



Data protection is not only a legal obligation, but also a strategic issue for customer trust and the sustainability of your business. This checklist has been designed to help you quickly assess your organization's maturity in terms of data security.

**Check Yes, Partially, or No for each action to identify your strengths and areas for improvement.**

The goal: to implement simple, effective practices that are tailored to your reality.

Yes	Partially	No
-----	-----------	----

## Data awareness

Are you familiar with the legal requirements for data processing in your industry?			
Have you identified personal data (name, email, address)?			
Have you identified confidential data (financial information, customer files)?			
Have you mapped the location of this data?			
Have you defined sensitivity levels for each type of data?			
Have you assessed the relevance of retaining this data?			
Have you defined the retention period and location for each type of data?			

## Access security

Are strong passwords mandatory?			
Is two-factor authentication (2FA) enabled on accounts (email, software, data access)?			
Are access rights controlled according to the principle of least privilege?			
Is access reviewed regularly (ideally every quarter)?			

## Physical protection

Do screens lock automatically after a period of inactivity?			
Are passwords enabled on computers and mobile devices when they come out of sleep mode?			
Are employees aware of the "Clean Desk" policy (no sensitive documents left on desks)?			
Is physical access to servers protected?			
Are network ports limited and controlled?			

## Device management

Is there a process in place for the secure destruction of data prior to recycling or donation?			
Is there a policy in place regarding the use of personal devices (BYOD)?			
Is there a policy in place regarding the use of work devices?			

## Backup and encryption

Are regular backups of critical data performed?			
Are backups encrypted?			

## Awareness and culture

Have employees received training on data security?			
Are employees aware of data categories and best practices?			
Do managers set an example in terms of security?			