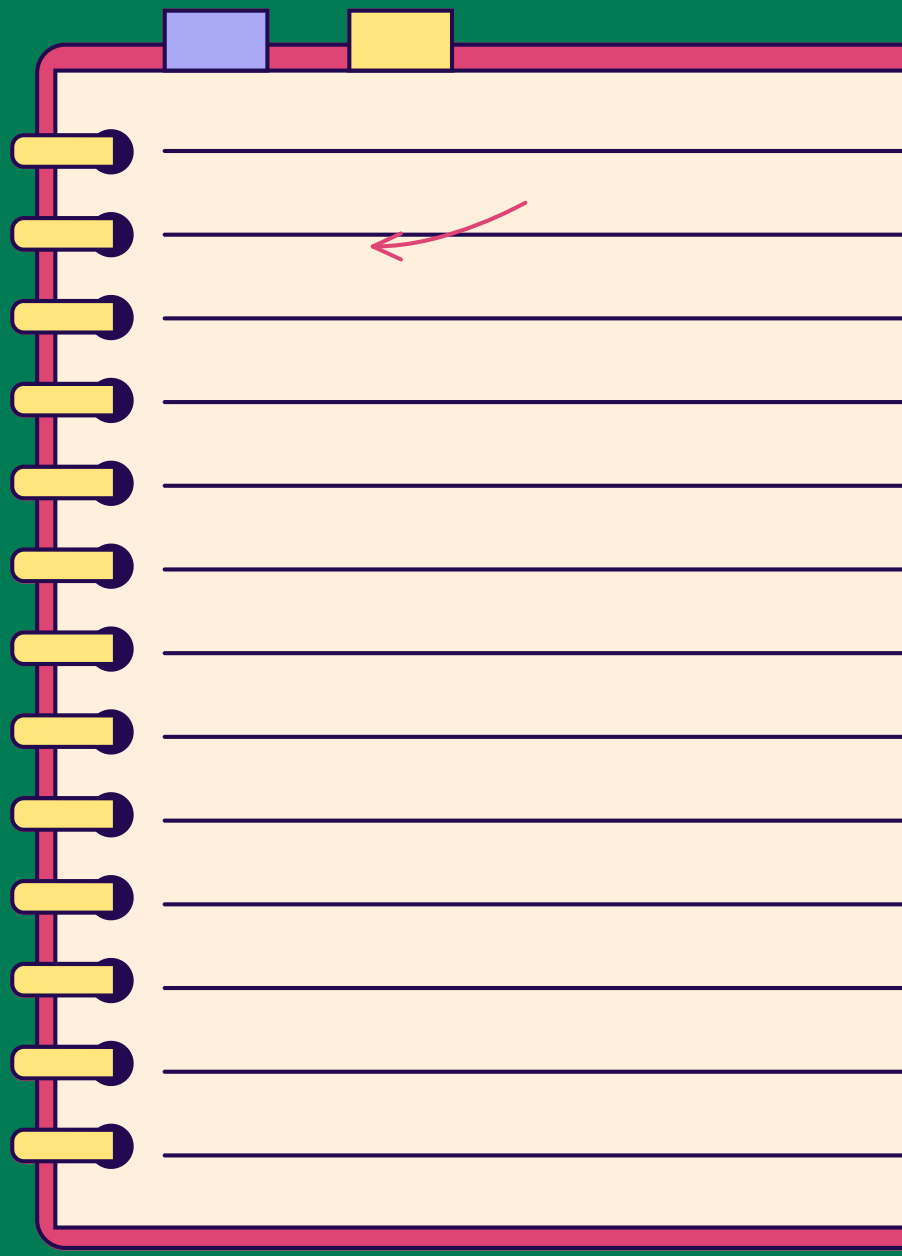
MODULE 5 - MANAGING, STORING AND RETRIEVING YOUR DATA

CHAPTER 1

STORING YOUR DATA

Skills to Connect



INTRODUCTION

In an ever-changing digital world, effective data management has become a crucial necessity for both individuals and businesses.

This chapter of Module 5 addresses the fundamental issue of storing, securing, and retrieving personal and business-related data.

We will explore the various methods and technologies available to securily store data and easily access it, such as cloud and hard drives.

This guide will provide you with the knowledge you need to choose the best storage solution for your specific needs, while ensuring your information remains protected and under your complete control.

1 STORING YOUR DATA

WHERE AND HOW TO SAVE YOUR DATA

Personal data is any information relating to an identified or identifiable person. But, because they concern people, they must retain control over them.

A person can be identified:

- directly (example: first and last name);
- indirectly (example: by a telephone number or license plate, an identifier such as a social security number, a postal or email address, but also voice or image).

The identification of a person can be carried out:

- from a single piece of data (example: name);
- from the cross-referencing of a set of data (example: a woman living at such an address, born on such a day and member of such an association).

However, company contact details (for example, the company “Company A” with its postal address, its switchboard telephone number and a generic contact email “company1[@]email.fr”) are not, in principle, personal data.
Source: CNIL, https://www.cnil.fr/fr/definition/donnee-personnelle

1 STORING YOUR DATA

WHERE AND HOW TO SAVE YOUR DATA

ON A CLOUD

The cloud is an online storage space. You save your files on remote servers accessible via the Internet.

PROS:

- Accessible from anywhere with an internet connection.
- Often secured with automatic backups.
- Space-saving (no physical hardware required).

CONS:

- Requires an internet connection to access your data.
- May have a cost (monthly or annual subscription).

Exemples de services cloud : Google Drive, Dropbox, OneDrive, ICloud, ...

ON A HARD DRIVE (EXTERNAL OR INTERNAL)

A hard drive is a physical storage device that you connect to your computer.

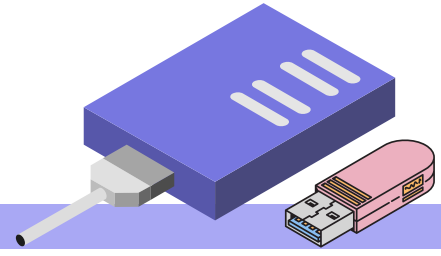
PROS:

- Quick access without the need for an internet connection.
- You have complete control over your data.
- Can store large amounts of data.

CONS:

- Risk of loss or physical damage (fall, fire, etc.).
- Less convenient for remote access.

Examples of hard drives: USB external hard drive, SSD (Solid State Drive).



1 STORING YOUR DATA

WHERE AND HOW TO SAVE YOUR DATA

WHAT TO CHOOSE? CLOUD OR HARD DRIVE?

VIDEO TUTORIAL

Find out how to store & backup your data with a Cloud or a hard drive.

2 STORING YOUR DATA

HOW TO SECURE YOUR DATA?

Securing your digital data is essential to protect your privacy, avoid identity theft, and prevent unauthorized access to personal or sensitive information. It also reduces the risk of financial loss or malicious exploitation of your data. Here are some simple steps you can take to secure your data:

1 - USE STRONG PASSWORDS:

MODULE ALERT

To find out more, go to module 1 which explains how to choose a good password!

- Choose complex passwords (letters, numbers, symbols) and unique for each account.
- Use a password manager to help you manage them.

A password manager is an essential tool for maintaining password security and organization, especially when following the recommendation to create complex and unique passwords for each account. Here are the two key aspects of what a password manager does:

SECURE STORAGE:

Password managers allow you to store all your passwords in a centralized location that is secured by a master password. The master password is the only password you need to remember. The data stored is often encrypted, meaning it cannot be read without the master password.

2 STORING YOUR DATA

HOW TO SECURE YOUR DATA?

PASSWORD GENERATION AND RECOVERY:

A password manager can also generate random, complex passwords for you that use a combination of letters, numbers, and symbols, in line with security best practices. When you need to access an account, the manager can automatically fill in the password for you, eliminating the need to remember it or type it manually.

2 - ENCRYPT YOUR DATA:

- Encryption transforms your data into a format that is unreadable without a decryption key. Many cloud services offer this option.
- On a hard drive, you can use software like VeraCrypt to encrypt your files.

2 STORING YOUR DATA

HOW TO SECURE YOUR DATA?

WHAT IS THE DATA ENCRYPTION PROCESS?

Data encryption is a bit like putting your information in a secure vault.
This process involves transforming data into an unreadable format, called “ciphertext,” so that only people with the correct key can read it.

HOW DOES IT WORK?

Encryption uses a key, much like a very complex password, to "encode" data. Without this key, no one can understand the contents.

Here's how it works in practice:

- Data transformation: When we encrypt data, we apply an algorithm (a kind of mathematical formula) that mixes and transforms the original information into a sequence of incomprehensible characters.
- Using a key: This “mixing” is guided by a unique encryption key. This key is like a safe key: it is needed to be able to decrypt (or read) the encrypted data.

2 STORING YOUR DATA

HOW TO SECURE YOUR DATA?

WHY IS IT USEFUL?

Encryption protects your sensitive information from unauthorized access. Even if someone intercepted your data, they wouldn’t be able to do anything with it without the key.

HOW TO DO DATA ENCRYPTION IN PRACTICE?

On your computer or in the cloud, you can use software like VeraCrypt to encrypt your files. In cloud services, some encryption options are built in, but you can also create your own passwords or keys to increase security.

To illustrate encryption in concrete terms, here is an example of a simple cipher, called the Caesar cipher. It is a type of substitution cipher that is perfect for understanding the concept.

2 STORING YOUR DATA

HOW TO SECURE YOUR DATA?

CAESAR CIPHER

Suppose you want to encrypt the word "CAT" using a shift of 3.

- Step 1: Set the key
- In this example, the key is "shift by 3". This means that each letter will be replaced by the letter that is 3 positions further down in the alphabet.
- Step 2: Apply the offset
- We apply the shift of 3 to each letter of the word "CAT":
  - C becomes F
  - A becomes D
  - T becomes W
- So, "CAT" becomes "FDW" after encryption.
- Step 3: Decrypt with the key
- To find the original word, simply shift each letter 3 positions in the other direction:
  - F becomes C again
  - D becomes A again
  - W becomes T again

When deciphering, we find "CAT".

2 STORING YOUR DATA

HOW TO SECURE YOUR DATA?

3 - MAKE REGULAR BACKUPS:

- Don’t keep all your data in one place. Make copies on a hard drive and in the cloud to minimize the risk of loss.
- Schedule automatic backups if possible.

4 - UPDATE YOUR SOFTWARE:

- Keep your operating system and software up to date to benefit from the latest security protections.

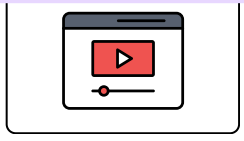
MODULE ALERT

To learn more, go to module 1 which explains how to update your devices & install an antivirus

5 - USE AN ANTIVIRUS:

- Install and keep up-to-date antivirus software to protect against malware and other threats

VIDEO TUTORIAL



Learn how to better secure your files on the Cloud

TO REMEMBER!

To manage your data well:

- Store them on the cloud for remote access and security.
- Use a hard drive for local backups.
- Secure your data with strong passwords, encryption, and up-to-date software.
- Make regular backups to avoid losses.