Data protection

Encryption

B2s1d1OBk4mBus91yYJ2yaO4Eob2Aqumk Nn8lr51Dk09a5ma6gE51Mkiw6tMkmAxc7wj9b

ico.

Information Commissioner's Office

Introduction

Introduction

In recent years there have been numerous incidents where personal data has been stolen, lost or subject to unauthorised access. In many of these cases, these were caused by data being inadequately protected or the devices the data was stored on being left in inappropriate places – and in some cases both. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued.

This guidance explores use of encryption through a range of practical scenarios to highlight when and where different encryption strategies can help provide a greater level of protection.

Overview

- Encryption protects information stored on mobile and static devices and in transmission.
- It is a way of safeguarding against unauthorised or unlawful processing of data.
- There are a number of different encryption options available.
- Organisations should consider encryption alongside other technical and organisational measures, taking into account the benefits and risks that it can offer.

What the DPA says

Principle 7 states:

> 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.

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).

Therefore the data controller requires that all data stored on laptops is 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 (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) 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 to keep algorithms and key sizes under consideration, normally by establishing a review period.

Encryption should be considered alongside a range of other technical and organisational security measures.

Organisations will need to ensure that use of encryption is effective against the risks they are trying to mitigate, as it cannot be used in every processing operation.

Organisations should consider the benefits that encryption will offer as well as the residual risks and whether there are other security measures that may be appropriate to put in place. A Privacy Impact Assessment will help document any decisions and the reasons for them. This can also ensure that the organisation is only using the minimum of personal data necessary for the purpose.

The importance of good key management should also not be underestimated. Organisations should ensure that they 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.

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

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 plain text form whilst being ‘actively processed’. For example, data contained within a spreadsheet can be stored in an encrypted format but in order to be opened by the spreadsheet software and analysed by the user it 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 is encryption useful?

When processing data, there are a number of areas that can benefit from the use of encryption. The benefits and risks of using encryption at these different points in the lifecycle should be assessed separately. The two main purposes for which data controllers may wish to 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

Data controllers 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.

Data controllers should also be aware of any industry or sector specific guidelines that may recommend a minimum standard for encrypting personal data.

Data storage

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.

Example

A civil monetary penalty of £150,000 was served on Greater Manchester Police 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.

The data controller 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.

Full disk encryption

Most modern operating systems have full disk encryption built in, which will encrypt the entire contents of the drive. The data is decrypted when the user accesses the device. Unfortunately, it may not be enabled by default, requiring it to be activated, for example by accessing the relevant settings options within the operating system of their device.

Some data controllers have considered setting a PIN or requiring users to provide a username/password in order to access a device. 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 plain text on the disk and 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)

Individual file encryption

Alternatively, organisations 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.

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 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.

Residual risks with encrypted data storage

Data controllers 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 that data is decrypted;
- 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 can also include employee awareness training.

Read our further guidance on protecting personal data in online services for more information:

Further Reading

> Protecting personal data in online services: learning from the mistakes of others
> For organisations
> PDF (469.54K)

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.

Data transfer

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

It is also good practice 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 above) 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 plain text).

Example

A data controller intends to use a cloud-based data storage service as a repository to archive data.

Data transfer
The data controller uses TLS to encrypt data whilst in transit such that is cannot be intercepted.

Data storage
The data controller recognises that Transport Layer Security will only provide appropriate protection whilst the data is in transit. Once received by the cloud provider the data would normally exist in a decrypted state. Therefore the data controller encrypts each file on his 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.

Residual risks with encrypted data transfer

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

- certain data relating to the communication may still be exposed (eg metadata) 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, data controllers should use an encrypted communication protocol (eg the latest version of TLS).

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.

Read our further guidance on protecting personal data in online services for more information:

Further Reading

Protecting personal data in online services: learning from the mistakes of others
For organisations
PDF (469.54K)

Types of encryption

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.

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.

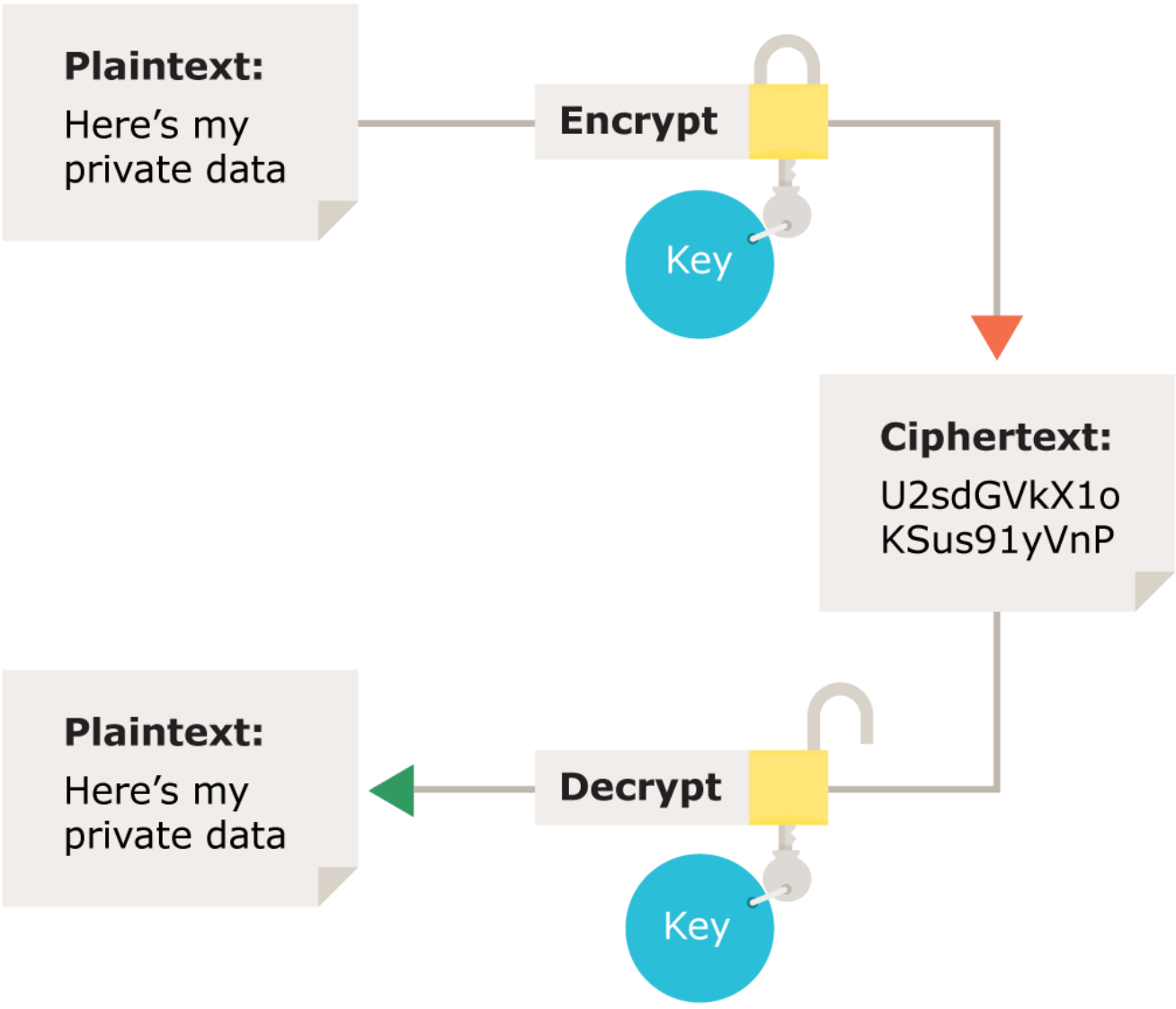

Figure 1: Symmetric encryption – Using the same key for encryption and decryption

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.

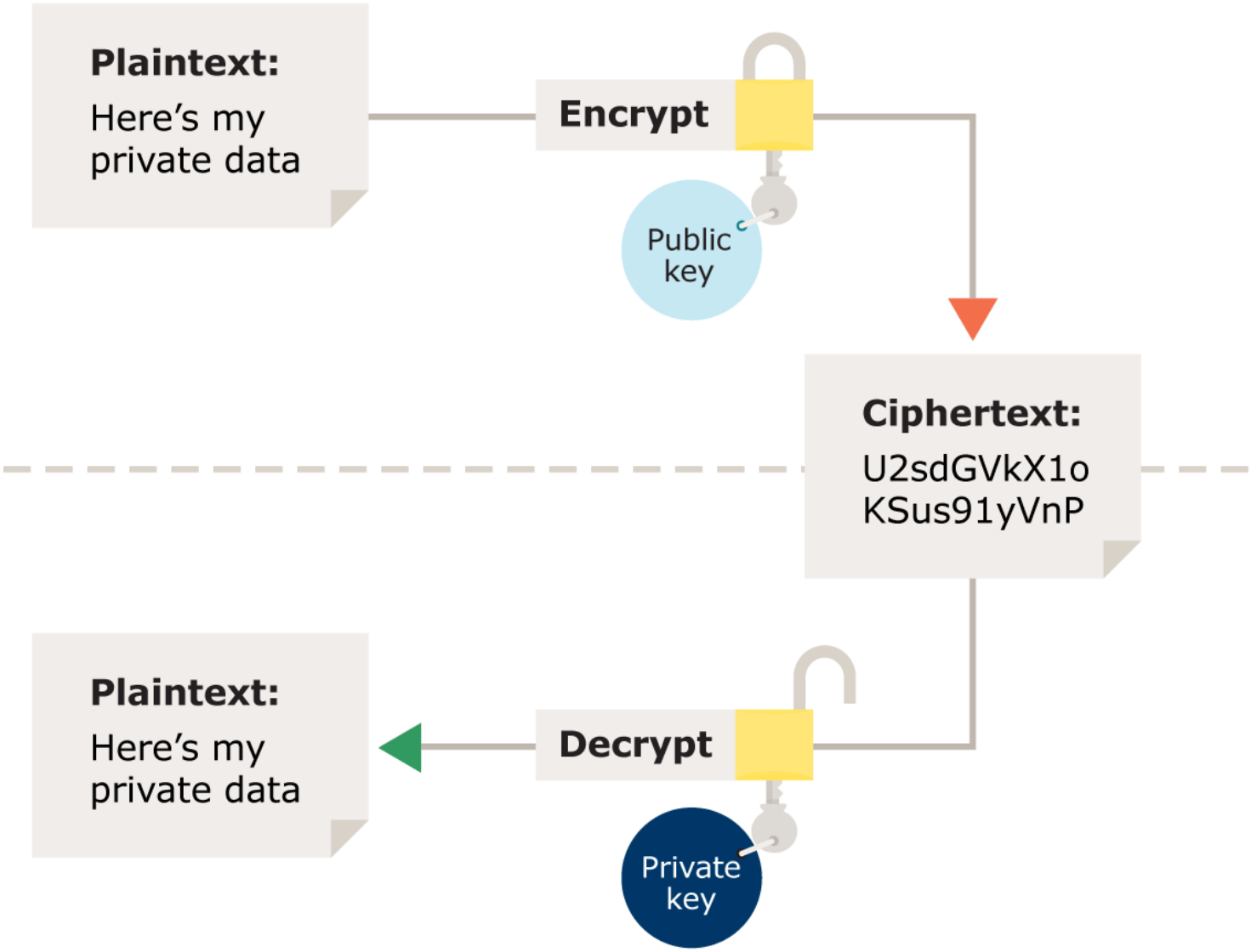

Figure 2: Asymmetric encryption – Using a different key for the encryption and decryption process

This use can also provide assurance of the identity of the sender or recipient of the communication. This is done using a process called digital signing. A message signed with the private key of the sender can be verified by the recipient using the corresponding public key. Certificates for signing communications can also be issued by trusted third parties (such as Certificate Authorities) who can provide further assurance that the owner of a particular key pair is who they say they are.

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.

Read our further guidance on protecting personal data in online services for more information:

Further Reading

Protecting personal data in online services: learning from the mistakes of others
For organisations
PDF (469.54K)

Implementing encryption

Choosing 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.

Organisations should therefore regularly assess whether their encryption method remains appropriate.

Rather than develop a custom algorithm it is recommended that a data controller uses a trusted and verified algorithm.

Accredited products (see 'Choosing the right software' below) can provide an assurance of suitability and also permit data controllers to demonstrate a level of compliance with legal obligations. However, it is important to review regularly the products being used due to the nature of technical development over time.

Choosing 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.

Data controllers should therefore regularly assess whether their encryption keys remain sufficiently large to prevent a brute force or other method of attack. They should also assess the risks and likelihood of an attack given the amount of personal data they hold.

Choosing 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 the weakness to bypass the protection and access the protected data.

It is therefore important to gain an external assessment of encryption software where it is of critical importance to have an assurance that such vulnerabilities do not exist. Such an assessment may also assist in defining an appropriate algorithm and key size.

It is recommended that data controllers ensure that any solution that they, or a data processor acting on their behalf, implement meets the current standards such as FIPS 140-2 (cryptographic modules, software and hardware) and FIPS 197.

Encryption products certified via the product and service tests from the National Cyber Security Centre (NCSC) – such as Foundation Grade assurance (under the Commercial Product Assurance scheme and/or International Common Criteria) or the CAPS Assisted Products scheme – would also meet the current standard.

Guidance from the European Union Agency for Network and Information Security on Recommended cryptographic measures and the United States National Institute of Standards and Technology Special Publication 800-131A Rev. 1 (Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths) also provide additional information on the current status of encryption algorithms.

In some instances such specific assurances may not be available. For example, many open source software products do not have sufficient capital to fund certification. However, government security agencies and private IT security organisations can offer advice regarding which specific protocols or algorithms which should be considered appropriate although a data controller should be aware of the limited assurances when no certification 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.

Keeping 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 data controllers 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. Loss of the decryption key could constitute an 'accidental loss or destruction of, or damage to, personal data' and would therefore be a breach of the seventh principle of the DPA.

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.

If the laptop is stolen and the thief powers on the laptop he is challenged for the password. Without knowledge of the password the attacker 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 ineffectual.

Scenarios

The purpose of this section is to explore some typical scenarios involving the processing of personal data, to indicate where an organisation can consider encryption and to highlight the remaining risks that a data controller should take into account.

Transferring personal data by CD or DVD

When it is necessary to transfer a large volume of personal data from one location to another a data controller might consider using a physical disc such as a CD or DVD. In this scenario the data controller 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 the data controller sent 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 to consider encryption to add 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.

The sender would 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 significantly reduces the protection offered from the encryption.

Example

The Nursing and Midwifery Council were issued with a £150,000 Civil Monetary Penalty 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 offer a convenient way to transfer data between two computers. 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 considered deleted by the data controller 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 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. Due to a number of security risks present in permitting the use of USB devices, a number of organisations have implemented policies which forbid or technically limit the functionality of USB devices.

The sender would 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 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 plain text 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. Data controllers 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 a data controller intends to send encrypted email between organisations, 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 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 emailed 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 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.

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

Data controllers 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.

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 the 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.

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 the data controller's system.

Read our guidance on the use of cloud computing for more information and advice on storing personal data in the cloud:

Further Reading

Guidance on the use of cloud computing
For organisations
PDF (329.06K)

If the data controller were to 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 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.

An organisation using a file sharing application would typically transmit data to be stored on a server and accessed, over the internet, from a remote location. This could be achieved by the data controller hosting their 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 the data controller 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. The data controller 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 (eg word processing) 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.

Read our further guidance on protecting personal data in online services for more information:

Further Reading

Protecting personal data in online services: learning from the mistakes of others
For organisations
PDF (469.54K)

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, data controllers 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 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.

As a result a number of organisations have moved 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 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.

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 DPA. The ICO has also issued a code of practice that provides recommendations on the use of CCTV systems to help organisations comply with the DPA.

Further Reading

> In the picture: A data protection code of practice for surveillance cameras and personal information
> For organisations
> PDF (407.24K)

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

CCTV systems which can transmit images over the internet (eg, to allow viewing from a remote location) 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, organisations 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, data controllers should consider an appropriate format of 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.

Example

A data controller receives a subject access request for CCTV images. The CCTV system can export images to an MP4 file format which can be accessed by the data subject on his personal computer. The data controller 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 data controller 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 data controller accepts the request but is unable to encrypt the images because the DVD Structure format is not compatible with encryption and would therefore not be accessible to the data subject because a consumer DVD Player will not understand the data format. The data controller 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 rarely contain 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 a data controller can take to ensure that the risk is reduced to a tolerable level. For example, transferring images from the camera to a secure location and securely deleting them from the memory card as soon as is practical.

It may also be possible to consider using an alternative device such as a smart-phone or tablet which does offer an encrypted file system and encryption of their memory cards. However, care should be taken 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. The extent of the damage and distress if it was accessed by an unauthorised person must therefore be taken into account by the data controller. Given the potentially active nature of individuals wearing BWV, data controllers 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 data controllers must give specific consideration to their 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, data controllers must ensure that they 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.

The data controller 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.

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.

Data controllers 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. The data controller 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.

The data controller 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.

Drones

Another emerging technology is the use of Unmanned Aerial Systems (UAS) also known as RPAS and drones. A common feature of UAS is the ability to record video footage.

Where images or other personal data are transmitted from the vehicle 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.

Additional legal requirements or best practice will 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.

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