Encryption

In more detail

- What is encryption?
- Encryption in practice
- If we encrypt personal data, does this count as processing?
- What are the other considerations?
- When should we use encryption?

What is encryption?

Encryption is a mathematical function using a secret value—the key—which encodes data so that only users with access to that key can read the information.

In many cases encryption can provide an appropriate safeguard against the unauthorised or unlawful processing of personal data, especially in cases where it is not possible to implement alternative measures.

Example

An organisation issues laptops to employees for remote working together with secure storage lockers for use at home and locking devices for use outside the home. However, there is still the risk of loss or theft of the devices (e.g. whilst being used outside of the office).

To address this risk, the organisation requires all data stored on laptops to be encrypted. This significantly reduces the chance of unauthorised or unlawful processing of the data in the event of loss or theft.

Encryption in practice

Information is encrypted and decrypted using a secret key. (Some algorithms use a different key for encryption and decryption). Without the key the information cannot be accessed and is therefore protected from
unauthorised or unlawful processing.

Whilst it is possible to attempt decryption without the key (e.g., by trying every possible key in turn), in practical terms it will take such a long time to find the right key—i.e., many millions of years, depending on the computing power available and the type of key—that it becomes effectively impossible. However, as computing power increases, the length of time taken to try a large number of keys will reduce so it is important that you keep algorithms and key sizes under consideration, normally by establishing a review period.

You should consider encryption alongside a range of other technical and organisational security measures. You also need to ensure that your use of encryption is effective against the risks you are trying to address, as it cannot be used in every processing operation.

Therefore, you should consider the benefits that encryption will offer in the context of your processing, as well as the residual risks. You should also consider whether there are other security measures that may be appropriate to put in place, either instead of encryption or alongside it.

You can do this by means of a Data Protection Impact Assessment (DPIA), which, depending on your processing activities, you may be required to undertake under Article 35 of the GDPR. In any case, a DPIA will also help you to assess your processing, document any decisions and the reasons for them, and can ensure that you are only using the minimum personal data necessary for the purpose.

**In more detail – ICO guidance**

We have published guidance on data protection impact assessments in the Guide to the GDPR.

We have produced further detailed guidance on DPIAs, including a list of processing operations that require a DPIA as well as a template (DOCX) that
In more detail – European Data Protection Board (EDPB)

The EDPB, formerly the Article 29 Working Party, includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

In October 2017, Article 29 published guidelines on DPIAs and high-risk processing under the GDPR (WP248rev01). The EDPB formally endorsed these guidelines on 25 May 2018.

If we encrypt personal data, does this count as processing?

Yes. Article 4(2) of the GDPR defines ‘processing’ as any operation or set of operations performed on personal data, including ‘adaptation or alteration’.

The process of converting personal data from plaintext into ciphertext represents ‘adaptation or alteration’ of that data.

Whether you are a controller or a processor, if you have encrypted personal data yourself and are responsible for managing the key then you will still be processing data covered by the GDPR.

If you also subsequently store, retrieve, consult or otherwise use that encrypted data, you will also be processing data covered by the GDPR.

You should therefore ensure that you do not view the use of encryption as an anonymisation technique or think the encrypted data is not subject to the GDPR. If you were responsible for encrypting the data and are the holder of the key, you have the ability to re-identify individuals through decryption of that dataset.
In this respect, encryption can be regarded as a pseudonymisation technique. It is a security practice designed to safeguard personal data.

**What are the other considerations?**

You should not underestimate the importance of good key management - make sure that you keep the keys secret in order for encryption to be effective.

Encryption can take many different forms. Whilst it is not the intention to review each of these in turn, it is important to recognise when and where encryption can provide protection to certain types of data processing activities. Later in this guidance, we outline a number of scenarios where encryption may be beneficial to you.

Encryption is also governed by laws and regulations, which may differ by country. For example, in the UK you may be required to provide access to the key in the event you receive a court order to do so.

Finally, not all processing activities can be completely protected from end to end using encryption. This is because at present information needs to exist in a plaintext form whilst being ‘actively processed’. For example, data contained within a spreadsheet can be stored in an encrypted format but in order for the spreadsheet software to open it and the user to analyse it, that data must first be decrypted. The same is true for information sent over the internet – it can be encrypted whilst it is in transit but must be decrypted in order for the recipient to read the information.

**When should we use encryption?**

When processing data, there are a number of areas that can benefit from the use of encryption. You should assess the benefits and risks of using encryption at these different points in the processing lifecycle separately. When first considering your processing, you should also ensure that you adopt a data protection by design approach, and using encryption can be
one example of the measures that you put in place as part of this approach.

The two main purposes for which you should consider using encryption are data storage and data transfer. These two activities can also be referred to as data at rest and data in transit.

**Recommendation**

You should have a policy governing the use of encryption, including guidelines that enable staff to understand when they should and should not use it.

For example, there may be a guideline stating that any email containing sensitive personal data (either in the body or within an attachment) should be sent encrypted or that all mobile devices should be encrypted and secured with a password complying with a specific format.

You should also be aware of any industry or sector-specific guidelines that may include a minimum standard or recommend a specific policy for encrypting personal data. Examples include:

- NHS Digital’s [encryption guidance for health and social care organisations](#);
- the General Council of the Bar’s [guidance on information security](#) (PDF), which includes a section on encryption;
- the Attorney General’s guidance on information security, which includes a section on the [storage and handling of electronic material](#); and
- Requirements 3 and 4 of the [Payment Card Industry Data Security Standard](#) (PCI-DSS) cover the protection of cardholder data in storage and in transit. If encryption is used as part of the measures, there are specific considerations detailed in each of the Requirements.