you to implement “appropriate measures” to restore the data in the event of a disaster. The ICO does not consider the payment of a ransom as an “appropriate measure” to restore personal data.

Appropriate measures include threat assessments, risk assessments and controls such as offline and segregated backups. If you can demonstrate appropriate measures in accordance with the state of the art, cost and risk of processing then you will be able to demonstrate “appropriate measures” and comply with those aspects of the UK GDPR.

If attackers have exfiltrated the personal data, then you have effectively lost control over that data. This means individuals have lost the protections and rights provided by the UK GDPR. For example, transparency of processing or subject access rights. For this reason, we do not view the payment of the ransom as an effective mitigation measure.

If you do decide to pay the ransom to avoid the data being published, you should still presume that the data is compromised and take actions accordingly. For example, the attacker may still decide to publish the data, share the data offline with other attack groups or further exploit it for their own gains. You still need to consider how you will mitigate the risks to individuals even though you have paid the ransom fee.

Scenario 8: Testing and assessing security controls

> I want to protect my organisation and the personal data I process from ransomware. Is there any type of testing I can do to assess whether my controls are appropriate?

The UK GDPR requires you to regularly test, assess and evaluate the effectiveness of your technical and organisational controls using appropriate measures. There is no one test that you can carry out, you should consider this within your wider security framework.

For the examples discussed within this review, we have provided several suggested methods which will support you in adopting appropriate measures:

- **Breach notification**: Document and perform regular tests of your incident response plan so you are prepared for a real incident. The NCSC Exercise in a Box tool can help you practice your incident response in a safe environment.
- **Account management**: Regularly audit your user accounts to ensure they are still required and contain the appropriate privileges. This should include reviews to ensure staff have not retained privileges from previous internal job roles that are no longer required, often called “privilege creep”. Ensure you document such reviews. Consider controls to identify weak or previously breached passwords.
- **Patch management**: Have a method to identify vulnerabilities in your network, such as missing patches. Vulnerability scans are an effective tool that can support this.
- **Attack tactics, techniques and procedure**: Risk assess and document your security controls to determine if they are appropriate to resist known TTPs. Penetration testers often simulate attacker activity by applying TTPs to vulnerabilities within your environment.
- **Audit**: Perform and record regular audits of your environment against a proven security standard, such as Cyber essentials (for smaller organisations) or ISO27001 (for medium and larger organisations).
- **Disaster recovery**: Perform and record regular tests of your disaster recovery plan to ensure it is effective. For example, perform a restore of personal data to ensure the data can be restored within the recovery time objective.

As with any tests, reviews, and assessments, ensure you document and appropriately retain these records, as you may need to submit them to the ICO.

Passwords in online services

At a glance

- Although the UK GDPR does not say anything specific about passwords, you are required to process personal data securely by means of appropriate technical and organisational measures.
- Passwords are a commonly-used means of protecting access to systems that process personal data. Therefore, any password setup that you implement must be appropriate to the particular circumstances of this processing.
- You should consider whether there are any better alternatives to using passwords.
- Any password system you deploy must protect against theft of stored passwords and 'brute-force' or guessing attacks.
- There are a number of additional considerations you will need to take account of when designing your password system, such as the use of an appropriate hashing algorithm to store your passwords, protecting the means by which users enter their passwords, defending against common attacks and the use of two-factor authentication.

In brief

What is this guidance about?

This guidance is intended for use when you want to implement a password-based authentication scheme for an online service. It outlines the considerations that you should have where your authentication scheme will be protecting access to personal data.

Using passwords or other credentials for your internal network and information systems are out of scope of this guidance. However, there may be content that applies in this context all the same.

Before reading and applying this guidance, you should consider whether passwords are the most appropriate method of authenticating users, or whether other alternatives will provide more security and less friction for users.

What is required under the UK GDPR?

The UK GDPR does not say anything specific about passwords. However, Article 5(1)(f) states that personal data shall be:

> ‘Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’

This is the UK GDPR’s ‘integrity and confidentiality’ principle, or, more simply, the ‘security’ principle. So, although there are no provisions on passwords, the security principle requires you to take appropriate technical and organisational measures to prevent unauthorised processing of personal data you hold.

This means that when you are considering a password setup to protect access to a system that processes personal data, that setup must be ‘appropriate’.

Although the UK GDPR does not define what is ‘appropriate’, it does provide further considerations in Article 32, ‘security of processing’:

> ‘Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.’

This means that when considering any measures, you can consider the state of technological development and the cost of implementation – but the measures themselves must ensure a level of security appropriate to the nature of the data being protected and the harm that could be caused by unauthorised access.

In other words, you cannot simply set up a password system and then forget about it – there must be a periodic review process.

What else do we need to do?

You must ensure that you are aware of the state of technological development in this area and that your processes and technologies are robust against evolving threats.

For example, advances in processing power can reduce the effectiveness of cryptography or particular design choices can become outdated.

You must also consider whether there might be better alternatives to passwords that can be used to secure a system.

Article 25 of the UK GDPR also requires you to adopt a data protection by design approach. This means that whenever you develop systems and services that are involved in your processing, you should ensure that you take account of data protection considerations at the initial design stage and throughout the lifecycle. This applies to any password system you intend to use.

At the same time, provided you properly implement a password system, it can be an element that can be used to demonstrate compliance with your obligations under data protection by design.

Further Reading

Relevant provisions in the UK GDPR - See Articles 5(1)(f), 25, 32 and Recitals 39, 78 and 83

External link

Further reading

- Security
- Data protection by design and by default
- ICO/NCSC security outcomes

What are the challenges in choosing the right authentication scheme?

One of the biggest challenges you face when dealing with personal data online is ensuring that such data can be accessed only by those with the correct permissions - in other words, authenticating, and authorising, the individual who is trying to gain access.

It is commonly accepted that there are three main ways of authenticating people to a system – checking for:

- something the individual has (such as a smart card);
- something the individual is (this is usually a biometric measure, such as a fingerprint); or
- something the individual knows.

Of these, the most commonly used is something the individual knows. In most cases something they know is taken to be a password.

Passwords remain the most popular way that individuals authenticate to online services. The reason for this is that a password is generally the simplest method to deploy and the most familiar for individuals.

Despite this, passwords carry well-known risks. The biggest risk is that people passwords as a mathematical problem that can be solved by increasing complexity rules. This fails to take into account natural human behaviour which is to make passwords more easily memorable, regardless of the cost to security.

A rigid focus on password strength rules with no consideration of the usual behaviour of people choosing passwords means that you can make inappropriate choices in setting up and maintaining of your authentication system. This could place the wider security of your systems or your users at risk, and could lead to unauthorised or unlawful access to personal data.

Are passwords the best choice?

The success of using a password to properly authenticate a user of your service relies on the fact that their password remains a shared secret between you and them. When a password is shared amongst users or can be easily guessed by an attacker it can become extremely difficult to tell the difference between an authorised user and an imposter with stolen or guessed credentials.

The proliferation of online services requiring individuals to create an account has created a risk that people become overwhelmed with access credentials and default to reusing a short and memorable password (often coupled with the same email address as a username) across multiple websites.

The risk here is that if one service suffers a personal data breach and access credentials are compromised, these can be tested against other online services to gain access – a technique known as ‘credential stuffing’.

Example

In 2012, the social networking site LinkedIn was hacked. It was thought at the time that passwords for around 6.5 million user accounts were stolen by cybercriminals. However, in May 2016, following the advertisement for sale on the dark web of 165 million user accounts and passwords, LinkedIn confirmed that the 2012 attack had actually resulted in the theft of email addresses and hashed passwords of approximately 165 million users.

The vast majority of the passwords were subsequently cracked and posted online less than a day after the further distribution, largely due to the use of SHA1 without a salt as the hashing algorithm. Due to the reuse of passwords across online services, a number of subsequent account takeovers at other services were attributed to the LinkedIn hack.

Before designing and implementing a new password system, you should consider whether it is necessary to do so, or whether there is a better alternative that can provide secure access.

One common alternative to building your own solution is to utilise a single sign on (SSO) system. While this has its advantages (not least a reduction in the number of passwords that a user has to remember) you must ensure that you are happy with the level of security that is offered by that system. You should ensure that you have a documented record of the considerations you made when reaching this decision.

You must also consider what will happen if the SSO is compromised, as this will most likely result in your user’s accounts also being compromised.

What makes a secure and useable password system?

A good password system is one that provides you with sufficient assurance that the individual attempting to log in is the user they claim to be. In practice, this means a good password system should protect against two types of attack:

- firstly, it should be as difficult as possible for attackers to access stored passwords in a useable form; and
- secondly, it should protect against attackers trying to brute force or guess a valid password and username combination.

Your system should also make it as easy as possible for users to create secure and unique passwords that they can remember or store easily. It should not place an undue burden on individuals to make sure that their account is secure. Putting such barriers in place can result in users making less secure password choices.

The advice provided in this guidance is a good starting point for most systems where personal data is being protected. It will be updated as necessary, but you should consider whether you need to apply a higher level of security given your particular circumstances.

This will largely depend on the nature, scope, context and purposes of your processing and the risks it poses. However, in essence, the more serious the consequences of a compromise, the higher the level of security that you will require.

You should ensure that you stay up to date with the current capabilities of attackers who might try to compromise password systems. You should also consider advice from other sources, such as the National Cyber Security Centre (NCSC) and GetSafeOnline.

Other resources

Guidance on passwords from the NCSC:

- NCSC passwords guidance collection
- Passwords: updating your approach
- Using passwords to protect your data from the NCSC small business guide

Guidance on passwords from GetSafeOnline:

- Password protocol and control

Guidance on avoiding credential stuffing attacks from the Global Privacy Assembly:

- Awareness raising for individuals
- Guidelines for organisations

What should we consider when implementing a password system?

If you are going to put in place a password system, you should take account of factors like:

- how you will process user passwords;
- how your users enter their passwords;
- the requirements you set for user passwords;
- what you do about password expirations and resets;
- the defences you put in place against attacks; and
- any additional considerations.

How should we store passwords?

Do not store passwords in plaintext - make sure you use a suitable hashing algorithm, or another mechanism that offers an equivalent level of protection against an attacker deriving the original password.

Well-known hashing algorithms such as MD5 and SHA1 are not suitable for hashing passwords. Both algorithms have known security weaknesses which can be exploited, and you should not use these for password protection in any circumstances. The biggest weakness with these algorithms is the speed that hashes can be calculated.

You should also consider avoiding other fast algorithms. Use a hashing algorithm that has been specifically designed for passwords, such as bcrypt, scrypt or PBKDF2, with a salt of appropriate length.

It is important that you review the hashing algorithms you use, as over time they can become outdated. Guidance on algorithms is available from a number of organisations such as the NCSC, the National Institute of Standards in Technology (NIST) and the European Union Agency for Cybersecurity (ENISA). You should also be aware of any sector-specific guidelines that are available and may be applicable to you.

You should make sure that you can replace any algorithm that becomes obsolete.

You should also ensure that the architecture around your password system does not allow for any inadvertent leaking of passwords in plaintext.

Example

In 2018, Twitter and GitHub discovered that errors in their logging systems had led to plaintext passwords for users being stored in log files. Although the log files were not exposed to anyone outside of the organisations, both Twitter and GitHub recommended or required that users changed their passwords.

Other resources

Information on the status of a number of hashing functions can be found in NIST Special Publication 800-131A Revision 2 – Transitioning the use of cryptographic algorithms and key lengths (2019) (PDF)

ECRYPT-CSA’s 2018 ‘Algorithms, key size and protocols ↗’ report (external link, PDF) provides further information on the status of cryptographic hash functions.

How should our users enter their passwords?

You should ensure that your login pages are protected with HTTPS, or some other equivalent level of protection. Failure to do so will mean that anyone who is in a position to intercept network traffic can obtain passwords and may be able to carry out replay attacks. You should also consider that browsers now mark pages that require secure input (such as login pages) as insecure if they are delivered over HTTP, and many browsers now mark all pages delivered over HTTP as insecure.

Further reading

Section on data transfer from our guidance on encryption.

Make sure that password hashing is carried out server-side, rather than client-side. Hashing client-side will remove the protection afforded by hashing in the first place, unless other mitigations are put in place. This is a complicated area with a number of factors to consider. At the most basic level, if you are hashing client-side and an attacker obtains your password database, then those hashes can be presented directly to the server for a successful login.

Also, you should not prevent users from pasting passwords into the password field. Preventing pasting is often seen as a security measure, but at the same time doing so can impede people from using password managers effectively. The NCSC’s position on password pasting is the same, as expressed in this blog post ↗ discussing this issue in much more detail. Any attacks that are facilitated by allowing pasting can be defended against with proper rate limiting (see below for more details on rate limiting).

Other resources

Read the NCSC’s ‘Let them paste passwords’ ↗ blog post for more information on why you should allow your users to paste passwords into password fields.

What requirements should we set for user passwords?

There are three general requirements for any password system that you will need to consider:

- password length - you should set a suitable minimum password length (this should be no less than 10 characters), but not a maximum length. If you are correctly hashing your passwords, then the output should be the same length for every password, and therefore the only limit to password length should be the way your website is coded. If you absolutely must set a maximum length due to the limitations of your website code, then tell users what it is before they try to enter a password. The reasoning behind having a maximum length should be documented and fully risk assessed;

- special characters - you should allow the use of special characters, but don't mandate it. If you must disallow special characters (or spaces) make sure this is made clear before the user creates their password; and
- password 'deny lists' - do not allow your users to use a common, weak password. Screen passwords against a password 'deny list' of the most commonly used passwords, leaked passwords from website breaches and common words or phrases that relate to the service. Update this list at least yearly. Explain to users that this is what you are doing, and that this is why a password has been rejected.

Example

A password 'deny list' could be a feature of the software you use. Other lists are available online, e.g. SecLists and haveibeenpwned's password list.

It is also possible to find easy implementations, such as NIST Bad Passwords, which uses SecLists.

Other than the three requirements listed above, do not set restrictions on how users should create a password. Research (see 'Other resources' below) indicates that doing so will cause people to reuse passwords across accounts, to create weak passwords with obvious substitutions or to forget their passwords. All this places unnecessary stress on your reset process and weakens the overall security of your service.

Properly set up and configured password strength meters can be a good way to easily communicate the requirements listed above to your users, and research has shown that good meters can assist users in choosing strong passwords. If you decide to use one, make sure it properly reflects what constitutes a strong or weak password.

Other resources

Microsoft's password guidance (PDF) (external link) contains advice on passwords in the context of several Microsoft platforms. It includes guidance for IT administrators as well as users, and details a number of common password attacks and highlights a number of issues including the risks of placing restrictions on how users create passwords.

Advice from the Federal Trade Commission (FTC) (external link) also discusses these issues.

For more information on password strength meters, read this analysis (external link) from Sophos as well as the significant amount of research (external link) from Carnegie Mellon University.

Finally, remind your users that they should not reuse passwords from other services. In most circumstances you should not know what your user's passwords are. However, some companies actively track compromised credentials that are traded on the dark web and will check these credentials against the hashes they hold on their systems to see if there is a match.

If you decide that this is something you want to do you need to carefully consider the potential legal implications of obtaining such lists, and you will need to explain very clearly how you use that data to your users (especially where the use of such data has led to a password reset or an account lockout).

If users receive an email asking them to reset their password without a proper explanation they will generally assume that the problem is with your service, so it is in your interests to explain precisely why you are taking this action.

What should we do about password expirations and resets?

You should only set password expirations if they are absolutely necessary for your particular circumstances. Regular expiry often causes people to change a single strong password for a series of weak passwords.

As a general rule, get your users to create a strong initial password and only change them if there are pressing reasons, such as a breach of your systems that may have resulted in the password hashes being compromised, or if you receive some other indication that a user's password may have been compromised.

When deploying a password reset process you should ensure that it is secure. Do not send passwords over email, even if they are temporary – use one time links, and ensure that you do not leak the credentials in any referral headers.

You should also not be in a position where a member of your staff is able to 'read out' a user's password to them, eg over the phone in a service call—this indicates that you are storing passwords in plaintext, which is, as described above, not appropriate. If you require a password to validate a user over the phone, set a separate phone password for the account.

You should also time limit any password reset credentials. The majority of users will probably reset their password immediately, but set a limit that fits your observed user behaviour.

Other resources

Read the FTC's advice about the potential issues with mandatory password changes from 2016 (external link).

What defences can we put in place against attacks?

Ensure that you are rate limiting or 'throttling' the number and frequency of incorrect login attempts. The precise number of attempts and the consequence of exceeding these limits will be for you to decide based on the specific circumstances of your organisation, but limiting to a certain number per hour, day and month is a good idea.

This will help to deter both bulk attackers and people targeting individual accounts.

Example

NIST guidance recommends that accounts with internet access should be limited to 100 consecutive failed attempts on a single account unless otherwise specified in the system being deployed.

There are additional considerations when implementing your rate limits:

- you should be aware that some attackers will deliberately work within your limits to avoid detection, and will still achieve a reasonable success rate, especially with targeted guessing;
- set your limits based on observed behaviour of both attackers and your users;
- be aware that overly-aggressive rate limiting can be used as a denial of service attack (remember that the UK GDPR requires the availability of personal data); and
- remember that a number of successful or unsuccessful access attempts to a range of different user accounts from the same device or IP address might be indicative of a bulk attack.

You should also consider whether other methods of preventing attacks might be appropriate. Examples of these methods could include, but are not limited to:

- the use of 'CAPTCHAs';
- creating an 'allow list' of IP addresses; and
- time limits or time delays after failed authentications.

What else do we need to consider?

You need to address how your system will respond to an attacker who has legitimate credentials for a user, or for multiple users. There is a distinct possibility that you will encounter this scenario given that both password reuse and website breaches are relatively common occurrences.

Techniques for recognising common user behaviour are becoming more advanced, and you could use these to develop a risk-based approach to verifying an authentication attempt. For example, if a user logs in from a new device or IP address you might consider requesting a second authentication factor and informing the user by another contact method of the login attempt.

It is however important to remember that collecting additional data from users in order to defend against authentication attacks could itself constitute processing personal data and should operate in compliance with the UK GDPR. This does not mean you cannot process this data, but you must ensure that you have considered the data protection implications of doing so.

You should consider providing your users with the facility to review a list of unsuccessful login attempts. This will allow people who might be specifically targeted to check for potential attacks manually. However, this will only be useful if you pay attention to reports from individuals that their accounts are being attacked.

You should implement two-factor or multifactor authentication wherever it is possible to do so - to take the most common example, a password and a one-time token generator. This will be more important where the personal data that can be accessed is of a sensitive nature, or could cause significant harm if it were compromised.

Other examples of a second factor that could be used include biometrics (fingerprints being the most common and easy to implement), smart cards or U2F keys and devices.

You will however need to ensure that any processing of biometric data for the purposes of uniquely identifying an individual is done in accordance with the requirements for processing special category data in both the UK GDPR and the Data Protection Act 2018.

Further reading

Key definitions section of the Guide to the UK GDPR

Other resources

Additional guidance on digital identities, hashing functions and algorithms and passwords in general includes:

- NIST's Special Publication 800-63 on digital identity guidelines (external link);
- NIST's policy on hashing functions (external link);
- ECRYPT-CSA's 2018 report into 'Algorithms, key size and protocols' (external link, PDF);
- The International Working Group on Data Protection in Telecommunications (the 'Berlin Group') Working Paper on biometrics in online authentication in 2016 (PDF) (external link);
- OWASP cheat sheet on password storage (external link);
- The NCSC's password guidance (external link);
- Additional NCSC guidance on the use of multi-factor authentication in online services (external link). Although primarily aimed at large organisations, this guidance summarises the considerations involved in implementing an 'extra factor' for authentication, including the options for those factors; and
- Cynosure Prime's analysis of 320 million leaked passwords from the HaveIBeenPwned website (external link)

Security outcomes

At a glance

- The UK GDPR requires you to process personal data securely using appropriate technical and organisational measures.
- What's appropriate for you will depend not just on your circumstances, but also the data you are processing and the risks posed.
- You must assess your information security risk and implement appropriate technical controls.
- The Information Commissioner's Office and the National Cyber Security Centre (NCSC) have worked together to develop an approach that you can use when making this assessment.
- It allows you to consider common expectations and either follow existing guidance, use particular services or develop your own processes if you have appropriate knowledge and resources to do so.
- The approach is based on four aims:
  - managing security risk;
  - protecting personal data against cyber-attack;
  - detecting security events; and
  - minimising the impact.

In brief

What does the UK GDPR say about security?

The UK GDPR requires you to process personal data securely. Article 5(1)(f) concerns 'integrity and confidentiality' of personal data - in short, it is the GDPR's 'security principle'. It states that personal data shall be:

> ‘processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’

The aim of this guidance is to describe an overall set of outcomes that are considered ‘appropriate’ to prevent personal data being accidentally or deliberately compromised.

Further Reading

Relevant provisions in the UK GDPR - See Articles 5(1)(f) and Recital 39
External link

In more detail — ICO guidance

- Security

What are the other requirements?

Alongside the security principle, the UK GDPR contains other relevant requirements, including data protection by design in Article 25 and security of processing in Article 32.

Data protection by design requires you to put in place appropriate technical and organisational measures designed to implement the data protection principles effectively and integrate necessary safeguards into the processing. You have to do this at the time of the determination of the means of the processing (ie the design phase of any processing operation) and at the time of the processing itself.

You also have specific security obligations under Article 32 which apply whether you are a controller or a processor. These require you to put in place appropriate technical and organisational measures to ensure an appropriate level of security of both the processing and your processing environment.

These provisions cover fundamental information security concepts including:

- minimisation of personal data collected;
- managing, limiting and controlling access to personal data;
- protecting the classic ‘CIA triad’ (confidentiality, integrity, and availability) of personal data;
- resilience of processing systems and services, and the ability to restore availability and access to personal data; and
- regular testing of the effectiveness of measures implemented.

The measures you implement should be appropriate to the risk presented.

Further Reading

Relevant provisions in the UK GDPR See Articles 25 and 32, and Recitals 78 and 83

External link

In more detail — ICO guidance

- Data protection by design
- Security

How does security relate to the UK GDPR's accountability principle and our responsibility as data controllers?

The accountability principle requires you to be able to demonstrate that your processing is done in compliance with the UK GDPR. Accountability also has direct relevance to your responsibility as a data controller.

You are required to implement appropriate technical and organisational measures to ensure, and be able to demonstrate, that processing of personal data is performed in accordance with the UK GDPR.

Further Reading

Relevant provisions in the UK GDPR See Article 5(2) and 24, and Recital 74

External link

In more detail — ICO guidance

- Accountability and governance

What are 'appropriate technical and organisational measures'?

The UK GDPR requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing. This reflects both the UK GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security.

This means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.

This guidance sets out a set of security outcomes that could form the basis of describing 'appropriate technical and organisational measures' to protect personal data. Whilst there are minimum expectations, the precise implementation of any measures must be appropriate to the risks you face.

In more detail — ICO guidance

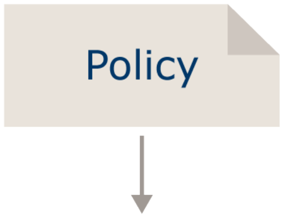
- Security

Why ‘security outcomes’?

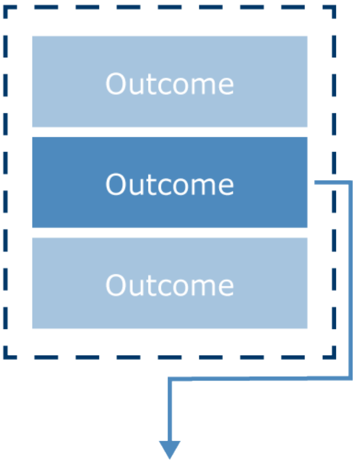
It may seem like there is a lot of confusion as to the technical security required to comply with your data protection obligations. There is lots of detailed guidance available, but it may not be immediately clear what you must put in place, what is simply a suggested approach and what is relevant to you and your circumstances.

The outcomes intend to provide a common set of expectations that you can meet, either through following existing guidance, using particular services or, if you are sufficiently competent, development of your own bespoke approach.

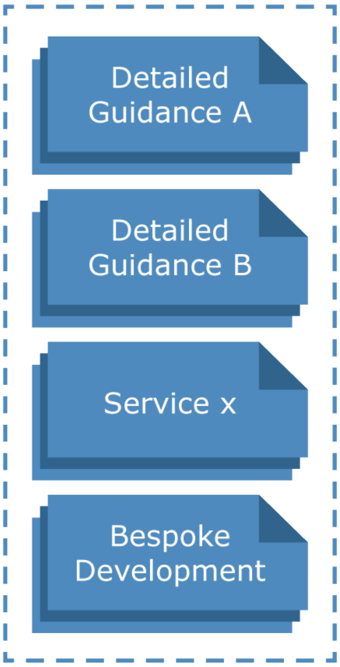
An outcomes-based approach also enables scaling to any size or complexity of organisation or data processing operation. The outcomes remain constant – it is how they are implemented that differs.



“…Implement appropriate technical and organisational measures…”



This is the abstract and outcome based view of what you must achieve.



Detailed guidance showing examples of how to achieve the outcomes or perhaps appropriate services may be available to procure, or alternatively a competent organisation might develop a bespoke approach.

What are the aims?

The approach has been developed in accordance with the following four aims:

- A) manage your security risk;
- B) protect personal data against cyber-attack,
- C) detect security events; and
- D) minimise the impact.

Each outcome is summarised under its respective aim, with specific reference to the data protection context following.

What are the outcomes?

A. Manage your security risk

You have appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to personal data.

A.1 Governance

You have appropriate data protection and information security policies and processes in place. If required, you ensure that you maintain records of processing activities and have appointed a Data Protection Officer.

In more detail — ICO guidance

The ICO has published guidance on data protection officers, accountability and governance, documentation and security.

In more detail—Article 29

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of EU version of the GDPR.

WP29 published guidelines on Data Protection Officers, which the EDPB endorsed in May 2018.

A.2 Risk management

You take appropriate steps to identify, assess and understand security risks to personal data and the systems that process this data.

The UK GDPR emphasises a risk-based approach to data protection and the security of your processing systems and services. You must take steps to assess these risks and include appropriate organisational measures to make effective risk-based decisions based upon:

- the state of the art (of technology);
- the cost of implementation;
- the nature, scope, context and purpose of processing; and
- the severity and likelihood of the risk(s).

Beyond this, where the processing is likely to result in a high risk to the rights and freedoms of individuals, you must also undertake a Data Protection Impact Assessment (DPIA) to determine the impact of the intended processing on the protection of personal data. The DPIA should consider the technical and organisational measures necessary to mitigate that risk. Where such measures do not reduce the risk to an acceptable level, you need to have a process in place to consult with the ICO before you start the processing.

In more detail — ICO guidance

- DPIAs

In more detail—Article 29

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of EU version of the GDPR.

WP29 produced guidelines on high risk processing and DPIAs, which the EDPB endorsed in May 2018.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Other resources

The NCSC has guidance on risk management for cyber security. Additionally, Step 1 of the 10 Steps to Cyber Security is about developing an information risk management regime.

A.3 Asset management

You understand and catalogue the personal data you process and can describe the purpose for processing it. You also understand the risks posed to individuals of any unauthorised or unlawful processing, accidental loss, destruction or damage to that data.

The personal data you process should be adequate, relevant and limited to what is necessary for the purpose of the processing, and it should not be kept for longer than is necessary.

A.4 Processors and the supply chain

You understand and manage security risks to your processing operations that may arise as a result of using third parties such as data processors. This includes ensuring that they employ appropriate security measures.

In the case of data processors, you are required to choose those that provide sufficient guarantees about their technical and organisational measures. The UK GDPR includes provisions where processors are used, including specific stipulations that must feature in your contract.

In more detail — ICO guidance

- Controllers and processors
- Contracts

Other resources

The NCSC has also published guidance on managing cyber risks in your supply chain.

B. Protect personal data against cyber-attack

You have proportionate security measures in place to protect against cyber-attack which cover:

- the personal data you process; and
- the systems that process such data.

B.1 Service protection policies and processes

You should define, implement, communicate and enforce appropriate policies and processes that direct your overall approach to securing systems involved in the processing of personal data.

You should also consider assessing your systems and implementing specific technical controls as laid out in appropriate frameworks (such as Cyber Essentials).

Other resources

Homepage of the Cyber Essentials schemes at the NCSC's website.

B.2 Identity and access control

You understand, document and manage access to personal data and systems that process this data. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed. You should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.

You should appropriately authenticate and authorise users (or any automated functions) that can access personal data. You should strongly authenticate users who have privileged access and consider two-factor or hardware authentication measures.

You should prevent users from downloading, transferring, altering or deleting personal data where there is no legitimate organisational reason to do so. You should appropriately constrain legitimate access and ensure there is an appropriate audit trail.

You should have a robust password policy which avoids users having weak passwords, such as those trivially guessable. You should change all default passwords and remove or suspend unused accounts.

B.3 Data security

You implement technical controls (such as appropriate encryption) to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest or accessing data that might remain in memory when technology is sent for repair or disposal.

B.4 System security

You implement appropriate technical and organisational measures to protect systems, technologies and digital services that process personal data from cyber-attack.

Whilst the UK GDPR requires a risk-based approach, typical examples of security measures you could take include:

- tracking and recording all assets that process personal data, including end user devices and removable media;
- minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity;
- actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching), and taking other mitigating steps, where patches can't be applied;
- managing end user devices (laptops and smartphones etc.) so that you can apply organisational controls over software or applications that interact with or access personal data;
- encrypting personal data at rest on devices (laptops, smartphones, removable media) that are not subject to strong physical controls;
- encrypting personal data when transmitted electronically;
- ensuring that web services are protected from common security vulnerabilities such as SQL injection and others described in widely-used publications such as the OWASP Top 10; and
- ensuring your processing environment remains secure throughout its lifecycle.

You also undertake regular testing to evaluate the effectiveness of your security measures, including virus and malware scanning, vulnerability scanning and penetration testing as appropriate. You record the results of any testing and remediating action plans.

Whatever security measures you put in place – whether these are your own, or whether you use a third party service such as a cloud provider – you remain responsible both for the processing itself, and also in respect of any devices that you operate.

Further reading — ICO guidance

- Security
- Encryption
- Passwords in online services

Under the 1998 Act, the ICO published a number of more detailed guidance pieces on different aspects of IT security. Where appropriate, we will be updating each of these to reflect the UK GDPR's requirements in due course. However, until that time they may still provide you with assistance or things to consider:

- IT security top tips – for further general information on IT security;
- IT asset disposal for organisations (pdf) – guidance to help organisations securely dispose of old computers and other IT equipment;
- A practical guide to IT security – ideal for the small business (pdf);
- Protecting personal data in online services – learning from the mistakes of others (pdf) – detailed technical guidance on common technical errors the ICO has seen in its casework;
- Bring your own device (BYOD) (pdf) – guidance for organisations who want to allow staff to use personal devices to process personal data; and
- Cloud computing (pdf) – guidance covering how security requirements apply to personal data

processed in the cloud.

Other resources

- The NCSC has detailed technical guidance (external link) in a number of areas that will be relevant to you whenever you process personal data. Some examples include:
- 10 Steps to Cyber Security (external link) - The 10 Steps define and communicate an Information Risk Management Regime which can provide protection against cyber-attacks.
- Guidance on cybersecurity for small businesses and for charities;
- Using passwords to protect your data;
- Penetration testing;
- Guidance on end-user device security; and
- Guidance on keeping your smartphones and tablets safe.

The OWASP Foundation maintains the OWASP Top 10.

The European Union Agency for Cybersecurity (ENISA) also has guidance on data protection and security, including a 'Handbook' on security of personal data and guidelines for SMEs.

B.5 Staff awareness and training

You give your staff appropriate support to help them manage personal data securely, including the technology they use. This includes relevant training and awareness as well as provision of the tools they need to effectively undertake their duties in ways that support the security of personal data.

Staff should be provided support so that they do not inadvertently process personal data (eg by sending it to the incorrect recipient).

Other resources

10 Steps to Cyber Security is about user education and awareness.

C. Detect security events

You can detect security events that affect the systems that process personal data and you monitor authorised user access to that data.

C.1 Security monitoring

You appropriately monitor the status of systems processing personal data and monitor user access to personal data, including anomalous user activity.

You record user access to personal data. Where unexpected events or indications of a personal data breach are detected, you have processes in place to act upon those events as necessary in an appropriate timeframe.

Other resources

10 Steps to Cyber Security is about monitoring.

D. Minimise the impact

You can:

- minimise the impact of a personal data breach;
- restore your systems and services;
- manage the incident appropriately; and
- learn lessons for the future.

D.1 Response and recovery planning

You have well-defined and tested incident management processes in place in case of personal data breaches. You have mitigation processes in place that are designed to contain or limit the range of personal data that could be compromised following a personal data breach.

Where the loss of availability of personal data could cause harm, you have measures in place to ensure appropriate recovery. This should include maintaining (and securing) appropriate backups.

Other resources

NCSC guidance on backing up your data.

D.2 Improvements

When a personal data breach occurs, you take steps to:

- understand the root cause;
- report the breach to the ICO and, where appropriate, affected individuals;
- where appropriate (or required), report to other relevant bodies (for example, other regulators, the NCSC and/or law enforcement); and
- take appropriate remediating action.

Further reading – ICO guidance

- Personal data breaches

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of EU version of the GDPR.

WP29 published guidelines on personal data breach notification, which the EDPB endorsed in May 2018.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Other resources

- Report a security breach to the ICO
- 10 Steps to Cyber Security - incident management