Seventh Data Protection Principle - Security – integrity and confidentiality

At a glance

- A key principle of the DPA is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security – integrity and confidentiality principle'.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- The security requirements 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 pseudonymization and encryption.
- Your measures should ensure the 'confidentiality, integrity and availability' of the personal data you process.
- You should ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.

Checklist

- 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.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- We use encryption and/or pseudonymization 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 up to date, and act on the results of those tests where they highlight areas for improvement.
- We ensure that any data processor we use also implements appropriate technical and organisational security measures.

In brief

What is the 'security – integrity and confidentiality principle'?

The seventh data protection principle says:

> Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

There are different aspects to this principle, including:

- Organisational measures e.g. staff training and policy development;
- Technical measures e.g. physical protection of data, pseudonymization, encryption;
- Securing ongoing availability, integrity and accessibility, e.g. by ensuring backups.

Why should you 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 or informers 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 recognize that individuals are also 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 DPA and other Acts you may be subject to.

The Ombudsman will consider the technical and organisational measures you had in place when considering an administrative fine.

What do your security measures need to protect?

The security – integrity and confidentiality principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just IT security. 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 to those who have a legitimate need to access and use it, i.e. if personal data is accidentally lost, altered or destroyed, you should be able to recover it

These measures should ensure 'confidentiality, integrity and availability'. Under the DPA they constitute best practice.

What level of security is required?

The DPA does not define the security measures that you should have in place. The Act 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 the DPA'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 and the individuals whose data you process.

For a small business this may mean little more than ensuring that the office and filing cabinet are locked and staff are aware of the personal and confidential nature of the information that is held. In larger organisations, or businesses that process personal data with higher levels of risk (e.g. health data), this may involve more complex organisational and technical measures.

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.

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 you need to consider?

Carrying out an information risk assessment is one example of an organisational measure, but you may 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 Head of a medium-sized organisation asks the Resources Manager 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 over time.

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 the size of your

organisation, 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 – integrity and confidentiality 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 (e.g. how to decommission and dispose of any IT equipment that may contain personal data);
- access to premises or equipment given to anyone outside your organisation (e.g. 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 in case of an emergency; and
- periodic monitoring to ensure that your security measures remain appropriate and up to date.

What technical measures do you need to consider?

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. While these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the inappropriate disposal of old computers, or hard-copy (paper) 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, particularly those which process personal data;
- data security – the security of the data you hold within your systems, e.g. ensuring appropriate access controls are in place and that data is held securely;
- online security – e.g. 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 may also be that you do 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 also 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.

What if you 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 DPA's security – integrity and confidentiality principle, the Ombudsman will nevertheless consider these carefully in any considerations of regulatory enforcement action.

Example

If you are processing payment card data, you may be 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 DPA's security – integrity and confidentiality principle, if you process card data and suffer a personal data breach, the Ombudsman 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 you do about security when a data processor is involved?

If an organisation processes personal data on your behalf, then it is a data processor under the DPA. A common example in the Cayman Islands financial services context will be where a mutual fund engages an administrator. Your own employees are not considered data processors under the DPA.

This can cause security problems – as a data controller you are responsible for ensuring compliance with the DPA and this includes what the data processor does with the data. However, in addition to this, the DPA's security requirements also apply to any data processor you use.

This means that:

- you must choose a data processor that provides sufficient guarantees about its technical and organisational security measures. Conducting appropriate due diligence as part of supply chain management is good practice, and may also be required by e.g. CIMA guidance;
- you must have a written contract (a "data processing agreement") that stipulates that the data processor acts only on instructions from yourself (the data controller), and that the data processor must undertake the same security measures that you would have to take if you were doing the processing yourself; and
- depending on the nature of the processing and the risk posed by the data processor, you may consider including in the data processing agreement provisions that require the data processor to provide you with appropriate information and assistance to help you comply with the DPA (e.g. in relation to any audit or investigation the Ombudsman may perform in relation to your organisation). This may also include, where appropriate, allowing you to audit and inspect the data processor to make sure they are in compliance with the contract and their obligations under the Act.

At the same time, your data 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 data processor that has these resources can assist you in making sure personal data is processed securely, provided that your contractual arrangements are appropriate.

Should you use pseudonymization and encryption?

Pseudonymization and encryption are two examples of measures that may be appropriate for you to implement. This does not mean that you are obliged to use these measures. Whether you do will depend 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 encryption has been widely used as an appropriate technical protection measure given its widespread availability and relatively low cost of implementation. The DPA does not change this. 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.

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 there can be serious consequences, both for you as a data controller, and for the individuals whose personal 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 the ability of your IT systems to resist or withstand adverse incidents. Again, there is a wide range of solutions available here, and what is appropriate for you depends on your circumstances.

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

Having appropriate organisational and technological security measures includes having the ability to restore the availability of, and access to, personal data in the event of a physical or technical incident in a 'timely manner'.

The DPA does not provide details on this, and the applicability of this rule will depend on the context and in particular:

- the nature of your organisation and processing purposes, including the risk for individuals if the personal data you process is unavailable for a period of time;
- the type of systems used.

The key point is that you should take these elements 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 for individuals and would constitute a personal data breach under the DPA.

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 while there will be some disruption to the service, the organisation is nevertheless able to comply with this requirement of the DPA.

Are you required to ensure your security measures are effective?

The DPA does not explicitly require you to have a process for regularly testing, assessing, and evaluating the effectiveness of any security measures you put in place. However, having such a process constitutes best practice and will be considered when you are under investigation by the Ombudsman.

What these tests look like, and how regularly you do them, will depend on your own circumstances. However, 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 for cybersecurity 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. There are equivalent tests for physical and operational security.

In some industries, you may be required to undertake tests of security measures on a regular basis. While the DPA does not make this an obligation, testing your security measures is considered best practice, depending on the nature of 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.

What about codes of practice?

If your security measures include a product or service that adheres to a code of practice (once any have been approved), you may be able to use this as an element to demonstrate your compliance with the security – integrity and security principle. It is important that you check carefully that the code is appropriately issued in accordance with section 42 of the DPA.

Apart from any codes of practice, the Ombudsman may, with your consent, assess your processing of personal data for adherence to good practice.

What about your staff?

It is 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, addressing specific security risks which are relevant to your organisation and taking into account the nature and scope of processing your organisation undertakes. Examples of training topics you could consider covering in your training program include:

- your responsibilities as a data controller under the DPA;
- 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 (e.g. by pretending to be the individual whom the data concerns, or enabling staff to recognize '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 (e.g. to avoid virus infection or spam).

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

Relevant provisions

Data Protection Act (2021 Revision):

Schedule 1, part 1, paragraph 7: Seventh data protection principle – Security – integrity and security

Schedule 1, part 2, paragraph 3: Processing contract to ensure reliability

Section 42: Codes of practice

Further guidance

ICO:

IT security top tips: https://ico.org.uk/for-organisations/guide-to-data-protection/it-security-top-tips/

IT asset disposal for organisations: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

A practical guide to IT security. Ideal for the small business: https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

Protecting personal data in online services: learning from the mistakes of others: https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf

Bring your own device: https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

Cloud computing: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

Encryption: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/

National Cyber Security Centre:

Technical guidance: https://www.ncsc.gov.uk/guidance

UK government:

Cyberaware: https://www.cyberaware.gov.uk/

Advice for small businesses: https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know

Data protection guidance of the European Union Agency for Network and Information Security (ENISA): https://www.enisa.europa.eu/topics/data-protection

ICO and NCSC:

Guidance on security Outcomes: https://ico.org.uk/for-organisations/security-outcomes/

Article 29 Working Party:

Guidelines on personal data breach notification: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052