Deloitte.

Information Security Policies for compliance by third parties - Specific

Deloitte Portugal

Version: 5
Date of 1st version: 14-09-2017
Data of current version: 30-03-2022
Classification: Restrict
Reference: SGSI_Políticas de Segurança de Informação a cumprir por terceiros_Específico_EN.docx

Target Audience - Notice

This document is directed to all third parties (companies or individuals) who provide services to Deloitte Portugal and must be aware of and enforce compliance with their content.

Control of Versions - Notice

This document is a controlled document, which supersedes all other versions. Any copies from previous versions or dated prior to the abovementioned publication shall not be deemed valid.

Copyright - Notice

Miscellaneous - Notice

Any product names used herein are for identification purposes only and may be trademarks of the respective organisations.

Once services are rendered, any third party undertakes to return and/or destroy any copies hereof (printed and/or electronic format), and shall be held liable for noncompliance with this procedure.

Index

1 Acceptable Asset Use Policy

1.1 Introduction

This document defines Deloitte Portugal's Acceptable Use Policy of IT and Communication Assets, as well as the responsibilities of employees in their use, in order to guarantee the confidentiality, availability and integrity of the information of Deloitte Portugal and its clients, employees, suppliers, etc. (hereinafter Deloitte Portugal's information).

1.2 Oversight and audit

Deloitte Portugal reserves the right to oversee and audit, without prior notice, randomly and whenever it is justified by legitimate business reasons, in accordance with applicable legislation in effect:

- Information and software installed on laptop computers and portable storage devices;
- The activities carried out by its employees in business support information systems provided by the company;
- The activities carried out on the internet;
- The source, destination, and subject of any sent emails.

1.3 Use of laptop computers

1. Software installation

In order to ensure the protection of the information of Deloitte Portugal and its clients, employees cannot:

- Install computer games;
- Install software that allows file sharing on the Internet (P2P software);
- Install personal software, even if licenced by the employee;
- Install illegal software (unlicensed or without prior approval);
- Install other software on computers without a legitimate business reason duly justified by the Project Manager and authorised by the IT Director.

2. Physical protection of equipment

Employees must ensure that they take all necessary precautions to protect Deloitte Portugal's equipment and the information in their possession, regardless of how it is stored, thus avoiding improper access by third parties, namely:

- **Whilst at Deloitte Portugal's premises/clients' premises/hotels/public places:**
    - Equipment must be supervised, secured with the padlock provided with the computer, or stored in a locker or safe.

- On vehicles:
    - Equipment with customer information should not be left on any vehicles.
- On airplanes:
    - Equipment with customer information taken on trips shall not be dispatched as hold baggage.
- At home
    - Equipment with customer information should not be left unprotected, and equipment use should be restricted to authorised users only. The use of Deloitte Portugal's equipment by any employee's family members or friends is forbidden.

3. Clean screen policy

If a Deloitte Portugal's employee or an external entity is absent from their workplace, they must manually activate the screensaver mechanism, which will require them to re-enter their password to log in, although the system automatically activates the screensaver mechanism after 10 minutes of inactivity.

Whenever a Deloitte Portugal's employee or external entity is accessing confidential customer information (at the office, at home or in a public place), care should be taken to position their computer screen in a way that does not allow reading by third parties. Employees who routinely use their computer on airplanes or trains should use screen protection filters.

4. Logical security protections of a laptop computer

Employees cannot remove, disable or change security system settings (e.g., firewall, encryption mechanisms, virus and malware detection, patch installation, etc.) without a valid business reason and express approval for such effect by the project Manager and IT Director approval.

5. Backups

If a Deloitte laptop as been assigned, employees must make sure they are frequently connected to the Deloitte's network for regular backup of the data on their laptop computer in order to prevent loss of information. Hence, they must use the backup software provided by Deloitte Portugal and follow the respective instructions.

In locations where this tool is not available, employees should contact the Service Desk and request instructions on how to proceed in order to ensure backup of their data.

If a copy is made to a removable external disk, it must be encrypted and cannot be carried together with the computer. The disk should be stored in another location in order to guarantee the existence of a backup file.

1.4 Portable storage devices

The use of portable storage devices (e.g. USB Pens, External external Disks, SD Cards, etc.) for storing, transferring or transporting information from Deloitte Portugal is only allowed if they are previously encrypted using the provided technology, in accordance with existing procedures.

Whenever a password is required to access any encrypted information on a portable storage device, this must be communicated orally or sent by SMS, without mentioning its purpose. In these cases, employees must ensure that the device only contains the necessary information for the recipient.

Portable storage devices should be stored in protected locations when not in use, and whenever an employee wishes to destroy a removable device, they must place it in a dedicated container in the office.

In cases where a client needs to transfer data to Deloitte Portugal's employees by means of portable devices, employees must ask the client to encrypt the device or, alternatively, to have any data recorded on the device as an encrypted Zip file with password, that must be provided by another way (orally or by SMS) without reference to its purpose.

1.5 Mobile devices (mobile phones, smartphones, tablets)

Deloitte Portugal’s data can only be downloaded to mobile devices (smartphones, tablets) if they:

- Are owned by Deloitte or by Deloitte employees;
- Have installed the Mobile Device Management software and protection (Mobile Threat Defense) indicated by the Firm;
- Are encrypted, and;
- Are protected by password or PIN according to the company’s rules in place. The geo-referencing service of the APP, especially those related to social networks, should, whenever possible, be disabled.

1.6 Password management

Users shall guarantee the password confidentiality of their individual access account to Deloitte Portugal’s information systems, being forbidden to share it.

Thus, the account owner is solely responsible for all the consequences arising from the misuse of their account.

Users should apply good security practices to protect their password:

• Passwords should not be disclosed to other persons, including any Deloitte Portugal’s employees, including system administrators or Service Desk employees;

• Whenever it is necessary to save any password, it must be done in software that guarantees encrypted protection.

In order to ensure proper management of passwords, the following rules are established:

- Password robustness, generated by the system or users:
  - it shall have more than ten characters;
  - It shall include characters from at least three of the following four classes:
    - Capital letters (A, B, C);
    - Small letters (a, b, c);
    - Numbers (0, 1, 2);
    - Symbols (#, &, %, @, -, *).

- They shall not contain the first or last name of the user, a family member, a famous person, dates of birth or other personal information;
- They shall not contain any other name or words easily associated with the user;
- They shall not be a word from a dictionary or another that is part of a dialect or slang of any language, nor any of these words written backwards;
- The last twenty-four passwords cannot be reused.

• The user shall change the initial password assigned to it and sent after the first login;

• By default, any password is valid for 84 days. After this period, the password expires and the user will have to change it to continue having access to the information systems.

• Passwords must be changed whenever there are suspicions that they may have been compromised;

• The password must not be displayed on the screen while it is being entered;

• It is only possible to change the password every 24 hours;

• Passwords used by users in accounts for private purposes (such as personal emails), should not be used in Deloitte Portugal's data access accounts;

• Passwords should not be stored in automatic registration systems (e.g., Remind/save password in browser) or in mobile phones;

• The consecutive number of wrong attempts to access systems with a password is limited to five. The system must deny access when this limit is reached by blocking the user's account for a period of 30 minutes.

1.7 Viruses and malicious code

All computers with access to Deloitte Portugal’s network must have duly lawful and updated antiviruses software. This rule applies not only to computers assigned to Deloitte's employees but also to third-party computers that need to connect their devices to the network.

Deloitte Portugal's employees must take all reasonable steps to ensure that they are not responsible for any malicious code (Viruses, Malware, etc.) in the company’s information and communication systems. This includes, but is not limited to, the duty not to open attachments from unknown sources and not to download unauthorised software.

1.8 Use of corporate email system

Deloitte Portugal provides access to an email account to all its employees, to perform their professional activities.

Sending or receiving emails related to Deloitte Portugal’s business activities can only be done by means of email accounts of the company itself. The use of employees’ personal emails (Gmail, Yahoo, etc.) for communications related to the company’s business is not allowed, unless there is a valid business reason and express approval of the party responsible for the client for such purpose. Likewise, no communications related to the company’s business should be made to personal emails from clients or employees of our clients, without prior approval and justified business reasons.

Each personal email address is associated with a staff member who is responsible for it. The owner can delegate authorisations to their mailbox, but is fully responsible for the actions of any person authorised by them.

1. Email account passwords

Passwords of personal email accounts cannot be shared. Whenever one employee needs access to another employee's email account (for justifiable business reasons, such as administrative assistants), this must be done through the permissions feature of the email system.

2. Email attachments

Users should avoid sending messages with attachments that are larger than 50MB and to too many recipients as they can jam the email service. If absolutely necessary, files must be compressed to reduce the size of the email message.

3. Email accounts assigned to external entities

Deloitte Portugal's temporary personnel or external entities who need an email account to perform their duties, must be aware of and explicitly agree with Deloitte Portugal's policies, by signing a document for this effect. These persons (temporary personnel and/or external entities) should be aware that all messages generated and processed by the electronic mail systems and regarding the projects where they are involved are considered Deloitte Portugal's property.

The email accounts assigned to external entities should be used exclusively for the professional activities developed pursuant to the outsourced services.

1.9 Use of the telephone network

The internal telephone network should be used for business purposes, with reasonable personal use allowed.

In addition, the company's telephone network should not be used to:

- Make phone calls to value-added telephone numbers with access to offensive content which is morally objectionable, discriminatory or pornographic;
- Make offensive or defamatory communications, which discredit or embarrass, or constitute moral or discriminatory harassment;
- Promote or carry out any business that is not company's business; and/or
- Promote or advocate issues, causes, charities or organisations of any kind (including political activism) unless authorised by Deloitte Portugal.

1.10 Internet use

Deloitte Portugal provides corporate access to the Internet so that its employees can perform their professional activities on a daily basis. Internet access can be additionally used for participating in training actions and development of new skills and competencies.

Internet use for personal purposes is only allowed in a reasonable manner, if it:

- Does not translate into consumption of corporate resources that impact the business;
- Does not interfere with any employee's productivity;
- Does not prevent or impact the company's business activities;

• Does not violate the company's policies or any established confidentiality, availability or integrity requirements.

All Deloitte Portugal's employees must be aware that Internet access is monitored in a non-permanent and non-systematic way.

Deloitte Portugal's employees should not use the corporate Internet for:

- Personal activities such as:
    a. Listen to and/or download music;
    b. Watch videos and streaming;
    c. Play or access online games or gambling websites;
    d. Organise games or manage gaming forums;
    e. Access social networks, without a justifiable and/or business purpose.

It is expressly forbidden to use the corporate Internet to:

• Download illegal software or unlicensed software (when it is subject to licencing rules);

• Download freeware without a duly approved and legitimate business reason;

• Download or copy copyrighted material, trademark or patent registration or trade secret without authorisation of the owner of such rights;

• Provide third parties software that is Deloitte's intellectual property or licenced for it;

• Access content deemed illegal, immoral, unethical, pornographic, offensive, fraudulent, among others.

The Technology Solutions area may block access to some Internet pages for users, user groups, or to all employees of the organisation in order to comply with acceptable security and use policies in force.

1. Secure internet connection

Internet access traffic through Deloitte Portugal's internal network must be filtered and authorised by means of existing corporate firewalls.

Whenever an employee needs to access the internet through their laptop computer, outside Deloitte Portugal's network, they shall not change or disable the firewall settings of the laptop.

Access to the Internet network should be by means of trusted networks, duly identified and following the best security practices:

• If it is a Wi-Fi network, it must use an encryption protocol, preferably WPA-2;

• Do not use public Wi-Fi networks that do not use any security protocol;

• Whenever possible, the use of any public Wi-Fi networks at hotels or airports should be avoided;

• Whenever possible, access outside Deloitte should be by means of the smartphone hotspot.

1.11 Social engineering

Deloitte Portugal's employees may not disclose confidential customer or corporate information, contacts or other employee information to unknown third parties without prior authorisation by the CISO. If the employee has doubts about the authenticity of the phone call, email or other communication, they should seek guidance and notify PT Security (ptsecurity@deloitte.pt).

Deloitte's employees should not provide their user name through any email link, phone call or other method until the person requesting such information is positively identified and the need to obtain this information is verified.

Users shall not provide their password to third parties inside or outside the firm. If this information is requested through a telephone call, email or other form of communication, the user should communicate this security event to PT Security (ptsecurity@deloitte.pt) as soon as possible.

1.12 Cloud Services

It is forbidden to send information from the company or clients to Cloud services, whether for information sharing, infrastructure or other services, without the suppliers of these services and/or their app solutions being expressly approved and authorised by Deloitte Portugal.

1.13 Information transfer or sharing

Deloitte Portugal's confidential information must be adequately protected when transferred between employees, clients or authorised external entities.

Thus, it is not allowed:

- The use of software or services for information sharing that are not authorised by Deloitte;
- The sharing of information, using USB pen or external disks, if they are not encrypted;
- File transfer via FTP (File Transfer Protocol);
- Other services, devices or media without being duly authorised by Deloitte.

Confidential customer information transfer channels in digital format or in print to authorised third parties shall ensure, wherever possible, the existence of control mechanisms that protect information against unauthorised interception, copying or modification, alteration of route or accidental or intentional destruction.

Whenever possible, approved encryption mechanisms should be used in the digital transfer of confidential customer information and software, regardless of the communication channel used and the authorised third party.

Agreements should be established for the transfer of confidential customer or software information to authorised third parties addressing:

- Responsibilities for the control and notification of its transmission/dispatch and delivery/reception;
- Responsibilities and obligations in the event of any information security incident;
- The techniques used for the correct identification by both parties as to the level of security of the contents to be transferred, seeking to establish common practice points regarding their transmission and reception;
- The techniques used to protect other sensitive items to be transferred, namely encryption keys;

- The procedures used to ensure the screening of all transmission and reception process stages and its non-rejection;

The minimum safety rules for packaging, if applicable, and transmission.

1.14 Third party access to the Deloitte network

Access to Deloitte's local networks should preferably be done by equipment owned by the firm. However, in exceptional and duly justified cases, it is allowed to connect by cable to the local networks of Deloitte Portugal's buildings, of equipment owned by external entities or service providers, exclusively for the performance of outsourced functions, after being duly verified and approved by the IT department, in accordance with the System Access Control Policy (see chapter 22 in this document).

Clients and visitors are allowed to connect to the internet through the "GuestDNET" wireless network, and the access key must be requested at Deloitte Portugal's reception.

1.15 Connection of Deloitte's equipment to third-party networks

Computers provided by Deloitte Portugal may, with the prior approval of LCSP and client, connect to the Client's IT infrastructure and resources with the Client and Partner approval.

Software can be installed and set up, for remote access to customer networks, on Deloitte's computers, when duly authorised by the client and authorised by the IT area.

Site-to-Site VPN settings between Deloitte and customer networks is allowed, when duly authorised and configured by Deloitte's and Customer IT area. Deloitte's network should be a network designed for this purpose and not Deloitte's internal network.

1.16 Access control systems

1. External Entities (long-term)

Deloitte Portugal's external entitles (temporary personnel, subcontractors, external suppliers, etc.) should only be granted access to the network, systems and business support applications, according to the function they will perform regarding the contract with Deloitte Portugal, and only for the necessary time.

Access by external entities should require the execution of a formal confidentiality agreement.

There shall be a person responsible for the external entity at Deloitte Portugal who must request, justify and approve:

- The allocation of access to the external entity and the necessary time;
- The change in the period during which the external entity needs such access;
- The timely exclusion of accesses as soon as the contract ends with the external entity.

Cable connection to the local networks of Deloitte Portugal's buildings is allowed, with equipment owned by external entities and exclusively for the performance of their duties, after being duly verified by the IT team, in order to guarantee the minimum network access requirements, namely:

- The minimum version of the Operating System must conform to the version used in Deloitte Portugal's PCs or higher;
- The Operating System must have the latest security updates installed;
- Properly updated antivirus software installed;

- Respect the access process to the local network in force.

2. External Entities (sporadic interventions in support and maintenance)

Deloitte Portugal's external entities, which fall into the category of IT service providers who need to make sporadic interventions for periodic maintenance of systems or troubleshooting support, should only be granted access to the network, systems and business support applications, according to the functions they will perform, pursuant to the contract with Deloitte Portugal, and only for the necessary time.

Access by external entities should require the execution of a formal confidentiality agreement.

There shall be a person responsible for the external entity at Deloitte Portugal who must request, justify and approve:

- The allocation of access to the external entity and the necessary time;
- The change in the period during which the external entity needs such access;
- The timely exclusion of accesses as soon as the contract ends with the external entity;
- Establishment of a confidentiality agreement.

In addition, whenever supplier intervention is necessary, the following principles must be guaranteed:

- Agree with the supplier regarding the need for the intervention to be performed as well as the intervention period;
- Reactivate the external entity’s account for this period, when the intervention ends, the account must be immediately deactivated;
- The work to be carried out by the supplier must be accompanied by the IT staff member in charge of the intervention.

Cable connection to the local networks of Deloitte Portugal's buildings is allowed, with equipment owned by external entities and exclusively for the performance of their duties, after being duly verified by the IT team, in order to guarantee the minimum network access requirements, namely:

- The minimum version of the Operating System must conform to the version used in Deloitte Portugal’s PCs or higher;
- The Operating System must have the latest security updates installed;
- Properly updated antivirus software installed;
- Respect the access process to the local network in force.

1.17 Clean desk policy

When a Deloitte Portugal’s employee or an external entity is absent from their workstation, all paper documents and all removable data storage devices containing confidential customer information must be removed from the desk and stored in a secure manner, in accordance with the procedures for handling information assets.

This procedure must be followed at Deloitte Portugal’s premises and at clients’ premises where services are being provided.

1.18 Printed information protection policy

Employees must ensure that they take all necessary precautions with printed information in their possession, preventing unauthorised access by third parties, namely:

- Whilst at Deloitte Portugal's premises/clients' premises/hotels/public places:
    - Documents printed with customer information must be kept in a locker or safe if they are not being used or supervised by the employee who keeps them;
    - Printed and unused documents or documents found on printers must be disposed of safely in accordance with current asset handling procedures.

- On vehicles:

    - Documents printed with customer information should not be left on any vehicles.

- On airplanes:

    - Printed documents with customer information taken on trips cannot be dispatched as hold baggage.

- At home

    - Printed documents with customer information should not be left unprotected, and the use of the equipment should be restricted to the user only.

Documents containing confidential customer information must be immediately removed from printers, fax machines and photocopiers.

In order to prevent the exposure of confidential customer information to unauthorised persons, a personal code system is implemented in printers to access this equipment.

Paper information must be destroyed safely in accordance with the asset management procedure in effect.

1.19 Copyrights

As per the commissioned work system, all intellectual creations directly or indirectly related to Deloitte's activities, namely inventions, ideas, studies, developments and improvements made by Deloitte Portugal's employees, as well as any media, are the exclusive intellectual property of Deloitte. Employees shall not be entitled to any remuneration or additional compensation due to such fact.

1.20 Return of company assets

Employees shall deliver to Deloitte Portugal, and until the contract termination date:

• Any asset (physical equipment and software licences), owned by Deloitte Portugal, and assigned to them for the performance of their duties;

• All work materials, documents, information and data in their possession, whatever the media they may contain, concerning Deloitte, its clients and suppliers, or that constitute Deloitte's intellectual property or know-how.

2 Cryptographic Control Policy

2.1 Cryptographic Control Policy

Any information that is shared via web services on Deloitte's internal network should, whenever possible, be the subject to encryption. For example: TLS, HTTPS or SFTP.

All and any information that is available externally (internet) from internal sites of the company should be subject to encryption.

Mechanisms that allow for the creation of secure communication channels should be provided for the transmission of information between Deloitte Portugal's devices and the company's internal network infrastructure, when accessed from the Internet.

In the specific case of confidential customer information transmitted externally through electronic mail, this should be encrypted, whenever possible, by using mechanisms or techniques approved and identified in the Acceptable Use Policy of the company's assets.

System and user passwords when transmitted over the network or saved in digital format must be protected using cryptographic techniques, in which case the use of non-reversible algorithms (hash) is recommended.

Data transmitted over wireless networks must be encrypted by cryptographic mechanisms that implement the SHA-256 algorithm.

The access for administrative management of systems should resort, whenever possible, to the SSH protocol, with 1024-bit keys, at least. Those devices that do not allow for implementing SSH, shall not be allowed remote access and their management must be done through local management.

The use of digital certificates requires that the issuing certification body be previously approved by Deloitte Portugal.

If required by law, regulation or contract, data must be encrypted in accordance with these specific requirements, after approval of Deloitte Portugal.

Cryptographic keys and other secret information (passwords) will be safeguarded according to the type of service in question. These services and the needs to protect this information will be formalised in ISMS documented information of reserved access.

Safe procedures and methods deemed necessary for the life cycle management of the cryptographic keys in a production context must be formalised. From the cycle phases to evaluating the relevance of formalisation, the following actions take place:

- Generation of keys for different encryption systems and applications;
- Issuance and delivery of public key digital certificates;
- Distribution of keys;
- Safeguarding of keys;
- Changing or updating keys;
- Removal of keys;
- Recovery of lost or corrupted keys;
- Safeguarding and archiving of keys;
- Destruction of keys.

2.2 Glossary

- SFTP – Secure File Transfer Protocol
- SHA – Secure Hash Algorithm
- SMIME – Secure /Multipurpose Internet Mail Extensions (secure email)
- SSH – Secure Shell
- TLS - Transport Layer Security

3 Information Asset Handling Procedures

3.1 Protection of confidential customer information

1. Information in digital format

All confidential customer information should be stored in Deloitte Portugal's central repositories. Confidential customer information outside Deloitte Portugal's central repositories, particularly on laptops, desktops or other mobile devices, should be restricted to absolutely necessary and for a very short time span. Users shall ensure the reproduction or transfer of this information from devices under their responsibility to the central repositories of the company. Only after information is copied or transferred will the user be able to delete it from their devices.

It is now allowed to save confidential customer information on external systems not authorised by Deloitte Portugal.

Regarding the services rendered to the company, saving engagement supporting information may occur in other equipment and systems that the Client expressly authorises in writing. Prior approval of the engagement partner is necessary.

2. Information in physical format

All confidential customer information should always be stored in proper places in order to mitigate non-authorised access risks by third parties. Whilst at any Clients' premises for the rendering of corporate services, the same principle shall be applied expressly requesting the availability of appropriate measures to the Client.

Whenever not in use, confidential customer information should be stored in places or compartments that have access control ([1]).

All confidential customer information in physical format should be converted, whenever possible, into digital format by using internal "Scanning" services provided by the Office Administration department. After scanning such information, the responsible party must evaluate the relevance and possibility ([2]) of its safe deletion.

3.2 Use and processing of confidential customer information

1. Information in digital format

The use and processing of customer confidential information is only allowed in applications, equipment and systems owned by Deloitte Portugal or others expressly pre-approved by the company or by the Client.

The printing of confidential customer information should be restricted to absolutely essential. Special care should be taken when printing this information, including:

- Being near the printing machine while confidential documents are being printed;
- Safely deleting any pages that do not conform to the desired result and require reprinting;
- At the end of the printout, make sure that all printed sheets are collected.

[1] Examples: Floor archives, individual or project locker, room with key at the Client's premises.

[2] Attention: For legal reasons (evidence), the original document may need to be maintained.

2. Information in physical format

The use and processing of confidential customer information is only allowed at Deloitte Portugal's premises or at other premises, for the provision of customer services.

3.3 Shipment and Sharing of Confidential Customer Information

1. Information in digital format

The sharing of confidential customer information by means of external systems ([3]) not authorised by Deloitte is forbidden, and the guidelines set forth in Chapter 1.13 - Information transfer or sharing, shall be followed.

2. Information in physical format

Whilst at the company's premises, the sharing of confidential customer information between employees or authorised third parties requires delivery of such information by hand.

The submission and shipment of confidential customer information to external entities through the use of postal or courier services requires that this information, as a minimum:

- Be enclosed in a Deloitte's envelope with the full address of the recipient, the name of the final recipient and the word "Confidential";
- This envelope must be placed inside an unidentified envelope with the full address of the recipient, the name of the final recipient and the postal stamp or other information necessary for the shipment, if necessary;
- Be sent by external mail, courier services or by duly authorised personnel.

That the information is permanently under personnel's supervision or protection.

3. Information in oral form

Sharing confidential customer information with family members, friends, or other staff members not directly related to the matter is forbidden.

Sharing confidential customer information in an oral form shall not occur in public spaces (e.g. elevators, means of transportation, restaurants, etc.).

3.4 Deletion of confidential customer information

1. Information in digital format

Copies of confidential customer information should be deleted in accordance with the following rules:

- Equipment or mobile devices in use - deleted by the user, when they are no longer needed; the user is responsibile to copy or move the information from those devices to the firm central repositories before elimination;
- Equipment for reuse or rebate - are subject to deletion/destruction in accordance with pre-established procedures to be performed by the IT.

[3] Examples: FTP Servers, Dropbox, Wetransfer, GoogleDrive, iCloud.

2. Information in physical format

Copies of confidential customer information in physical format, when no longer required, must be destroyed by using a shredder ([4]) or placed in paper shredding containers.

[4] Minimum cross-cutting capacity or safety level P-3 - DIN 66399 = ≤2 mm wide and any length or particles ≤320 mm² (any width)

Deloitte.