Security obligations under the GDPR

Although the security of personal data has been a legal obligation for data controllers under the Data Protection Act 1998, the GDPR reinforces the existing provisions and also extends this responsibility directly to those individuals who actually process the data.

Security of data processing

The GDPR requires personal data to be processed in a manner that ensures its security. This is commonly known as the GDPR's 'security principle'.

The security principle means that you must take measures 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.

The GDPR requires organisations to secure information assess risk and put appropriate security measures in place.

What do security measures need to protect?

The security of personal data 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 so that 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'. The controller and processor must also take steps to ensure that any person acting under their authority and having access to personal data, does not process the data except on instructions from the controller (unless otherwise required by law).

What level of security is required?

The GDPR requires you to have 'appropriate' security measures in place.

The GDPR does not dictate which security measures you should have in place as no 'one size fits all'.

What's 'appropriate' depends on your individual circumstances, the processing you're undertaking and the risks presented by the processing. When deciding which security measures are 'appropriate' you will also take into account the costs of implementation and the nature, scope, context and purpose of your processing.

GDPR relates the risk to the measures taken in order to protect the rights and freedoms of individuals about whom the information relates.

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: for example, an external organisation who processes personal data (such as pupil photographs) on your behalf. (We shall be providing you with guidance on data processors acting on your behalf in a future bulletin).

What security measures need to be considered?

'Appropriate' technical and organisational security measures for the protection of personal data should be implemented to ensure data security.

- **Organisational measures –** Examples include carrying out an information risk assessment; encouraging and creating a culture of security awareness; introducing an information security policy which demonstrates the steps you take to ensure data security; ensuring premises or equipment are protected against unauthorised access; having arrangements in place to protect and recover personal data you hold; and carrying out periodical checks to ensure security measures are appropriate and up to date.
- **Technical measures –**These include both physical and IT/computer security. Examples of physical security include: door locks in areas where personal data is stored; protecting your premises by alarms, security lighting or CCTV; procedures you have in place to ensure IT equipment is secure; and how you dispose of paper and electronic waste (i.e. old computers). Examples of IT/computer security include: taking steps to ensure your network and systems are secure; having access controls in place on your network and systems; ensuring IT/computer devices are secure (i.e. USB sticks and laptops).

Whatever you do, you should remember the following: your security measures need to be appropriate to the size and use of your network and information systems; you should 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.

Pseudonymisation and encryption

The GDPR provides specific suggestions for what types of security measures might be considered “appropriate to the risk”. These include the pseudonymisation and encryption of personal data.

Pseudonymisation (removing personal identifiers) and encryption (encoding it – by use of password protection, for example) are recommended by the ICO as tools for safeguarding information. However both of these can be implemented at relatively low cost and with minimal difficulty. The ICO has for a number of years considered encryption to be an appropriate technical measure – this position has not altered under the GDPR.

‘Confidentiality, integrity and availability’

These 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.

What about your staff?

You are required to take steps to ensure that any person acting under your authority with access to personal data, does not process the data except as you have instructed them to do so (unless otherwise required by law).

It’s therefore important 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:

●responsibilities under the GDPR;

●staff responsibilities for protecting personal data; and

●any restrictions you place on the personal use of your systems by staff (e.g. to avoid virus infection or spam).

We will be providing materials to help you do this.

Are your security measures effective?

You should have a process for regularly testing, assessing and evaluating the effectiveness of any security measures you put in place.

It does not specify the type of testing which should be carried out or how regularly the testing should occur. These will depend on your organisation and the personal data you are processing.

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.