Security

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?
- Why should we worry about information security?
- What do we need to protect with our security measures?
- What level of security is required?
- What organisational measures do we need to consider?
- What technical measures do we need to consider?
- What if we operate in a sector that has its own security requirements?
- What do we do when a data processor is involved?
- Should we use pseudonymisation and encryption?
- What are 'confidentiality, integrity, availability' and 'resilience'?
- What are the requirements for restoring availability and access to personal data?
- Are we required to ensure our security measures are effective?
- What about codes of conduct and certification?
- What about our staff?

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