Encryption guide for self-employed professionals and SMEs

December 2025

EXECUTIVE SUMMARY:

Encryption of information is a tool whose use should be encouraged in the task of protecting personal data and the security of communications in all areas, including in the professional sphere.

This is expressed in Recital 83 of the General Data Protection Regulation, which states that 'in order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should assess the risks inherent in the processing and implement measures to mitigate those risks, such as encryption'.

This guide is aimed at self-employed professionals and small and medium-sized enterprises (SMEs), in order to provide them with a practical approach that will make it easier for them to implement secure and appropriate encryption measures in various scenarios, such as sending e-mails, storing cloud and protecting information stored on devices.

The guide analyses significant real events in various sectors, where the serious consequences of failing to apply minimum protection measures can be seen, which can result not only in data leaks, fraud or identity theft, but also in serious harm to the physical or psychological integrity of individuals, as well as the administrative and other consequences that those responsible will have to face.

It also underlines the importance of taking measures to ensure data protection, i.e. privacy measures. We refer in particular to the application of the principle of data minimization, which ensures that only information that is strictly necessary at each stage of the processing and for its specific purpose is processed, and which makes it possible to reduce the impact on individuals when security measures fail.

Throughout the document, tools and resources are provided to help professionals and SMEs improve information security, minimizing risks for individuals and complying with the data protection rules in force.

Keywords: Privacy, GDPR, internet, data protection, cybersecurity, gap, encryption, password, data, risks, anonymization, authentication, credentials, personal data, email, fraud, pseudonymization, attack, cloud, mail, cryptography.

INDEX

I. OBJECTIVE AND TARGET AUDIENCE

The aim of this guide is to provide self-employed professionals and small and medium-sized enterprises (SMEs) with the necessary tools and knowledge to effectively implement data encryption in their operations. Encryption consists of transforming the information into an illegible format for anyone who does not have the decryption key. In this way, only authorized persons can access the data[1].

This guide is intended for those processing personal data, which in some cases may include sensitive data, such as customer personal data or financial records, and should ensure the protection of the rights and freedoms of those third parties, identified or identifiable natural persons, whose personal data are processed. It aims to mitigate the impact of personal data gaps, protecting the confidentiality, integrity and availability of information. In addition, as a desirable collateral effect, it helps to protect the object of business from unauthorized access.

The use cases analyzed in this guide, extracted from real gaps that have been reported and reported to the AEPD, reflect situations in which the lack of security measures in the processing of information has had serious consequences for natural persons. **Sections IV** and **V** provide solutions based on encryption that, had they been applied beforehand, would have mitigated or avoided the problems described.

II. WHAT CAN HAPPEN IF THE INFORMATION IS NOT ENCRYPTED?

First, the entity responsible for handling personal data, own or third party, must be aware of which processing involves a risk for natural persons: those who may have a significant impact on the rights and freedoms of individuals, and in some cases may have an impact on their physical integrity. It is necessary to reflect on the impact that the processing of personal data carried out in the context of any activity may have and to incorporate the necessary safeguards to minimize or even eliminate possible risks.

The impact of a gap can be severe, even if it does not affect special categories of data. For example, an address or telephone are not special categories of data, but when linked to victims of gender-based violence, their disclosure to third parties can have a fatal impact on individuals' physical integrity.

If data processing is not carried out with appropriate security measures in place, personal data can be intercepted, stolen or exposed, increasing the risk of unauthorized access, tampering, impersonation, fraud, personal or virtual attacks and other crimes. Furthermore, the inappropriate handling of sensitive information can lead to serious consequences for the persons concerned, such as discrimination, harassment, violence or even endangering their physical integrity, as well as reputational damage and breaches of law. We must not forget that the lack of appropriate organizational, legal and technical safeguards in data processing may also lead to civil or criminal liability, as well as administrative penalties for breaching data protection rules.

The following are examples of failures in information processing that have had serious consequences in different areas:

[1] See Guidance on the validation of cryptographic systems in data protection (https://www.aepd.es/documento/orientaciones-criptografía-aepd-isms-apep.pdf)and the associated tool Valida-Cripto GDPR (https://validacriptorgpd.aepd.es/)

A. LOST DEVICE: LEAKING CHILDREN'S CONFIDENTIAL DATA ON THE DARK WEB

An employee at a travel agency sends a file containing all the travel contracts made for the upcoming holidays to headquarters. By mistake, they enter the wrong email address and send it to a large number of people. The file contains the postal addresses of people going on holiday and the dates when their homes will be empty. This leak exposes customers to potential theft, as third parties can use the information to plan burglaries while the owners are away.

Should the hard disk have been encrypted?

In March this year alone, the AEPD received almost 170 notifications of personal data gaps affecting the confidentiality of information, 50 % of which were due to data exfiltration, **loss of devices** or personal data communications that were not adequately encrypted.

Devices that contain data with a high potential impact and that are used outside secure environments should be appropriately encrypted. This case is significant in terms of the number of times it has occurred.

It should also be noted that data encryption, which is an essential security measure under the GDPR, is not sufficient on its own. The best way to protect children's data on portable devices is to minimize the amount of data stored on them, keeping – exclusively – those that are indispensable to fulfil the purpose for which they were collected.

Where do we need to be involved?

In this case, there has been a serious breach of the confidentiality of particularly sensitive data, such as data related to children. Regardless of whether encryption measures have been applied, in the event of such an incident, it must be reported immediately to the centre's data protection officer and the competent authorities, as it may pose a high risk to the rights of those affected. It should also be assessed whether the controller should communicate immediately[2] to the persons concerned (in this case, those exercising parental authority or guardianship over children) the information necessary to make them aware of the risks caused by this situation and to take appropriate measures to be able to minimize them.

Should the files have been protected differently?

Yes, in addition to the encryption of the hard disk, the files could have been protected by encrypting them individually before storing them on the laptop. This would have minimized the risk of exposure in case of loss or theft of the device, without prejudice to the fact that other privacy measures have been implemented consisting of: assess the strict need to remove such information from the school, apply minimization and pseudonymization criteria in data collection and storage, remove information on minors when it is no longer needed, set passwords to restrict access and follow school security protocols.

How could this case have been avoided?

The loss of a laptop with confidential information of pupils poses a significant risk, as third parties could access personal data, photographs, addresses or itineraries. If the **hard disk of the computer were encrypted**, even if the device fell into the wrong hands, it would make access to the stored information more difficult or impossible, allowing both the centre and

[2] The communication of personal data gaps is explained in detail in the AEPD's Guide to reporting data gaps and infographic Protecting people in the digital world.

stakeholders to take appropriate protective measures. Implementing restricted access measures, such as two-step authentication and remote erasing of the device, would add an additional layer of protection against such incidents.

B. UNINTENTIONAL PUBLICATION: EXPOSURE OF SENSITIVE FAMILY PLANNING DATA ON THE INTERNET

A doctor at a family planning clinic has all the data on his procedures stored in an unencrypted spreadsheet. When a file-sharing application is installed on his computer, he accidentally shares the spreadsheet publicly. The data of many women who have had voluntary terminations of pregnancy has been freely exposed on the Internet, with family and social consequences. Some of these women are even residents of countries where they are prohibited from exercising their rights and may face consequences worse than criminal penalties.

Is there liability?

Yes, the doctor and the clinic have legal responsibility, as they have failed to comply with data protection regulations by failing to ensure the security of sensitive information held by them. This situation can be described as a personal data confidentiality gap, which must be notified to the AEPD and immediately communicated to the data subjects, assuming responsibility, and including advice to minimize the impact that this gap might have on them[3]. In addition, they may also have ethical responsibility for not having adequately protected the professional secrecy obligations that may be applicable.

Were the data encrypted?

No, in this case the data were not encrypted, allowing them to be easily accessible by third parties when they were accidentally shared. If they had been correctly encrypted, even if they had been exposed, access to information would have been much more complex and time-consuming and resource intensive. Moreover, not being available to a general public, removal of online content would have been easier. This highlights the importance of encryption as an essential measure in the protection of sensitive data. **Sections IV and V** present some tools to be able to apply information encryption techniques.

In addition to encryption, other practices that could have mitigated the impact of this leak would be pseudonymization and data minimization, consisting of first replacing patients' full names with codes that can only be decrypted by the controller, and second storing the strictly necessary information, for the necessary time, and avoiding including personal data that could directly identify patients. This would have significantly reduced the risk of unauthorized access to information in the event of a security gap.

How could this case have been avoided?

The accidental sending of the register of patient treatments represents a serious breach of confidentiality. If the patient files were **encrypted before being** published or sent, only the authorized recipient with the key to decrypt them would be able to access their content. In addition, in the professional field, the use of **encrypted emails** and **secure file-sharing**

[3] AEPD publishes guidance for healthcare professionals | AEPD

platforms would also help to further reduce these risks, ensuring greater protection of information. It should also be considered that, where the decryption key enabling access to information in readable format has to be distributed, that distribution should be carried out by a means other than that used to send the files, for example by means of a telephone call, a secure SMS message or the use of a shared password manager, ensuring that, in the event of erroneous sending, the data remain inaccessible. Implementing strict access controls, regular security audits and double verification mechanisms in sending confidential information would further strengthen the protection of medical data.

C. ERRONEOUS SENDING OF EMAIL: DISCLOSURE OF CONFIDENTIAL INFORMATION TO THE WRONG PERSON

A solicitor emails an encrypted legal document to his client. In the same message, he indicates that the password to decrypt it corresponds to the client's national identity number. By mistake, the solicitor sends the email to his client's ex-partner, who has a restraining order for gender-based violence. Since she knows her ex-partner's national identity number, she can access the confidential information in the message. In addition, the solicitor included unnecessary details in the subject line of the email, which exacerbates the exposure of the information.

Is it secure to send encrypted documents by email?

The security of encrypted information depends, among other things, on how the decryption key is handled. In this case, including the password in the same message (e.g. an email) nullifies the security of the encryption, as the encryption key of the attached files can be accessed if the mail is intercepted. Including leads or information to help find the key is a practice that also negates the effectiveness of encryption. In these cases, the key should ideally be shared by a separate channel, which is not obvious, nor information that is easy to infer by a third party (e.g. through a call or alternative text message, or by using obvious keys such as the telephone or ID of the recipient). Sending the key by the same means, e.g. mail, but in two separate messages is not fully effective, as if the channel has been compromised, the attacker will have access to the messages exchanged by it[4]. It is also essential to always verify the address of the recipient before sending confidential information to avoid human errors that could compromise data security.

Can the content of the mail case aggravate the consequences?

Yes. If the subject of the mail contains information that is unnecessary, sensitive or that makes the content of the message evident, it could increase the risk of exposure and aggravate the liability of the sender and the consequences for the customer. In this case, disclosing details about the client or the type of document in the case could facilitate decryption and thus undue access to information, constituting a potential breach of data protection law obligations, in addition to the obligation to maintain professional secrecy contained in the Bar Code.

[4] For example, Directive (EU) 2015/2366 (PSD2) provides that where strong authentication is required within its scope, it should be based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is), which should be independent of each other, i.e. in such a way that the breach of one does not compromise the reliability of the others, and designed in such a way as to protect the confidentiality of the authentication data (Article 4.30).

How could this case have been avoided?

The erroneous sending of a legal document to an unauthorized addressee constitutes a breach of **confidentiality**, especially in the situation referred to above. Even if the document is encrypted, including the key in the same email removes any protection that encryption could offer, allowing **undue access** to sensitive data. To prevent such errors, it is crucial to use secure document exchange platforms and more robust authentication methods. In addition, the access password should never be sent in the same message as the encrypted document, but via a **separate secure channel**. It is also essential to write email matters in a neutral and cautious manner so as not to reveal unnecessary information that could exacerbate the exposure of the data.

D. NOT AUTHORIZED ACCESS TO DATA IN THE INFORMATION SYSTEM THROUGH ABUSE OF PRIVILEGES OF AN EXTERNAL SERVICE

An agency manages the property and insurance of a large number of owners. It has a backup copy stored on third-party services that is not encrypted. This copy has been accessed due to negligence or fraudulent data sales by the staff of that service. The data allows the identification of, among others, elderly people who live alone, their addresses, and the valuation of their assets, including their financial details. All of them are now exposed to scams or even assaults in their own homes.

Are they personal data?

In the eight cases set out in this section, the data handled by the various professionals are personal data (Article 4.1)[5]. In this case, the information contains the name, an identification number, bank details and location data that allow a person to be identifiable or identified.

Is it legal to store owner information in the cloud?

Personal data, once encrypted, remains personal data. Personal data can be stored on third-party services, e.g. the cloud. However, hiring a processor does not lead to a diversion of the liability required by the GDPR to a third party. The controller must diligently select a third party that guarantees, by contract, compliance with data protection rules, in particular the requirements of Article 28 GDPR regarding the relationship with a processor and the quality of service levels that guarantee the necessary availability required by Article 32 GDPR, and even – in some cases – manage the resilience of the processing using its own or other third parties' means. In addition, the third party should store the data on secure servers, using techniques such as restricted access to the files and encryption of the files. In case the cloud provider is outside the country, the conditions for international data transfers must also be met.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

How could this case have been avoided?

When contracting a cloud service, it must be ensured that the provider keeps the stored encrypted data. In addition, it is necessary to check whether there have recently been security incidents with that provider or whether it is subject to legislation obliging it to provide data to its authorities.

Implementing **pre-encryption of files** and using **end-to-end encryption platforms would ensure** that only authorized parties access information. It is also advisable to use two-step authentication to strengthen access security and monitor cloud activity to detect potential intrusion attempts or data leaks. In addition, establishing restricted access policies and regularly consulting specialists on the actual security of such a service would contribute to a better protection of confidential information.

E. SENDING E-MAIL TO MULTIPLE RECIPIENTS BY MISTAKE, DISCLOSING CONFIDENTIAL INFORMATION

An employee at a travel agency sends a file containing all the travel contracts made for the upcoming holidays to headquarters. By mistake, they enter the wrong email address and send it to a large number of people. The file contains the postal addresses of people going on holiday and the dates when their homes will be empty. This leak exposes customers to potential theft, as third parties can use the information to plan burglaries while the owners are away.

Could the same have happened if the information had not been sent?

Any storage of data is exposed to the possibility of theft of information and intrusions of access to information, but also to human error that does not necessarily have an intention to do so. We must assume the reality that we are human and a situation of stress can lead us to make mistakes.

What measures can be taken to prevent such an incident in the future?

A protocol for handling confidential information should be established, including the use of secure data sharing tools, such as encrypted platforms, which, while not preventing misposting, would contribute to mitigating the risk of unauthorized disclosure. In addition, strengthen privacy training and carefully check recipients before sending information, ensuring that only the indispensable is shared.

How could this case have been avoided?

The accidental sending of a confidential passenger register poses a significant risk, as third parties could access data such as bank accounts, itineraries or passport numbers. To prevent such incidents, it is crucial to encrypt documents containing sensitive information, limiting access to authorized persons. In addition, using **encryption tools** to protect files before they are sent and avoid sharing documents by unsecure means would minimize the risk of data leak. Implementing additional measures, such as the use of secure file transfer platforms, two-step authentication and strict controls on recipients, worker awareness or process review, would strengthen security and reduce the possibility of human errors.

F. ABUSE OF ACCESS PRIVILEGES: UNAUTHORIZED DISCLOSURE OF SENSITIVE DATA FOR DISCRIMINATORY PURPOSES

A laboratory conducts human DNA studies. Samples, results, and other personal information are stored in an unencrypted database. In the international context, an ethnic war breaks out with dramatic consequences. Someone with administrative permissions and access to the entire database leaks it so that third parties can use DNA to select potential data on people associated with the rival group. Although the source of the information is identified, it already appears in violent Telegram groups that promote attacks against the people affected and, by extension, against their families.

How should the database have been protected to prevent this incident?

In addition to encryption as a basic and essential measure, strict access control and privacy strategies ensuring the deletion or pseudonymization[6] of personal identifiers and data should have been implemented. In addition, the erasure or anonymization of the data should have taken place as soon as they are no longer strictly necessary.

The handling of genetic data requires an even higher level of security due to its sensitivity, the impact on the environment of the person concerned and its potential ethical implications. Accidental publication of genetic or health data could lead to discrimination, hate crime, attacks, psychological consequences or even legal repercussions.

What impact does the leak of these data have on the safety of those affected?

Exposure of genetic information in a context of conflict may endanger the lives of the individuals concerned and their family members. Genetic discrimination can lead to persecution, exclusion from services or targeted violence, as seen in conflicts with ethnic components.

These facts underline the need to process the data with the highest level of security and confidentiality. Moreover, genetic data is **irreplaceable** (as opposed to a password), so a leak has permanent consequences for the individuals concerned.

How could this case have been avoided?

The publication of DNA information could have been avoided by implementing strict security and privacy measures in the management of genetic data. First, the database should have been encrypted both at rest and in transit, ensuring that even if someone accessed it, the information could not be easily read or used. In addition, the principle of **minimum privileges** should have been applied, limiting access to data only to those who really need it and establishing **granular access controls**. **Auditing** and **continuous monitoring** of access to the database would have made it possible to detect suspicious behavior on time. It would also be essential to implement **traceability** measures and two-factor authentication (**2FA**) for the extraction of sensitive information, preventing a single person with administrator permissions from accessing and filtering all data without supervision.

[6] You can learn more about genetic data and association with the GDPR in Scientific research with genetic personal data and data concerning health: a European perspective on the globalised challenge'

G. TECHNICAL IMPACT: ONLINE PUBLIC DISPLAY OF USERS' PERSONAL HABITS

A running app (mobile or wristband) stores the routes of subscribed users on a server. These routes are only associated with a numerical identifier and certain parameters, such as the time of the run, gender or age, and are only accessible to each runner. Due to an error in the server configuration, the database is exposed on the Internet. Popular routes can be identified, as they are followed by many runners. However, other routes are also visible, some of which are used by only one runner, at isolated times and with information about their gender.

Are they considered personal data if there are only numerical identifiers and parameters such as sex or age?

Yes, even if no names are stored, unique identifiers are personal data if they allow an individual to be indirectly identified by singling out the individual, allowing actions specifically targeting the individual to be carried out in combination with other data, such as locations, movement patterns or specific characteristics.

What are the risks involved in making these routes publicly accessible?

The main risk is the physical safety of corridors, especially on solitary or short-distance routes. An attacker could identify habits, schedules and journeys of certain people, increasing the risk of stalking, harassment or assault. Additional data could identify the most vulnerable targets, such as children.

There is also a risk of impersonation if someone crosses the data with another source of information. To mitigate this, the app should implement encryption in the database, restrict access with robust authentication and further anonymize the data or introduce information from false journeys of imaginary people to avoid the existence of individual cases.

In addition, there is the possibility of a general security impact, such as revealing information on critical infrastructure, such as security, sanitary, energy or water facilities, etc.

How could this case have been avoided?

The accidental exposure of the database of a corridor app poses a serious risk to the safety of its users. If the information stored had been encrypted, even if third parties accessed the database, it could not be **interpreted** without the key. In addition, applying stricter anonymisation techniques, such as removing unique route patterns, would minimize the risk of someone identifying and tracking corridors. Implementing more **secure access controls** and restricting the visibility of sensitive data would also help avoid situations that compromise the privacy and security of users.

H. STOLEN DEVICE: DISCLOSURE OF SENSITIVE AND CONFIDENTIAL DATA ON THE INTERNET

An association that provides support to people undergoing addiction rehabilitation suffers a robbery at its headquarters, in which several unprotected computers are stolen. These devices stored confidential user data, including photographs, medical records, addresses, contact telephone numbers, and psychological evaluations. Subsequently, some of this data appeared on Internet forums, exposing those affected to discrimination, loss of employment and even blackmail.

Could the impact have been minimized if stolen devices were protected?

If computers had had full disk encryption[7], it would have been more complicated to access files without the decryption key. In addition, a robust authentication system could have prevented access even if they managed to switch on the devices. Also, the implementation of remote erasure solutions would have made it possible to remove the information after the theft. These measures should not only be limited to laptops, but also to all devices used.

What consequences could leaking this data have for those affected?

Participants in the association's programs could face serious problems, including discrimination at work, social and family level. Moreover, leaking their addresses and phones exposes them to potential threats, blackmail or violence. In some cases, this information could be used by criminal networks to coerce those affected or force them into risky situations.

How could this case have been avoided?

Leaking data from assisted persons could have been prevented with a comprehensive information security approach. The association should have implemented **encryption** on all devices to prevent access to the data by third parties outside the organization without permission to access the data. In addition, the use **of multi-factor authentication** and **restricted access** would have ensured that only authorized staff could access the information. Other essential measures include **physical security policies**, such as installing heightened alarms, cameras and locks, as well as training staff in **good cybersecurity practices**. Having a **remote erasure strategy and encrypted backups** would have made it possible to mitigate the impact in the event of theft, protecting those affected.

III. IF THE DATA IS ENCRYPTED, SHOULD NOTHING ELSE BE DONE?

Encryption is a fundamental tool for the protection of personal data, as it aims to allow only authorized persons to access protected information, such as databases with names and addresses. It also helps preserve the integrity of digital documents from manipulation and restrict unauthorized access to sensitive information, such as medical records or financial data. In cases of personal data gaps, and provided that the encryption and key management

[7] Setting the user and password for access to equipment does not equate to encryption of the device, they are complementary measures.

process has been properly carried out[8], using this technique would demonstrate diligence on the part of the controller[9], and what is really important, would reduce the impact on the individuals concerned. The effectiveness of encryption depends on the strength of the techniques and protocols used. Minimum requirements would be the adoption of secure and robust standards, such as AES-256 for data encryption and TLS 1.2 or higher to protect communications, as well as regularly reviewing that no obsolete algorithms or keys are used.

To ensure the robustness of encryption, i.e. an appropriate level of security and data protection, it is recommended to use algorithms and standards recognized as secure, such as the AES standard with at least 256-bit keys (AES-256) for data encryption, and TLS in versions equal to or greater than 1.2 to protect communications. Cryptographic techniques and protocols evolve over time; it is therefore important to regularly review security configurations and avoid the use of obsolete and unsafe algorithms or keys.

However, encryption alone is not a definitive solution to data protection compliance, as it does not guarantee **privacy, nor confidentiality,** nor does it amount to **anonymization** of data. The fact that an individual has access to your personal data or knows information about you beyond what is strictly necessary may affect your privacy, even if the data is protected with encryption. However, it is a diligent practice that can reduce liability if it has been correctly applied.

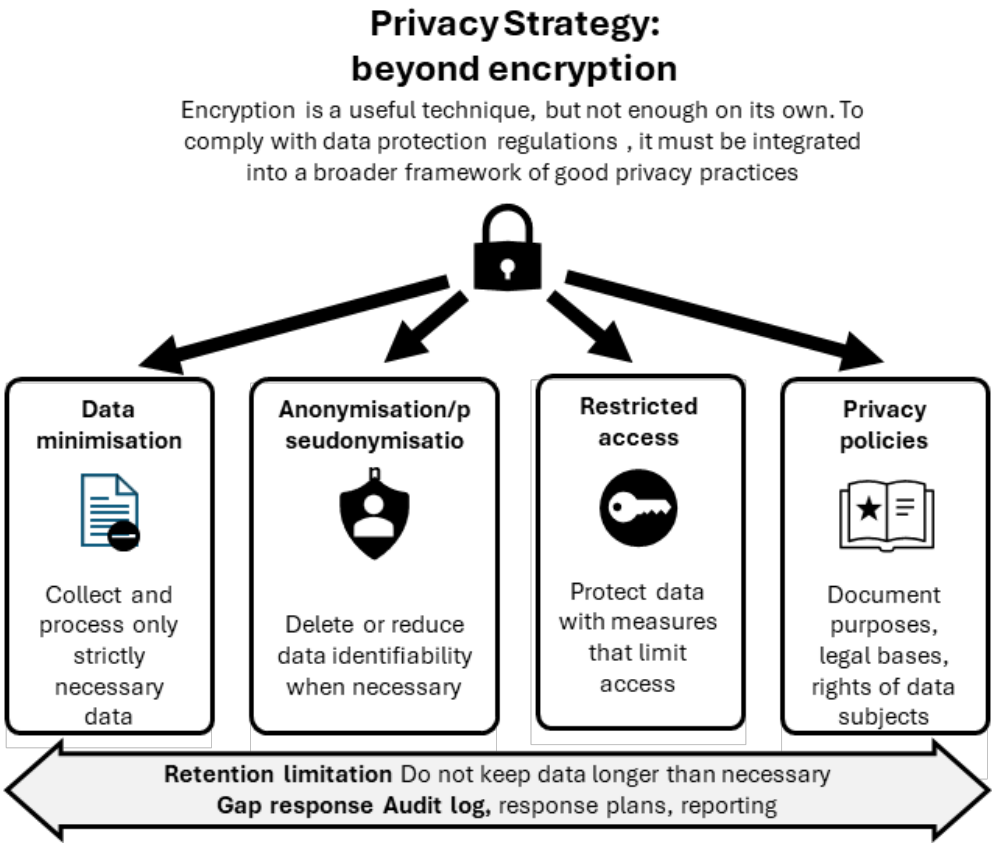
On anonymization, encryption does not eliminate the relationship between data and individuals, as there is still an identifying link. In order for data to be truly anonymous, any connection to the identity of individuals needs to be removed or dissociated. In addition, the decryption process for authorized operations implies that the data can be further processed. If the keys used are compromised, by filtration or deduction, or the data is unduly decrypted, the information would be exposed, with all the personal, legal and ethical implications that this entails.

ENCRYPTED PERSONAL DATA REMAINS PERSONAL DATA

For this reason, encryption should be embedded within a broader privacy strategy that combines techniques for minimization, storage limitation, access control, audit logs and procedures for reacting to personal data gaps aimed at protecting individuals and society. As explained by the AEPD blog post, Figures and Privacy: encryption in the GDPR, encryption is a powerful measure, but not sufficient on its own to ensure proper data processing. Indeed, Guide 10 Misunderstandings related to anonymisation highlights in its equivocal No. 2 that encryption does not replace anonymization, as it does not break the link between data and individuals.

For all these reasons, the application of the principles and obligations deriving from data protection rules does not depend solely on encryption, but on the application of a set of good privacy practices in the management, legal and technical fields. These measures include data minimization in the different processing operations, anonymization where necessary, restricted access protocols and appropriate privacy policies. The combination of these strategies makes it possible to ensure that data are protected at all stages of their processing and storage.

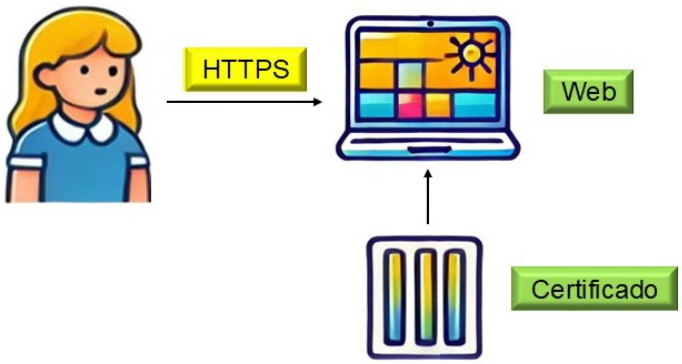
[8] See Guidance on the validation of cryptographic systems in data protection (https://www.aepd.es/documento/orientaciones-criptografía-aepd-isms-apep.pdf)and the associated tool Valida-Cripto GDPR (https://validacriptorgpd.aepd.es/)
[9] With regard to compliance with the principle of accountability laid down in Article 5.2 of the GDPR



IV. HOW CAN COMMUNICATIONS BE ENCRYPTED?

A. WEB BROWSING

Web browsing is the process of accessing websites to search for information or perform online activities. For the self-employed and SMEs, it is essential to be cautious when navigating, as many sites may be vulnerable to cyberattacks that try to steal information or infect devices with malware or *malware*. Using secure connections (https) and being alert to suspicious sites is key to protecting online safety. Encryption helps to ensure that communications, even if intercepted by a third party, do not serve them anything because they cannot know the content.



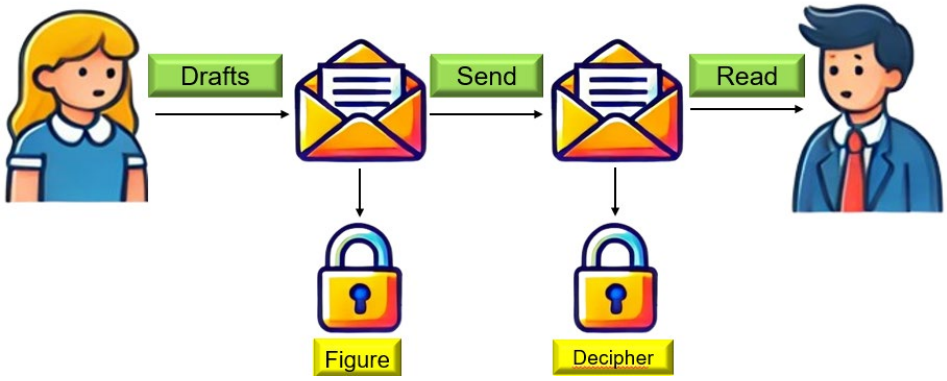
If you would like to know more about the functioning of electronic certificates on the web, you can consult the following information:

If your website has a security certificate, check that you use a secure version of the TLS | Empresas | INCIBE protocol

Encryption of information | Citizenship | INCIBE

B. EMAIL

E-mail is an essential day-to-day tool for any self-employed person or SME, both for customer communication and internal management. However, couriers can be an attack route if appropriate precautions are not taken. In order to protect the data sent, it is important to encrypt emails. This ensures that only the recipient can read the message, preventing unauthorized persons from having access to sensitive information[10]. In addition, the use of strong passwords and two-step verification increase security[11].



If you would like to know more about encryption of emails, you can consult the following information:

Secure email encryption with PGP | INCIBE-CERT | INCIBE

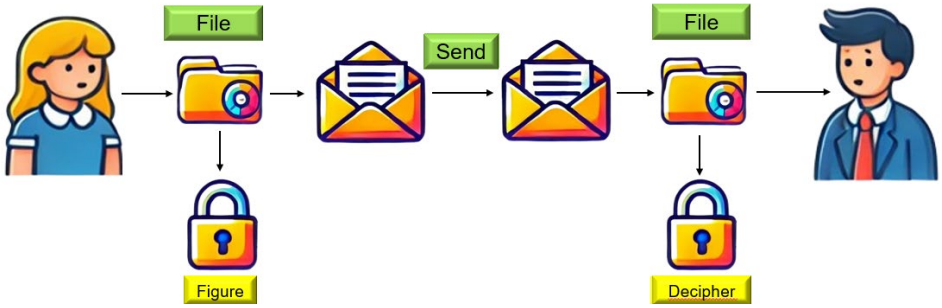
Information on Mail Encryption in Gmail – Gmail Help

C. ATTACHMENTS

The attached files are commonly used to share documents, presentations, contracts or other important files. However, attachments may be a security risk as they may contain malware or viruses. To protect the information, it is advisable to encrypt the files before sending them by email or sharing them via messaging platforms. Encryption ensures that even if a file is intercepted, only those with the right key can open it and access its content.

[10] There are also authentication methods complementary to email encryption that make it possible to avoid SPAM, phishing attacks and other security risks. Providers of email services should provide appropriate security measures configured by default, including sufficient information to enable them to be used correctly, as well as clear and precise information on the risks involved in deactivating these security measures. On the other hand, the self-employed and SMEs are obliged to contract services to guarantee these security measures. More information can be found here: Technology and training to protect your email domain | Enterprises | INCIBE

[11] You can learn more about the two-step verification (2FA) with the following resources: How to use the two-step verification with your Microsoft account – Microsoft technical support and how to activate the 2-step verification – computer – Google account support



If you want to know more about the encryption of the files to be attached, you can consult the following information:

Encryption and secure storage of step-by-step files | Citizenship | INCIBE

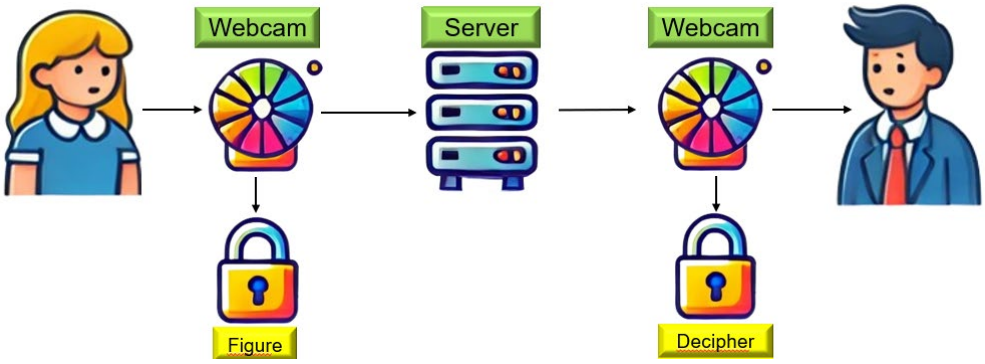
WinRar support – To secure a file with password

Protect data in 7zip file

How to encrypt your files with WinZip

D. VIDEOCONFERENCING

Videoconferencing is a crucial tool for communication between work teams or with clients. However, conversations can be vulnerable if secure platforms are not used. Encryption of videoconferencing is essential to protect the privacy of meetings and the information shared during meetings. In doing so, unauthorized persons are prevented from accessing conversations, which is essential when handling confidential data or sensitive discussions.

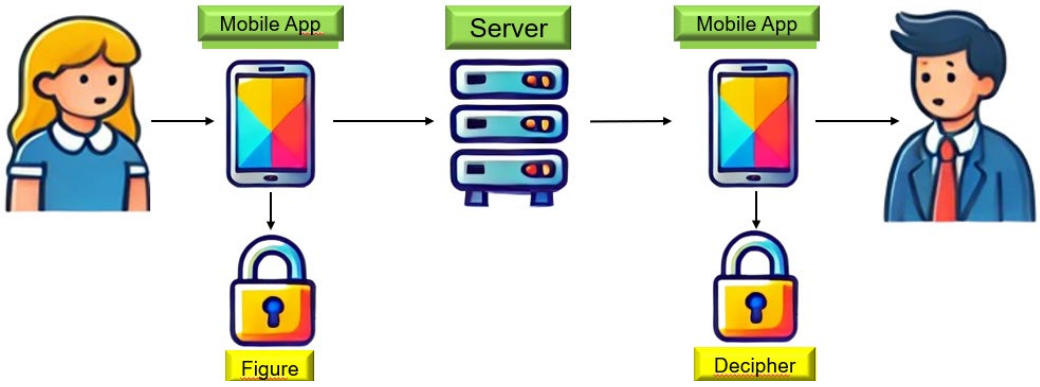


For more information on videoconferencing encryption, please consult the following information:

End-to-end encryption for Microsoft Teams – Microsoft Teams | Microsoft Learn

E. COURIER APPS

Messaging apps have become a daily tool for fast and effective communication. However, these applications may be vulnerable if not used properly. End-to-end encryption is crucial to ensure that messages cannot be intercepted by third parties during sending. It is important to choose messaging applications that offer this level of security, thus protecting confidential information and avoiding potential data leaks.



For more information on encryption of messaging apps, please consult the following information:

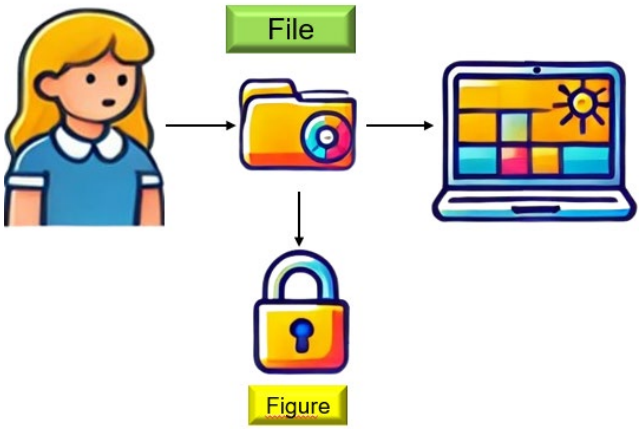
Encryption of information | Citizenship | INCIBE

Information about end-to-end encryption | WhatsApp Helpdesk

V. HOW CAN STORED DATA BE ENCRYPTED?

A. FILES

Files are one of the most common ways to store and share information in any business. They may range from contracts to financial reports. Encryption of files is essential, especially when they contain sensitive data such as personal customer information or financial data. Encryption ensures that even if a file is stolen or intercepted, it cannot be read without the appropriate key. Implementing encryption measures for both locally stored files and those shared over the internet is one of the best ways to protect information.



If you want to know more about encryption of files, you can consult the following information:

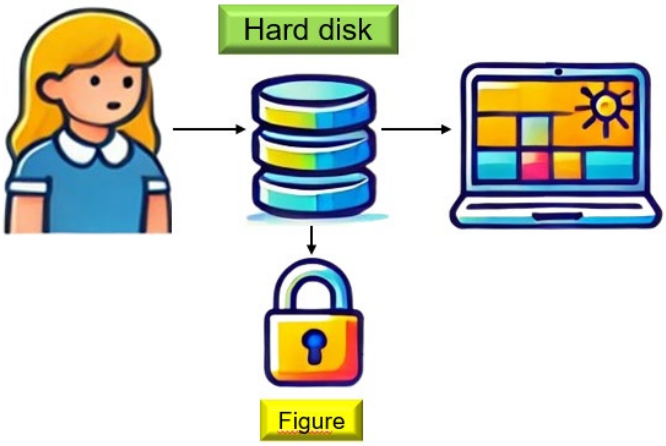
Encryption and secure storage of step-by-step files | Citizenship | INCIBE

Protect a document with a password – Microsoft technical support

B. HARD DISK OF A COMPUTER

The hard disk of a computer is the space where all the files, programs and data of the equipment are stored. If not protected, anyone who has access to the device can obtain

valuable information. Encrypting the hard disk is one of the most effective measures to protect stored information. When encrypting the hard disk, even if the device is stolen or lost, access to data would be significantly more difficult without the decryption key. Encrypting the hard drives of all devices used is essential to prevent the leakage of confidential data.



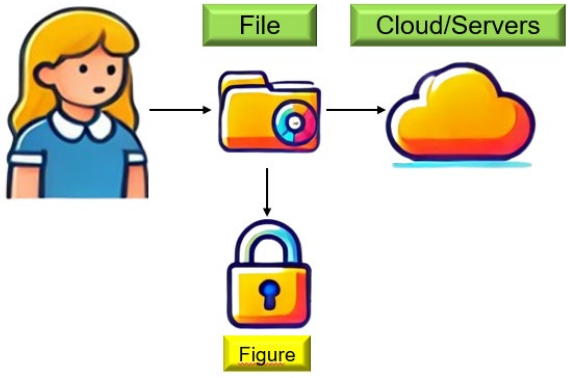
If you want to know more about encryption of a computer's hard disk, you can consult the following information:

Recommendations for the use of devices outside | CCN environments

Encrypted hard disk drives | Microsoft Learn

C. CLOUD DATA

Data in the cloud is increasingly common in businesses, as it allows information to be stored and accessed from anywhere. However, cloud services can also be vulnerable to attacks. Encryption of data in the cloud ensures that even if files are accessed from a remote server, the information will be protected. This encryption can be applied both before uploading the files to the cloud and during the storage process. It is important to choose cloud providers offering encryption and implement their own protection measures, such as encryption of sensitive files before storing them.



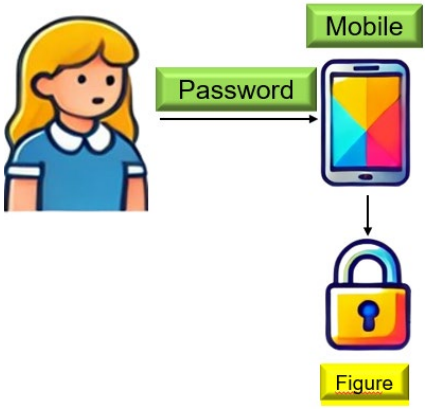
To find out more about encryption of data in the cloud, you can consult the following information:

Start using encrypted files in Drive, Documents, Calculation sheets and Presentations – Android – Google Drive support

Data protection through encryption – Amazon Simple Storage Service

D. MOBILE PHONES

Mobile phones are a key tool for the self-employed and employees of SMEs, as they are used both for communication and to access company information. However, mobile devices are susceptible to theft or unauthorized access. Encrypting the content of mobile phones is essential to protect the information they contain, such as emails, documents and contacts. In addition, when encrypting phones, it is ensured that, if the device is lost or stolen, personal and professional data will be protected, preventing unauthorized access to confidential information.



Figure

If you would like to know more about encryption of mobile phones, you can consult the following information:

Encryption of information | Citizenship | INCIBE

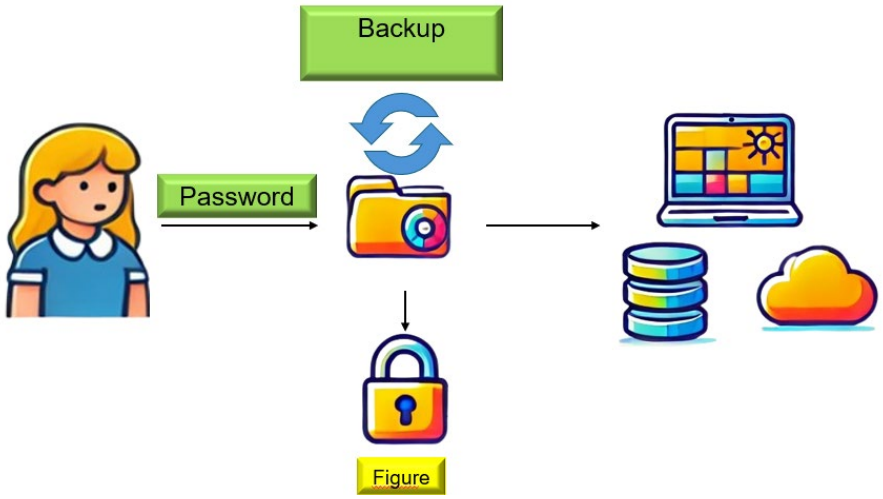
Encryption of the Android device: Microsoft Intune | Microsoft Learn

Use a code with iPhone, iPad or iPod touch – Apple technical support (ES)

E. BACKUPS

Backups are duplicates of files, documents and any kind of information stored for storage on another medium or location. They are essential to ensure business continuity and data recovery from incidents such as information losses, *ransomware* attacks or system failures. As they may contain sensitive information, they should be protected with the same level of security as the original data whether stored locally or in the cloud.

Encryption of backups is a key measure preventing unauthorized access to information stored, whether on hard drives, tapes or other devices, or in cloud services. In addition, it is important to audit access to the encryption keys used for these copies and to control the restoration processes, ensuring that only authorized staff can perform them.



Figure

If you would like to know more about encryption of backups, you can consult the following information:

- Backups: an approach guide for the entrepreneur | Empresas | INCIBE
- Backups: Security policies for SMEs | | tools INCIBE

VI. TO LEARN MORE ABOUT CRYPTOGRAPHY

Cryptography serves to protect the confidentiality, integrity and authenticity of information by preventing[12] unauthorized persons from accessing or manipulating it. By means of encryption techniques, data are transformed into an apparently illegible format that can only be decrypted with the appropriate key, reducing the risk of theft, fraud or leaks. Its use is essential in communications, digital transactions and the storage of sensitive information, ensuring security and compliance with data protection regulations.

A. WHAT IS CRYPTOGRAPHY?

Cryptography is the discipline that protects information by using mathematical techniques and algorithms to convert readable data (clear text) into an encrypted format (encrypted text), which in principle can only be understood by those who possess the keys necessary to decrypt it.

Its main objective is to ensure information security through four key pillars:

1. **Confidentiality**: It ensures that only authorized persons can access the data.
2. **Integrity**: It ensures that information is not altered or manipulated during storage or transmission.
3. **Authentication**: Verifies the identity of the parties involved in communication or access to the data.
4. **Non-repudiation**: Warns that someone denies having performed an action, such as sending a message or making a transaction.

In basic terms, cryptography transforms a legible message (clear text) into an encrypted message (encrypted text) using an encryption key and algorithm. Only the correct key will be

[12] This is generally impossible, as there is no guarantee that access to the information will be impossible with the necessary information, time and resources. It therefore gives a degree of confidence which is very important, but not absolute.

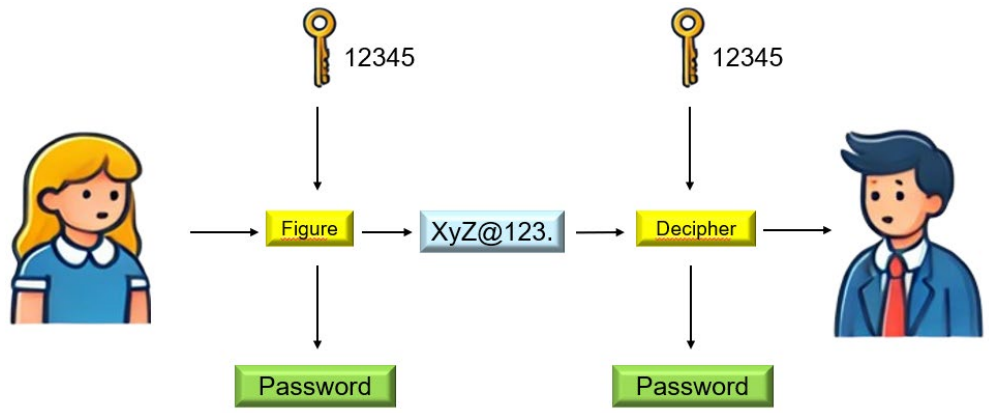
able to decrypt and read the message. This ensures that the information is secure even if it is intercepted by unauthorized third parties.

B. CORE CONCEPTS

1. **Clear text (original message):** The information to be protected.
2. **Encryption:** The message is transformed into an illegible format for others.
3. **Key:** A series of characters or numbers used to encrypt or decrypt the message.
4. **Encryption:** The process of transforming clear text into encrypted text. To ensure the robustness of encryption, i.e. an adequate level of security and data protection, it is recommended at least to use algorithms and standards recognized as secure, such as the AES standard with at least 256-bit keys (AES-256) for data encryption, and TLS in versions equal to or above 1.2 to protect communications. Cryptographic techniques and protocols evolve over time; it is therefore important to regularly review security configurations and avoid the use of obsolete and unsafe algorithms or keys.
5. **Decryption:** The reverse process, which converts encrypted text back into clear text.

C. SIMPLE EXAMPLE: ALICIA (SUPPLIER) AND BERNARDO (CUSTOMER)

1. **Encryption:** Alicia wants to send Bernardo a password so he can access her services. Instead of sending it directly, she encrypts it using a key (for example, 12345') and a simple algorithm. The plaintext message, 'password', becomes ciphertext, for example, XyZ@123.
2. **Transmission:** Alicia sends the encrypted text to Bernardo via an unsecured channel, such as an email.
3. **Decryption:** Bernardo, who knows the key "12345", uses the same algorithm to decrypt the message and get the original password.



Note: In this example, the key used to encrypt and decrypt the message is the same, but this may not always be the case (asymmetric encryption).

The Guidance on the Validation of Cryptographic Systems in Data Protection[13] published by the AEPD details the elements that it is advisable to assess in the design and validation of an encryption system used in the processing of personal data. This guide takes into

[13] https://www.aepd.es/documento/orientaciones-criptografía-aepd-isms-apep.pdf

account the significance of encryption in such processing, especially in cases where encryption is used to preserve confidentiality.

The guide proposes a non-exhaustive and non-enforceable list of controls to provide the controller or processor GDPR, the functional controller within these entities, the DPO, data protection advisors and internal and external auditors with the selection, validation and monitoring of encryption systems under a specific processing, as part of privacy by design and accountability.

The ValidaCripto GDPR tool[14] allows for simple and practical implementation of the guidance included in the guide, facilitating the assessment of cryptographic systems in the area of regulatory compliance.

VII. GENERAL RECOMMENDATIONS

In order to improve information security and prevent such incidents, it is recommended to adopt the following practices:

1. **Apply the principle of data minimization.** Only information strictly necessary for each purpose should be collected, processed and stored. Reducing the amount of data processed reduces the risk of exposure in case of safety gaps.
2. **Encrypt sensitive files before sending them by email or storing them in the cloud.** This ensures that even if a file is intercepted, it cannot be read without the key to decrypt it.
3. **Send the decryption key by a separate channel from the encrypted file.** To prevent an attacker intercepting the message from accessing the protected information, the key should never be sent in the same mail or platform as the encrypted file.
4. **Encrypt the hard disk of devices used to manage confidential information.** In the event of theft or loss, the data shall remain inaccessible without the relevant key.
5. **Use encrypted e-mail services and secure tools for document exchange.** Prioritize platforms offering end-to-end encryption to ensure data protection.
6. **Enable two-step authentication on mail accounts, cloud storage platforms and other critical services** to reduce the risk of unauthorized access.
7. **Be careful when sharing sensitive information, reviewing recipients before sending emails or messages with confidential files.** Applying access restrictions to shared documents can prevent accidental leaks.
8. **Avoid including in the subject of the email information that could reveal sensitive data or give clues about the content of the message.** This includes explicit references to personal data, diagnostics, transactions or possible keys to decrypt content.
9. **Use messaging applications with end-to-end encryption when transmitting sensitive data.** This prevents third parties from intercepting and accessing the information.
10. **Encrypted backups of important information on devices and in the cloud.** This ensures the availability of data without compromising their security in case of incidents.
11. **Implement access controls and role-based permissions.** Limiting access to information only to those who really need it within an organization significantly reduces the risk of leaks.

[14] https://validacriptorgpd.aepd.es/

12. **Training and raising staff awareness of data protection.** Many security gaps occur due to human error. Regular cybersecurity training and good practices in handling confidential information help prevent incidents.

As a final recommendation, just as the self-employed and SMEs use specialists to install their alarm systems, manage their accounting, tax or contracting duties, install their electricity, plumbing or mechanical equipment, etc., we advise them to use privacy and security specialists when needed.

By implementing these measures, the self-employed and SMEs can strengthen information protection, minimizing the impact of human errors, unauthorized access and cyberattacks.

VIII. REFERENCES

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Journal of the European Union. Available at https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e40-1-1

Spanish Data Protection Agency (AEPD). (2021). *How to report a personal data gap.* Available at https://www.aepd.es/documento/comunicar-brecha-datos-personales.pdf

Spanish Data Protection Agency (AEPD). (2022). *The AEPD publishes a guide for healthcare professionals.* Available at https://www.aepd.es/prensa-y-comunicación/notas-de-prensa/aepd-publica-guia-dirigida-profesionales-del-sector-sanitario

Spanish Data Protection Agency (AEPD). (2025). *Notification of personal data gaps to the Supervisory Authority.* Available at https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificación

Spanish Data Protection Agency (AEPD). (2019). *Encryption and Privacy: encryption in the GDPR.* Available at https://www.aepd.es/prensa-y-comunicación/blog/cifrado-y-privacidad-cifrado-en-el-rgpd

Spanish Data Protection Agency (AEPD). (2020). *Encryption and Privacy II: The data life time.* Available at https://www.aepd.es/prensa-y-comunicación/blog/cifrado-y-privacidad-ii-el-tiempo-de-vida-del-dato

National Institute for Cybersecurity (INCIBE). (2020). The man in the middle *attack on the company: risks and ways to avoid it.* Available at https://www.incibe.es/empresas/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo

National Institute for Cybersecurity (INCIBE). (2018). *Secure email encryption with PGP.* Available at https://www.incibe.es/incibe-cert/guias-y-estudios/guias/cifrado-seguro-de-correo-electrónico-con-pgp

PassFab. (2025). *How to unlock a protected Excel file.* Available at https://www.passfab.es/excel/desbloquear-excel-protegido.html

Information **Commissioner's Office (ICO)**. (2025). *Encryption scenarios.* Available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/encryption-scenarios/

National Cyber Security Centre (NCSC). (2025). *Cyber Aware.* Available at https://www.ncsc.gov.uk/cyberaware/home

National Institute of Standards and Technology (NIST). (2020). *Cybersecurity Basics – Case Study Series.* Available at https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series

Commission Nationale de l'Informatique et des Libertés (CNIL). (2021). *Violation of quarter: Tattaques sur les messageries.* Available at https://www.cnil.fr/fr/violation-du-trimestre-les-attaques-sur-les-messageries

Commission Nationale de l'Informatique et des Libertés (CNIL). (2011). *Comment réagir face à une usurpation d'identité.* Available at https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite

IX. ANNEXES

Spanish Data Protection Agency (AEPD). (2016). *Guide to privacy and security on the Internet.* Available at https://www.aepd.es/documento/guia-privacidad-y-seguridad-en-internet.pdf

Spanish Data Protection Agency (AEPD). (2020). *Guide on data protection by default.* Available at https://www.aepd.es/documento/guia-protección-datos-por-defecto.pdf

Spanish Data Protection Agency (AEPD). (2019). *Privacy by Design Guide.* Available at https://www.aepd.es/documento/guia-privacidad-desde-diseno.pdf

Spanish Data Protection Agency (AEPD). (2021). *Risk management and impact assessment on processing of personal data.* Available at https://www.aepd.es/guias/gestion-riesgo-y-evaluación-impacto-en-tratamientos-datos-personales.pdf

Spanish Data Protection Agency (AEPD). (2020). *List of data protection measures by design and by default.* Available at https://www.aepd.es/documento/PDpD-listado-medidas.xlsx

Spanish Data Protection Agency (AEPD). (2020). *Recommendations to protect personal data in mobility and teleworking situations.* Available at https://www.aepd.es/documento/nota-técnica-proteger-datos-teletrabajo.pdf

Spanish Data Protection Agency (AEPD). (2023). *Guidance for the validation of cryptographic systems in data protection.* Available at https://www.aepd.es/documento/orientaciones-criptografía-aepd-isms-apep.pdf

Spanish Data Protection Agency (AEPD). (2024). *Roadmap to ensure compliance with data protection rules.* Available at https://www.aepd.es/documento/hoja-de-ruta-v13.pdf