Encryption

This guidance discusses encryption in more detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding to help you apply encryption in practice. It is aimed at DPOs and those with specific data protection responsibilities in larger organisations.

If you haven't read the 'in brief' page on encryption in the Guide to Data Protection, you should read that first. It introduces this topic and sets out the key points you need to know, along with practical checklists to help you comply.

This guidance will help you to understand the importance of encryption as an appropriate technical measure to protect the personal data you hold. Whether you are a controller or a processor, encryption is a technique that you can use to protect personal data.

The guidance outlines the concept of encryption in the context of the UK GDPR's integrity and confidentiality principle, and particularly Article 32 on security processing. It provides a summary of current forms of encryption and the considerations you should have when putting it in place, along with outlining the residual risks. Finally, it provides a number of scenarios where personal data is processed, outlining how encryption can be used to safeguard such data in respect of each scenario, and detailing some of the risks that remain.

This guidance also includes several recommendations, namely that where you are storing or transmitting personal data, you should use encryption due to its widespread availability and relatively low cost of deployment

What's required under the UK GDPR

In detail

What does the UK GDPR say about encryption?

Article 5(1)(f) of the GDPR 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 'security principle' for short. Although the security principle does not define the meaning of 'appropriate', the UK GDPR has 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, including inter alia as appropriate:
>
> (a) pseudonymisation and **encryption** of personal data'

This means that you can consider the state of technological developments and costs involved when assessing what security measures to implement. However, as encryption is an established, well-understood and widely-deployed technology that is available in a large number of solutions and can be implemented relatively easily, it is likely that in many cases it will form part of the technical measures you look to put in place.

Are we required to encrypt personal data?

The UK GDPR includes encryption as an example of a technical measure that can be appropriate to protect the personal data you hold. Ultimately, whether or not encryption is the right measure to put in place depends on your circumstances—the sort of processing

you are undertaking, the risks that may be posed to individuals' rights and freedoms, and the state of the art of technology available to you to protect that data.

Recital 83 of the UK GDPR says:

> 'In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.'

This is not a new approach. The Information Commissioner has seen numerous incidents where personal data has been lost, stolen, or subject to unauthorised access. Many of these cases involved data being inadequately protected, or the devices the data was stored on being left in inappropriate places – and sometimes both.

Where such losses occur, and where encryption has not been used to protect the data, it is possible that regulatory action may be pursued. This is particularly the case given the widespread availability of encryption solutions, and the ease with which you can deploy them in your organisation.

Relevant provisions in the UK GDPR - See Articles 5(1)(f) and 32 and Recital 39 and 83

External link

Further reading

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

What is encryption?

In more detail

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 (eg 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 (eg, by trying every possible key in turn), in practical terms it will take such a long time to find the right key—ie 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 UK 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.

Further reading

Data protection impact assessments

Accountability

Documentation

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

Yes. Article 4(2) of the UK 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 UK GDPR.

If you also subsequently store, retrieve, consult or otherwise use that encrypted data, you will also be processing data covered by the UK 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 UK 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 measure designed to protect 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 an encryption 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 in general 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.

Developments in the state of the art may eventually enable computation of encrypted data more widely. This may change some of the considerations you need to have regarding encryption. Irrespective of this, the security requirements mean you need to keep your encryption solution under regular review, including taking account of the state of the art (see 'How should we implement encryption?').

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:

- 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.

Encryption and data storage

In more detail

What is the benefit of encrypting the data that we store?

Encrypting data whilst it is being stored (eg on a laptop, mobile, USB or back-up media, databases and file servers) provides effective protection against unauthorised or unlawful processing. It is especially effective to protect data against unauthorised access if the device storing the encrypted data is lost or stolen.

Depending on the circumstances, an effective and appropriate encryption solution can also be a means of demonstrating compliance with the security requirements of the UK GDPR. The ICO considers encryption to be an 'appropriate technical measure', and in cases where data is lost or unlawfully accessed and encryption was not used, we may consider regulatory action.

Example

A civil monetary penalty of £150,000 was served on Greater Manchester Police under the Data Protection Act 1998 ('the 1998 Act') after a USB stick containing data on police operations was stolen from an officer's home. The stick contained personal data of over 1,000 people with links to serious organised crime investigations going back over an 11 year period. It was unencrypted and had no password protection.

An investigation established that an officer had used the device to copy information from his personal folder on the force's network in order to access the data from outside the office. It was subsequently discovered that a number of other officers were also using unencrypted memory sticks on a regular basis.

Greater Manchester Police failed to implement appropriate technical measures against the loss of personal data. Although there was an order requiring the use of encrypted memory sticks, it was not enforced and no steps were taken to restrict the downloading of files onto external devices.

Encryption can also benefit you in other ways. If you do suffer a personal data breach, the acquisition of an encrypted dataset by an attacker still requires notification to the ICO under Article 33 of the UK GDPR.

However, Article 34(3)(a) states that notification to individuals is not required where you have:

> 'implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption'

There is still a requirement for you to be able to demonstrate that the data was appropriately encrypted. Therefore, you need to assess whether this was the case and document your decision not to notify. You should also provide this information to the ICO when you notify us.

We will use this to assess whether:

- the breach is likely to result in a high risk to those individuals, in which case we may direct you to notify them, or
- your security measures have rendered the data unintelligible and therefore notification is not required.

What is 'full disk encryption'?

This involves encrypting the entire contents of a device's disk. Most modern operating systems have full disk encryption built in, although in some cases you may need to ensure you are using a device with specific hardware.

With full disk encryption, the data is decrypted only when the user accesses the device. Unfortunately, full disk encryption may not be enabled by default. You may need to activate it, for example by accessing the relevant settings options within the operating system of your device(s) and following the resulting instructions. Alternatively it may be an option that is available when you install the operating system.

> **Examples**
>
> Although the ICO does not endorse nor recommend any one particular encryption solution, there are a number of modern operating systems that feature full-disk encryption as a feature. This list is not exhaustive and there may be other

solutions that apply depending on your circumstances. The key is to ensure that the encryption adheres to accepted standards (see the section on 'How should we implement encryption?').

The Windows operating system includes a feature known as Bitlocker Drive Encryption which encrypts all user files and system files on the drive. For more information on Bitlocker, including additional considerations in respect of hardware, you can consult the 'Information Protection' section of the Windows IT Pro Center' (external link).

macOS includes the FileVault feature which encrypts the startup disk. For more information on this feature you can read the FileVault section on Apple's support site (external link). You should however note that full disk encryption is only possible with FileVault 2.

A number of operating systems based on GNU/Linux also include disk encryption features. If you are using Linux, we advise you to consult the online documentation of your particular distribution for more information. Disk encryption solutions are also available on BSD-derived operating systems.

Other third party solutions may also apply depending on your circumstances.

It is possible that you may consider setting a PIN or requiring users to provide a username/password in order to access a device provides sufficient protection. Whilst this can offer assurance that the user is authorised to perform certain functions, this approach offers little protection to the underlying data which is commonly stored in plaintext on the disk. This method must not be considered as equivalent to encryption. The data can also be easily accessed by an attacker with physical access to the device.

Passwords used to decrypt the hard disk or for access control must be sufficiently complex in order to provide an appropriate level of protection (see section Keeping the key secure)

What is individual file encryption?

Alternatively, you can encrypt files individually, or place groups of files within encrypted containers. In the event of loss or theft of the device an attacker might gain access to the device and to some data but not to the encrypted files—assuming the key remains secure.

The ability to create encrypted containers may be part of encryption or other archive software or be built-in to the operating system. Once a container is created, files can be placed within it and encrypted and the container itself can be moved and/or copied.

What about application or database encryption?

Some software applications and databases can also be configured to store data in an encrypted form. The benefit here is that the application controls the encryption, so it can access the keys when needed without relying on the underlying IT infrastructure.

When data is shared between applications then processes are required to share keys securely.

What are the residual risks with encrypted data storage?

You should recognise that there are occasions where data can still be accessed by an unauthorised person, even if a system uses encrypted data storage. For example:

- if an encrypted device is left unattended whilst a user is logged in, then an attacker can gain access to the decrypted material;
- devices that store data in encrypted volumes or containers must mount or open these containers in order for the data to be accessed. If the volumes are not closed or unmounted once the user has finished, the data may be accessible to others;
- if a device is infected with malware which has appropriate permissions to access the data, full disk encryption or use of secure containers will offer little protection once a user has decrypted the data;
- if applications on the device are compromised by an attacker then any data which can be accessed by the application is vulnerable. For example, successful exploitation of a website vulnerable to an SQL injection attack could expose data whether or not the device itself is encrypted; and
- APIs which permit web content to read and write files on the underlying file system may pose additional security considerations.

Addressing these types of risks is therefore an important part of an encryption policy, which should also include employee awareness training.

> **Recommendation**
>
> Personal data should be stored in an encrypted form to protect against unauthorised access or processing, especially if the loss of the personal data is reasonably likely to occur and would cause damage or distress to individuals.

Encryption and data transfer

In more detail

Why is it important to consider encrypted data transfer?

Encrypting personal data whilst it is being transferred from one device to another (eg across the internet or over wired or wireless connections) provides effective protection against interception of the communication by a third party whilst the data is in transfer.

It is also strongly recommended to use encrypted communication when transmitting any data over a wireless communication network (eg Wi-Fi) or when the data will pass through an untrusted network.

Data can be transformed into an encrypted format (see individual file encryption) and transferred over a non-secure communication channel yet still remain protected. An example would be sending an appropriately encrypted attachment via email.

However, use of secure communication methods such as Transport Layer Security (TLS) or a Virtual Private Network (VPN) will provide assurance that the content of the communication cannot be understood if intercepted provided the method is implemented correctly.

It is important to remember that without additional encryption methods in place (such as encrypted data storage) the data will only be encrypted whilst in transit and will be stored on the recipient's system in the same form as it is stored on the data controller's system (ie in plaintext).

Example

An organisation intends to use a cloud-based data storage service as a repository to archive data.

Data transfer

The organisation uses TLS to encrypt data whilst in transit so that it cannot be intercepted.

Data storage

The organisation recognises that TLS will only provide appropriate protection whilst the data is in transit. Once the cloud provider receives the data, it would normally exist in a decrypted state. Therefore the organisation encrypts each file on its system prior to upload. The cloud provider, or other third-party, is therefore unable to gain access to the personal data whilst it is stored in the cloud.

What is HTTPS?

'Hypertext Transport Protocol Secure' or HTTPS is a method for encrypting the content of a webpage between your servers and the user's browser and protecting user input on your website and/or mobile applications.

While the primary purpose of using HTTPS is to encrypt and protect all traffic between a user and a website, it can have other benefits such as verifying the identity of the website, and ensuring that a user can trust the whole website. These additional benefits are not the focus of this guidance, however, and are dependent on the type of certificate you use and whether you apply HTTPS across your entire site.

What's the difference between HTTPS, TLS and SSL?

TLS and SSL are often used interchangeably to refer to the same concept – the creation of an encrypted communications channel. Essentially, TLS is the 'successor' to SSL and uses more modern cryptographic protocols. HTTPS is a combination of HTTP with TLS to provide encrypted communication with, and secure identification of, web servers.

When implementing HTTPS on your site or within your app, you will have a choice of what protocols and cipher suites your server will support. These choices are important, as the use of an outdated protocol or an insecure cipher suite can compromise the protection HTTPS offers.

In terms of protocols, you should not support any versions of SSL, and you should ensure that your configuration is not susceptible to downgrade attacks. All versions of SSL suffer from a number of well-known vulnerabilities and should not be supported under any circumstances for a public-facing HTTPS implementation.

You also need to carefully consider the cipher suites that your server will support. Guidance from the National Institute of Standards and Technology (NIST) provides a list of approved

suites and also recommends that all cryptography provides at least 112 bits of security. The use of cryptographically broken ciphers such as RC4 is specifically prohibited, and you should avoid their use wherever possible.

Other resources

NIST Special Publication 800-52 Revision 2 – Guidance for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations (external link to PDF).

Historically, there has been an issue with browsers not supporting the latest TLS protocols. However, browser support for TLS 1.2 is now almost universal, as the chart below demonstrates, and as such you should only use previous versions where there are very specific needs.

Figure 1: : Browser support for TLS 1.2 as of November 2020. Source: Can I Use.

You should also ensure that you have documented the potential risks in using an older scheme, as well as the mitigations you have put in place to protect user data.

It should also be noted that TLS 1.3 was approved by the Internet Engineering Task Force (IETF) in March 2018. TLS 1.3 provides a number of improvements over TLS 1.2 and its approval enables the wider implementation of the protocol in software products and browsers. Although TLS 1.2 still provides a high standard of protection you should nevertheless ensure that, if or when required, you are able to support TLS 1.3 in the future.

Where should we use HTTPS on our site?

There are a number of factors to consider when implementing HTTPS on your website. You should have HTTPS across your entire site, although there are circumstances that can make this difficult – mixed origin content being the biggest issue that many sites will encounter. You must ensure that at the very least all pages with user input are protected, and if you are not using HTTPS across your entire site you should ensure that you are not leaking any sensitive information – for example, in referral headers or through failing to use secure cookies. You should also have mitigations against an attacker being able to hijack unprotected pages to redirect users to malicious pages.

Using HTTPS across your entire site is a much better solution as it prevents your non-HTTPS pages from being hijacked to point to malicious links. If you ensure that you redirect all HTTP traffic to HTTPS only, you can then also utilise HSTS (HTTP Strict Transport Security) which provides additional protections against man in the middle attacks.

If you are using a content distribution network or a reverse proxy you need to make sure you have considered where the HTTPS scheme ends, as this could leave user data still being transmitted in an unprotected form.

How can we test if our HTTPS implementation is appropriate?

You do not necessarily need to undertake an external penetration test to check the effectiveness of your HTTPS implementation. There are a number of publicly-available online testing services that you can use to do this. These services function by performing a test of a web server once a particular web address is entered.

A low rating on any of these does not automatically mean that you are not complying with the security principle; however, it is a fairly strong indication you need to review your security measures and make appropriate improvements.

What are the residual risks with encrypted data transfer?

You should recognise that even if a system uses encrypted data transfer there are still occasions where data can be subject to unauthorised access. As with data storage, is important to be aware of these residual risks and address these as part of an encryption policy which should also include employee awareness training. Some examples include:

- certain data relating to the communication may still be exposed (eg metadata or DNS queries) in an unencrypted form; and
- implementations relying on public-key infrastructure must implement strict certificate checking to maintain trust in end-points.

Recommendation

When transmitting personal data over the internet, particularly sensitive personal data, you should use an appropriate encrypted communications protocol (eg TLS versions 1.2 or above).

This also applies when transmitting any data over a wireless communication network (eg Wi-Fi), or when the data will pass through an untrusted network. Many web hosts will also offer options to add TLS to existing websites.

Other resources

The NCSC has produced guidance on TLS, IPsec and VPNs:

- Using TLS to protect data
- Using IPsec to protect data
- End user devices: VPNs

What types of encryption are there?

In more detail

What types of encryption are there?

There are two types of encryption in widespread use today: **symmetric** and **asymmetric** encryption. The name derives from whether or not the same key is used for encryption and decryption.

What is symmetric encryption?

In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient.

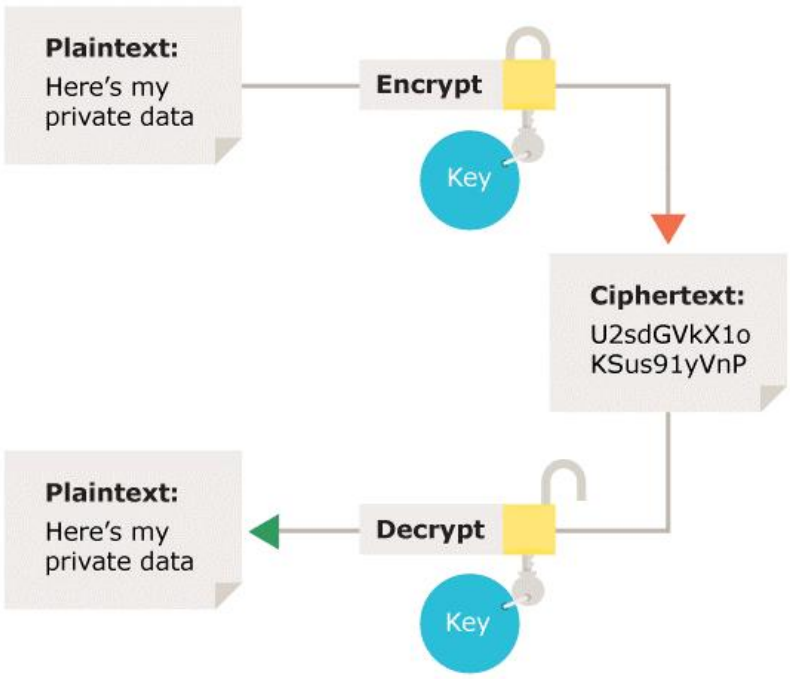

Figure 2: Symmetric encryption – Using the same key for encryption and decryption

What is asymmetric encryption?

Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key

and the other is known as the public key.

The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large.
Data encrypted with the recipient's public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised or unlawful access to the data.

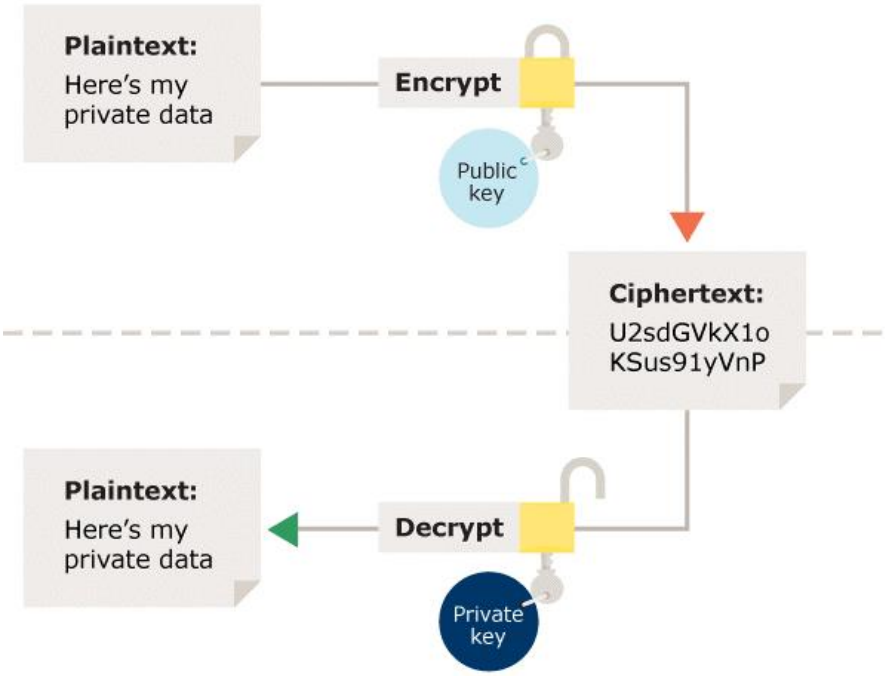

Figure 3: Asymmetric encryption – Using a different key for the encryption and decryption process

What about hashing?

Hashing is a technique that generates a fixed length value summarising a file or message contents. It is often incorrectly referred to as an encryption method.

Hash functions are used with cryptography to provide digital signatures and integrity controls but as no secret key is used it does not make the message private as the hash can be recreated.

Further reading

Passwords in online services

How should we implement encryption?

In detail

Choose the right algorithm

An encryption algorithm is a mathematical function that transforms plaintext into ciphertext. Choosing the right algorithm is important because vulnerabilities may be discovered over time, or advances in computing processing power may mean that a brute-force attack (ie attempting every possible key) is no longer a time-consuming task.

Example

The 'Data Encryption Standard' or DES was developed in the 1970s and standardised as a 'Federal Information Processing Standard' in 1977 (FIPS 46). It had a total of 72 quadrillion possible keys.

By the late 1990s, computing power had advanced to the point that it was possible to 'crack' a DES key in less than 24 hours by conducting a brute-force search of all possible keys.

The Advanced Encryption Standard (AES) was subsequently published as a replacement for DES as FIPS 197. AES with a 256-bit key size has a potential 115 quattuorvigintillion possible keys, or 115 with 78 digits following it. There is presently no known practical attack that could brute-force an AES 256 key.

You should therefore regularly assess whether your encryption method remains appropriate.

Rather than develop a custom algorithm it is recommended that you use a trusted and verified algorithm. Accredited products can provide an assurance of suitability and also permit you to demonstrate a level of compliance with legal obligations. However, it is important to keep the products being used under regular review, due to the nature of technical development over time.

Choose the right key size

Algorithms use keys to encrypt and decrypt data. Encrypting the same data with a different key will produce a different result. Just as it is important to choose the right algorithm, it is also important to ensure that the key size is sufficiently large to defend against an attack over the lifetime of the data. As computing processing power increases or new mathematical attack methods are discovered, a key must remain sufficiently large to ensure that an attack remains a practical impossibility.

Example

The RSA algorithm is one of the first public-key systems and is used for secure data transmission. It has a potential maximum key size of 4096-bits.

For a number of years, key sizes of 1024-bits were commonplace. However, in 2007, the National Institute of Standards and Technology recommended increasing minimum key size due to advances in computing power. The minimum recommended was 2048-bits up to the year 2030, and 3072-bits after 2030.

This required some certificate providers to increase the key size of their certificates to take account of the recommendation. In other cases, operating system providers took the decision to issue security updates informing administrators of the change.

You should therefore regularly assess whether your encryption keys remain sufficiently large to prevent a brute force or other method of attack. You should also assess the risks and likelihood of an attack given the amount and type of personal data you hold.

Choose the right software

The way that encryption software is put together is also crucially important. Software can use a state-of-the-art algorithm and a suitably long key to output encrypted data, but if its development did not follow good practice, or the product itself is poorly tested or subject to insufficient review, there may be vulnerabilities or other opportunities for attackers to intercept data or break the encryption without the users' knowledge. It is also possible that the encryption software includes an intentional weakness or backdoor to enable those with knowledge of that weakness to bypass the protection and access the data.

In cases where it is critical to have an assurance that these vulnerabilities do not exist, it is important to gain an external assessment of encryption software. An assessment may also assist you in defining an appropriate algorithm and key size.

It is recommended that you ensure that any solution that you, or a processor acting on your behalf, implement meets current standards such as FIPS 140-2 (cryptographic modules, software and hardware) and FIPS 197 (PDF). Encryption products certified via the National Cyber Security Centre's CAPS scheme would also meet the current standard. (You should also note that the reference to certification here is not to certification under Articles 42 and 43 of the UK GDPR.)

You can also find additional information on the current status of encryption algorithms in the following publications:

- guidance from the European Union Agency for Network and Information Security (ENISA) on Recommended cryptographic measures as well as its Algorithms, key sizes and parameters report (2014);
- ECRYPT-CSA's Algorithms, Key Size and Protocols Report (2018) which builds on the ENISA publications above and may have more up-to-date information; and
- the United States National Institute of Standards and Technology Special Publication 800-131A Revision 1 (Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths).

In some instances such specific assurances may not be available. For example, many open source software products do not have sufficient capital to fund an appropriate external assessment. However, government security agencies and private IT security organisations can offer advice regarding which specific protocols or algorithms which should be considered appropriate, although you should be aware of the limited assurances when no assurance or guidance is available. An example of such advice from the NCSC on the use of TLS includes:

> 'The lack of formal assurance in TLS implementations means there may be implementation weaknesses. Using recent, supported and fully patched versions of TLS implementations from reputable sources will help to manage this risk.'

This statement highlights the importance of keeping software up to date as vulnerabilities in the code may be discovered over time, eg Heartbleed and Shellshock.

Keep the key secure

It is important to ensure that symmetric keys and private keys remain secret as these provide the ability to decrypt the data.

In many cases keys are stored in a hierarchy for ease of management. The top level key is used to encrypt the keys below it and must therefore be managed securely.

All keys should have a finite lifespan and you need processes in place to generate a new key and re-encrypt the data. The old key should then be archived and securely deleted when no longer required.

In symmetric encryption, the key is sometimes derived from a shorter, more memorable password. It is therefore imperative that any password used to derive or secure the keys also remains secret. A poor choice or a compromise of the password can significantly lower, or even eliminate, the level of protection offered by an encryption product.

In the event that the key is compromised, or even if this possibility cannot be excluded, it may be necessary to revoke the existing key and generate a new key or key pair to protect data in the future.

It is also the case that loss of the decryption key will likely mean that no-one will be able to gain access to the data. Depending on the circumstances, loss of the decryption key could constitute 'accidental loss, destruction or damage' to personal data and would therefore be a contravention of the UK GDPR's security principle; additionally, if you cannot restore the data, this may also constitute a personal data breach due to a lack of availability, depending on the risks this poses.

Example

A laptop is protected using a secure full disk encryption product. This means that when the laptop is switched off the personal data is stored in an encrypted form.

The laptop is stolen. The thief powers on the laptop and is challenged for the password. Without knowledge of the password the thief is unable to access the data.

However, if the laptop user's username and password were written on a piece of paper stored alongside the laptop the thief has all the necessary information in order to decrypt the data and gain full access to it, thereby rendering the encryption ineffective.

Other resources

Encryption publications from the European Union Agency for Network and Information Security (ENISA):

- Report on recommended cryptographic measures (2013) (PDF)
- Study on cryptographic protocols (2014) (PDF)
- Algorithms, key sizes and parameters report (2014)) (PDF)

ECRYPT-CSA's publications, including:

- Algorithms, key sizes and protocols (2018) (PDF)

NIST Federal Information Processing Standards and Special Publications:

- FIPS 197 – the Advanced Encryption Standard (2001) (PDF)
- FIPS 140-2 – Security requirements for cryptographic modules (2002) (PDF)
- SP800-131A Revision 2 – Transitions: Recommendations for transitioning the use of cryptographic algorithms and key lengths (2019) (PDF)

NCSC certified products schemes and further guidance:

- CAPS Assisted Products
- Common Criteria (CC) international scheme
- List of products currently certified by the NCSC
- Data-in-transit protection, from NCSC's Cloud Security Principles

Encryption scenarios

In detail

There are a number of typical data processing activities where you should consider using encryption. In each case, it is important that you consider the residual risks even after implementing encryption.

The purpose of this section is to explore some of typical scenarios where personal data is processed, to indicate where you should consider encryption and to highlight the remaining risks that you should take into account.

- Transferring personal data by CD or DVD
- Transferring personal data by USB device
- Sending personal data by email
- Encrypted email
- Encrypted attachments
- Digital signatures
- Backups
- Sharing personal data online
- Mobile devices
- Fax
- Online Faxing
- CCTV
- Photography and video equipment
- Body worn video
- Law enforcement use of BWV
- Audio recordings
- Unmanned Aerial Systems (UAS)

Transferring personal data by CD or DVD

When it is necessary to transfer a large volume of personal data from one location to another you might consider using a physical disc such as a CD or DVD. In this scenario, you must consider the format of the data on the disc and the security of the transfer (eg the postal service used).

Using a recorded delivery method or specialist courier will give assurances that the disc is signed for by the intended recipient. This reduces, but not entirely eliminates, the risk of the personal data being intercepted, lost or stolen.

If you send the data unencrypted there is a risk that if it was lost or stolen any third party could gain unauthorised access to the personal data.

It is therefore necessary for you to consider encryption as a means of adding an additional layer of protection.

Encrypting the data on the disc ensures that an attacker could only gain access to the personal data by breaking the encryption.

However, in order to decrypt the data the recipient must have access to the correct type of hardware to read the disc (ie access to a CD drive) and compatible software to decrypt the data (in some cases the exact same software will be needed). This can cause some difficulties in corporate environments which have disabled access to CD drives or do not permit users to install unauthorised software.

You also need to consider a method to transfer the key or password to the recipient. To achieve the maximum guarantees that can be offered by the use of encryption the password must be transferred over a separate communication channel, eg by disclosing the password over the telephone upon confirmation that the package has been delivered. Including the password within the same envelope as the disc effectively removes the protection offered from the encryption.

Example

The Nursing and Midwifery Council were issued with a £150,000 Civil Monetary Penalty (under the DPA98) after the council lost three DVDs related to a nurse's misconduct hearing, which contained confidential personal information and evidence from two vulnerable children.

The ICO investigation found the information was not encrypted.

Transferring personal data by USB device

USB devices such as memory sticks or external hard drives offer a convenient way to transfer data. However, their small physical size and large data capacity means that large volumes of personal data can be lost or stolen with relative ease.

Furthermore, if personal data is not securely wiped from USB devices prior to reuse there is a possibility that data you consider 'deleted' could be recovered by a third-party.

Personal data can be encrypted by placing the files within an encrypted container on a USB device but this requires the recipient to have access to the same encryption algorithm or

software.

Hardware-encrypted USB devices are also available which contain the necessary encryption capability embedded within the device, meaning that the data can be decrypted without the need for the user to install additional software. However, due to the security risks present in permitting the use of USB devices, it is possible that you have implemented policies which forbid or technically limit the functionality of USB devices within your network. In this case you would need to consider how you might transfer data to these devices, and likewise how you would access data on any you receive.

You also need to consider a method to transfer the key or password to the recipient over a separate communication channel.

Example

North East Lincolnshire Council was issued with a civil monetary penalty of £80,000 (under the DPA98) after a serious data breach resulted in the sensitive information of hundreds of children with special educational needs being lost.

The information was stored on an unencrypted memory stick and went missing after the device was left in a laptop at the council's offices by a special educational needs teacher. When the teacher returned to the laptop the memory stick was gone and it has never been recovered.

The device contained sensitive personal information about the 286 children who attended local schools, including information about their mental and physical health problems and teaching requirements. The device also included the pupils' dates of birth and some included details of their home addresses and information about their home life.

Sending personal data by email

Another common method of sharing information is by email. By necessity the TO, FROM, DATE and SUBJECT fields of an email are transmitted in plaintext and may be accessed by any unintended recipient or third-party who intercepts the communication. Without additional encryption methods in place, the email body and any attachments will also be accessible to any unintended recipient or third-party who intercepts the communication.

A common type of personal data disclosure occurs when an email is sent to an incorrect recipient. You should be aware that encryption will only provide protection to personal data send by email if the incorrect recipient does not have the means to decrypt the data (eg does not have the decryption key).

Personal data can also be at risk if an individual gains unauthorised access to the email server or online account storing emails which have been read or waiting to be read.

The choice of password securing the server or email account is similarly important when considering the security requirements of the email system.

Some types of encrypted email solutions can be complex to set up and require the sender and recipient to have compatible systems for the encryption and decryption process. This can cause problems when you intend to send encrypted email to another organisation, to members of the public, or to anyone who has not previously been contacted.

Other systems are available which rely on the sender uploading encrypted data to a web application and using ordinary email to notify the recipient that a message is available (See 'Sharing information online' below).

There are efforts to design and implement a secure email protocol however there is still currently no universally-adopted method for sending email securely.

Some sectors have developed their own secure email systems, such as CJSM for criminal justice practitioners and NHSmail for sharing patient data. These solutions may be available to organisations working in these sectors and as a result should be used where possible, for as long as they continue to be supported. It is however important to recognise any residual risks with such systems and have appropriate policies in place to ensure correct usage. For example, systems may permit communication with external addresses in an unsecure and unencrypted manner. Sending a communication to the incorrect recipient may still remain a possibility.

Example

Surrey County Council was served with a civil monetary penalty of £120,000 (under the DPA98) after three data breaches that involved misdirected emails:

- a member of staff emailed a file containing the sensitive personal data of 241 individuals to the wrong email address. As the file was neither encrypted nor password protected, every recipient of the email could access the data. Subsequently, the Council was unable to confirm whether the recipients had destroyed the data or not;
- personal data was email to over 100 recipients on the Council's newsletter mailing list; and
- the children's services department sent sensitive personal data to an incorrect internal group address.

Example

North Somerset Council was served with a civil monetary penalty of £60,000 (under the DPA98) after five emails, two of which contained details of a child's serious case review, were sent to the wrong NHS employee.

A council employee selected the wrong email address during the creation of a personal distribution list. The data itself was not encrypted, and thus was able to be viewed by the unintended recipient.

Following the receipt of the data, the council employee was informed of the error by the recipient, yet the information was emailed to this individual on several further occasions. After an internal investigation the recipient confirmed the emails had been destroyed.

The ICO also found that the Council had not delivered appropriate data protection training to relevant staff, and recommended that the Council adopt a more secure means of sending information electronically such as using encryption.

Other resources

For more information on NHSMail and data protection, visit the NHSMail Portal.

Encrypted email

Encrypted email can provide the capability to encrypt the body and attachments of emails. For example, OpenPGP and S/MIME standards are widely-used encryption methods which have been implemented by a range of free and commercial software products.

The sending and receiving of encrypted email requires the use of compatible email client software and requires configuration in advance. A wide range of free and proprietary products are available for desktop, laptop and mobile operating systems. There are some specialist webmail providers which support encrypted email but it is not generally supported by the majority of online email providers, although there are some browser plug-ins which can provide this capability and further progress is being made in this area.

Encrypted email uses asymmetric encryption and requires a user to generate a key pair before they will be able to send an encrypted email. Users will also have to exchange public keys before an encrypted email can be sent between them.

The private key must be kept secret.

Configuring encrypted email within a corporate environment can cause complications for server-based malware scanning products as the content and attachments will be encrypted and may even be actively blocked by the scanning software. There can also be compatibility issues with automated email processing systems or managing multiple private keys amongst multiple staff (eg a common mailbox at support@example.com).

It can also be difficult for some individuals to install compatible software, generate key pairs, and appreciate the necessity of key management. Furthermore, loss of the private key can mean that received emails that were encrypted with the associated public key cannot be decrypted.

It is therefore necessary for you to consider the risks and investment required and whether there are alternative solutions for encrypted transfer of data should be considered.

You should have a policy governing encrypted email, including guidelines that enable staff to understand when they should or should not use it. For example, there may be a guideline stating that any email containing sensitive personal data (either in the body or as an unencrypted attachment) should be sent encrypted.

Encrypted attachments

Email can also send information by encrypted attachments. The file is encrypted using software on the sender's device and added as an attachment to a standard email.

This is similar in concept to sending data via USB devices or optical disks. In order to decrypt the attachment the recipient must have compatible software (in some cases the same software) and have access to the key. Commonly the key is derived from a shorter, more-memorable password which can be transferred to the recipient; however the password must be sufficiently long and complex to prevent compromise.

To achieve the maximum guarantees that can be offered by the use of encrypted attachments the key must be communicated over a separate communication channel, eg by disclosing the password over the telephone upon confirmation that the email has been delivered. Including the password within the same email as the encrypted attachment affords little protection to the encrypted personal data.

A common limitation to this method of data transfer is that most email providers will set an upper limit on the size of attachments that can be sent and received. Encrypted attachments that exceed any such limit would not be successfully sent.

Digital signatures

A digital signature can provide a level of trust that an email has not been intercepted or spoofed and that the contents match those that were sent by the sender. A digital signature by itself will not encrypt the communication.

Backups

Creating and storing a backup of data is an important component of a disaster recovery strategy. It is also important to keep a backup in a remote location (ie not in the same physical location as the live copy).

A common scenario is for an organisation to record backups onto tape, disk or other physical media which are moved to a secure location. If the data is stored in an encrypted format then it will be protected against unauthorised access. It will be important however to have good key management to ensure that the data can be accessed when necessary in the future.

In the case of a long-term backup or archive it may also be important to ensure that the data can still be accessed and that the encryption that was used remains appropriate over time. You will also need to consider the 'right to erasure' under Article 17 of the UK GDPR, and how this may apply when determining both the use of encryption and the retention period of your backups.

An additional option is for an organisation to use a cloud-based service for offsite backup or data storage. The data would typically be transmitted over the internet and stored on a remote server managed by the third-party cloud provider. Use of a secure transfer protocol (eg TLS) will ensure that data cannot be intercepted in transit. However, it is important to remember that without additional encryption methods in place the data will only be encrypted whilst in transit and be stored on the cloud provider's system in the same form as it is stored on your system.

If you encrypt the data prior to transmission (and keep the key secure) this would mean that the cloud provider, or any third-party who gained unauthorised access to the data, would be unable to access the data.

Example

Welcome Financial Services Limited was served a civil monetary penalty of £150,000 (under the 1998 Act) after the loss of more than half a million customers' details. The organisation was unable to locate two backup tapes which contained the names, addresses and telephone numbers of customers. Data on the backup tapes was not encrypted.

Sharing personal data online

There is a range of web applications that enable online file sharing. The feature can also be part of a larger product, such as within online word processing software where documents can be shared with a range of users to enable collaboration.

If you used a file sharing application you would typically transmit data to be stored on a server and accessed, over the internet, from a remote location. This could be achieved by you hosting your own system or by using a service managed by a third-party cloud provider.

Use of a secure transfer protocol (eg TLS) will ensure that data is not able to be intercepted whilst in transit. However, it is important to remember that without additional encryption methods in place the data will only be encrypted whilst in transit and not encrypted on the server or client device.

If the purpose of the online service is merely to provide a storage area from where the recipient can collect the data then you can encrypt the personal data prior to upload. This will ensure that no third-party (including a service provider) can gain access to the personal data. You can then grant the recipient access to the encrypted package. The sender will then need to transfer the key to the recipient.

If the web application performs some processing on the personal data then insisting that data remains in an encrypted form on the cloud server is a complex requirement. It either means that the service provider overlays their own encryption solution (for which they will likely hold the key) or requires a sophisticated key management system, which is not a feature found on most cloud-based file-sharing systems today.

It is more common that a web application offers the ability to 'share a private URL' or grant specific users access to individual files or folders. Whilst this can provide a secure and auditable means to share information, unless additional encryption methods are in place the files should not be regarded as being stored in an encrypted form. Even if data was stored encrypted a robust user authentication process, eg requiring a username and password, would still be a necessary component.

Mobile devices

By their very nature mobile devices such as laptops, smartphones and tablets have a high risk of loss or theft. Encryption of the data contained on the device can provide an assurance that, if this happens, the risk of unauthorised or unlawful access is significantly minimised.

Non-mobile devices, such as desktop PCs and servers, have a lower risk of loss or theft when they are stored and used in a secure location, eg, in a server room with restricted access. Although encryption is not generally used in non-mobile devices, you should recognise that there is still a risk of loss or theft of a disk or the device itself (eg during a break-in). Therefore, using encryption on non-mobile devices can be beneficial especially when the physical security cannot be maintained at an appropriate level.

Example

A civil monetary penalty notice of £150,000 (under the 1998 Act) was served to Glasgow City Council, following the loss of two unencrypted laptops, one of which contained the personal information of 20,143 people.

The laptops were missing from the unlocked storage where they were being kept overnight.

Fax

Fax remains a common means of transmitting personal data from one location to another in particular industries. Due to the limitations of the technology it is not generally possible for a data controller to overlay additional encryption measures.

Although fax machines are not immune from interception whilst in transit the Privacy and Electronic Communications Regulations require the provider of a public communications network to assure the security and confidentiality of the service.

As it is not possible to implement encryption of the message, it is essential to ensure that faxes are sent to the correct recipient or to consider whether another means of communication may be more appropriate.

Fax machines in public areas also present a risk that received faxes are not collected and any personal data they contain can be read by any passing individual. One method of addressing this risk is to move fax machines into 'safe havens' - a secure physical location with an agreed set of organisational measures surrounding their usage.

Example

A civil monetary penalty of £75,000 (under the 1998 Act) was served on Bank of Scotland plc for repeatedly faxing customer's account details to the incorrect recipients. The information included payslips, bank statements, account details and mortgage applications, along with customers' names, addresses and contact

details.

The data controller failed to implement additional technical and organisational measures having been previously informed that faxes were being misdirected.

Further reading

Read our Guide to PECR for more information about public communications networks and their security obligations.

Online Faxing

Online faxing, also called internet faxing or e-faxing, allows for the sending or delivery of faxes via the internet without the need of a dedicated phone line or a fax machine. It may be offered as a subscription service, and may form part of a wider package of cloud-based communications products.

Online faxing may offer benefits such as reduced infrastructure cost, ensuring the receipt of documents and enabling faxes to be sent and received from anywhere with an internet connection. From a security perspective any benefits will depend on how the particular service is implemented. For example, faxes could be delivered to the email inbox of the recipient rather than immediately printed on receipt by the fax machine. Online services may also offer additional encryption whilst the data is in transit – although the actual extent of protection may be limited. It is also the case that sending a fax to an email inbox would be at risk from a similar set of security risks as sending personal information entirely via email.

When deciding whether to use online faxing, some factors to consider may include:

- whether the provider offers encryption of any part of its services and faxes sent through them, as standard or for additional cost;
- similarly, whether the provider offers secure online storage, and whether it includes additional features (eg, the ability to delete faxes from its servers upon delivery in cases where sensitive information may be sent);
- whether the provider offers an audit trail of faxes sent and received through its servers; and
- where the provider's services are located and whether they are based in a secure environment.
- Use of online faxing has grown in some sectors, such as housing and healthcare. Where sensitive personal data are likely to be transmitted using online faxing, it is important to make sure that suitable technical and organisational safeguards for the

transmission and/or storage of data are in place.

CCTV

In general, CCTV is directed at viewing and/or recording the activities of individuals. Therefore, most uses of CCTV by organisations or businesses will be covered by the UK GDPR. The ICO issued a guidance on the use of video surveillance systems.

If you use CCTV systems that make use of wireless communication links (eg, transmitting images between cameras and a receiver), you should ensure that these signals are encrypted to prevent interception.

If you use CCTV systems that transmit images over the internet (eg, to allow viewing from a remote location), you should ensure that these signals are encrypted to prevent interception and also require some form of authentication for access (eg, a username and secure password).

The devices used to store CCTV images are also a common target during a break-in (eg, to remove potential evidence of the crime). In the first instance, you should consider the physical security of the storage device such as whether it is kept in a locked room. Newer systems may allow for recordings to be stored in an encrypted format which will prevent unauthorised access in the event of loss or theft, and which could be considered in addition to a range of appropriate access controls.

In responding to subject access requests or other disclosures, you should consider an appropriate format for the data to be disclosed, and appropriate security controls. During procurement, the capability of the device or prospective system to export data securely to third parties should also be considered. However, you should ensure that you do not use proprietary encryption that will restrict a data subject's ability to access their personal data.

Example

An organisation receives a subject access request for CCTV images. Its CCTV system can export images to an MP4 file format which can be accessed by the data subject on his personal computer. The organisation uses a file encryption product to encrypt the data before saving onto a CD (with a copy of the encryption software) and posting it to the data subject. Once the data subject confirms the safe receipt of the disc the organisation discloses the password used to generate the encryption key.

A second data subject submits a subject access request for CCTV images to be provided in a DVD Structure format (ie compatible with a standard DVD player).

The organisation accepts the request but is unable to encrypt the images because the DVD Structure format is not compatible with encryption and the data would therefore not be accessible to the data subject because a consumer DVD Player will not understand the data format. The organisation makes the data subject aware of this limitation and offers them the choice of collecting a DVD in person, recorded delivery, or to export in an alternative format.

Photography and video equipment

Use of digital photography and video recording can provide a permanent record of an event for a range of different purposes. Consumer devices may not possess the ability to encrypt images stored on the device. As a result there is a risk of unauthorised access if the device, or a removable memory card, is lost or stolen.

When encryption is not a reasonable option, it is important to consider the measures you can take to ensure that the risk is reduced to a tolerable level. For example, you could transfer images from the camera to a secure location and securely delete them from the memory card as soon as is practical.

It may also be possible to consider using an alternative device such as a smartphone or tablet which does offer an encrypted file system and encryption of their memory cards. However, you should take care that the device does not automatically upload images to a remote cloud service or social network and that the method used to transfer the images from the device does not present a further security risk (eg transfer as an email attachment).

Example

The Royal Veterinary College signed an undertaking to comply with the seventh data protection principle following the loss of a memory card containing personal data.
The ICO investigation revealed that a personal digital camera was lost which included a memory card containing the passport images of six job applicants.

Given that the camera in question did not support encryption additional technical and organisational measures could have been put in place to militate against the loss or theft of the camera or memory card. This could include a process for the transfer of images to a secure location and deletion from the memory card as soon as practicable.

A further option would include use of a photocopier or a scanner to take copies of the documents where necessary.

Body worn video

Body worn video devices (BWV), worn as part of a uniform, are increasingly being considered for use in the workplace, especially by the emergency services. There are also a range of 'sports action cameras' which are being used by data controllers for this purpose.

The sensitivity of the footage (including both audio and video) will differ according to the situation. If you use such devices, you must therefore take into account the extent of the damage and distress if they were accessed by an unauthorised individual. Given the potentially active nature of individuals wearing BWV, you must also take into account the increased likelihood of loss or theft. This is complicated by the method by which the device stores data. For example, some BWV devices store data directly on the device, whilst others store data on removable memory cards. Loss of such a card, either due to theft or technical issues, may be perceived as a greater risk than the loss of the device itself.

If video was stored in an encrypted form on the device and it is lost or stolen then the potential for unauthorised access is greatly reduced. Therefore, you should give specific consideration to your own circumstances and consider the most appropriate encryption or other compensatory methods such as retaining a log of device usage, secure fastenings, copying data to a secure location and securely destroying data on the device as soon as practical.

Many BWV devices have replay screens, meaning that data may still be viewable on the device even if that data is stored in an encrypted form. This could pose a risk if the device in question is lost or stolen. Access controls such as PIN codes may mitigate this risk; however, you must ensure that you have appropriate protocols and management procedures in place, particularly if BWV devices may be issued on a personal basis as well as from a general repository.

Using a BWV device which stores data in encrypted form, in conjunction with appropriate access control to prevent any replay directly on the device, would protect against unauthorised access to footage should the device be lost or stolen. Encryption and access control may also protect against unauthorised copying of the footage to a personal device – encryption alone would not prevent unauthorised copying, but it could make accessing the data more difficult.

Law enforcement use of BWV

The use of BWV by law enforcement will often be in connection with a crime being committed. This type of personal data is likely to be particularly private and therefore should be treated with particular care. Additionally, there will be frequent occasions where footage will show victims, potential witnesses, suspects or other third parties in a state of

distress. The proximity and vantage point of cameras may also increase the level of privacy intrusion, for example recording footage from within someone's home.

In respect of BWV, the ICO's CCTV code of practice states:

> 'Because of the volume of personal data and potentially sensitive personal data that BWV cameras will process and the portability of them, it is important that you have appropriately robust technical and physical security in place to protect this information. For example, make sure devices can be encrypted, or where this is not appropriate have other ways of preventing unauthorised access to information.'

Technical guidance from the Home Office on body worn video includes the warning that:

> 'some suppliers may erroneously claim files are encrypted when they are in reality recorded in a non-standard format.'
> You must also consider the security of footage once transferred from the device for long-term storage and its accessibility in response to a subject access request.

Other resources

Read the Home Office's technical guidance on BWV at the GOV.UK website (PDF) (external link).

Audio recordings

The recording of audio can also provide an important permanent record of an event, for example, in a call centre or recording audio in addition to video as is possible with some CCTV systems. However, it can also be intrusive, as recognised in an enforcement notice issued in July 2012. The ICO's CCTV code of practice offers additional guidance on the proportionality considerations of audio recording.

You must consider the security of lawful recordings and whether this can be achieved through the use of full-disk or file encryption products. However, some types of audio recording devices such as a dictation machines may not routinely offer encryption. You must consider whether an alternative device is more appropriate or consider additional technical and organisational safeguards such as deleting the data as soon as practicable and locking the device away when not in use.

In the event that an unencrypted version of the recording should be retained (eg for playback in a Court of Law) then a range of other compensatory measures must be considered. These can include storage within a secure facility, limited and authorised access and an audit trail of ownership and usage.

You must also consider the security of recordings once transferred from the device for long-term storage and be aware of other requirements which may prohibit audio recording of certain types of data. For example, the Payment Card Industry Data Security Standard prohibits the recording of card validation codes.

Other resources

For more information on the PCI-DSS, visit the PCI Security Standards website (external link).

Unmanned Aerial Systems (UAS)

Unmanned Aerial Systems (UAS), also known as unmanned aerial vehicles (UAVs), remotely-piloted aircraft systems (RPAS) or drones, commonly include features allowing the user to record video footage.

Where you are using UAS and images or other personal data are transmitted from the drone back to the pilot (eg a live feed of video footage over Wi-Fi to a smartphone app) then the data should be appropriately protected against interception by using an encrypted wireless communication link. Using an encrypted wireless communication link may also give some protection against potential hijacking of the vehicle.

Where images or other personal data are stored on the vehicle (eg an on-board memory card) then the data should be appropriately protected in the event of loss or theft (eg following a crash). The data can be appropriately protected using encryption.

You must also consider the security of footage once transferred from the device for longer-term storage.

Additional legal requirements or best practice may include flying RPAS within line of sight, retaining a log of usage, copying data to a secure location and securely destroying data on the device as soon as practical. More general requirements regarding drone use are outside the scope of this guidance. For more information, wish to visit the website of the Civil Aviation Authority.

Further reading

Visit the Civil Aviation Authority’s website for guidance on the general requirements for drone use.