Plàstics Dertosa

ICT Security Plan

Co-funded by the
Erasmus+ Programme
of the European Union

Security in ICT

Erasmus+

Contents

1. Our training firm: Plàstics Dertosa
2. Current state of the security environment
3. Security measures and control

1. Plastics Dertosa: our simulated company

- Since October 2002,
- Design and manufacture of furniture
- High quality and functionality

PD: our simulated company

Plastics Dertosa: simulated company in Institut de l'Ebre (Tortosa):

- Managed by students of business administration and finance
- Work environment
- Working relationships
- Learning and training of situations, tasks and processes: active methodology with a clearly professional component
- Learning by doing, learning by working

PD: how it works

- A constant desire to innovate
- Our motto: “*Feel our creativity in the atmosphere*”
- Our collection: multifunctional and transversal
- Colour, transparencies and unique shapes for unique objects
- Emotion, functionality and quality
- Continuous evolution in the use of materials
- Experimentation with new technologies

PD: business culture

	In business	In our training firm
MISSION	Manufacture of plastic furniture for different spaces	Real working situations (SEFED Project - Inform Foundation)
VISION	Desire to innovate Benchmark in decoration of everyday spaces	To train future entrepreneurs in administrative and business management tasks
VALUES	Innovation, transnationality, networking, teamwork, responsibility, organisation at work, initiative, autonomy and interpersonal relationships	

Erasmus+

PD: departments

- Reception
- Human Resources Department
- Purchasing Department
- Sales and Marketing Department
- Accounts Department
- Financial Department

2. Current state of the security environment

- Insecure passwords. (email, internet banking)
- Loss of data (digital folders, factusol, nominasol, contasol)
- Download damaged files. (quotations and invoices, spam)
- Insecure network. (software: virtual city, factusol, nominasol, contasol, internet banking)
- Hacking / phishing. (virtual city, online transactions)

Security in ICT
Erasmus+

Insecure password

Need of secure passwords for:

- personal information
- internet banking
- e-mails
- online communication
- ...

Loss of data

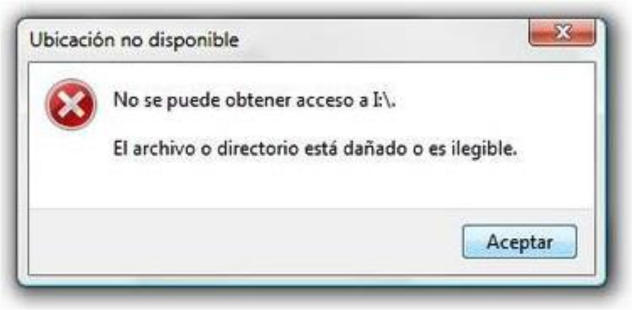
Different types of documents with important data:

- Contracts and agreements
- Invoices
- Files in applications
- ...

Hackers can steal or destroy them with viruses

Security in ICT
Erasmus+

Download damaged files



Ubicación no disponible

No se puede obtener acceso a I:\.

El archivo o directorio está dañado o es ilegible.

- Free apps: danger of infestation
- Ransomware or spyware: check/skim computer for passwords and private information

What is a Trojan?

“Trojan”: a type of malware often camouflaged as legitimate software.

Cyber drunks and hackers can use Trojans to try to access users' systems.

What can a Trojan do?

1. Data deletion
2. Data lock
3. Data modification
4. Data copy
5. Interruption of the performance of computers or networks

Unlike viruses and computer worms, Trojans cannot multiply.

I have suffered a cyberattack, what can I do?

- One solution: Turn off the infected computer and all the devices that are interconnected to it.
- Recommended: Disconnect the infected devices from the network

What is phishing?

Phishing: fraudulent method to catch personal data using a false identity on the Internet is punished.

- Passwords
- Credit card information
- Bank account numbers, ...

Phishing in PD

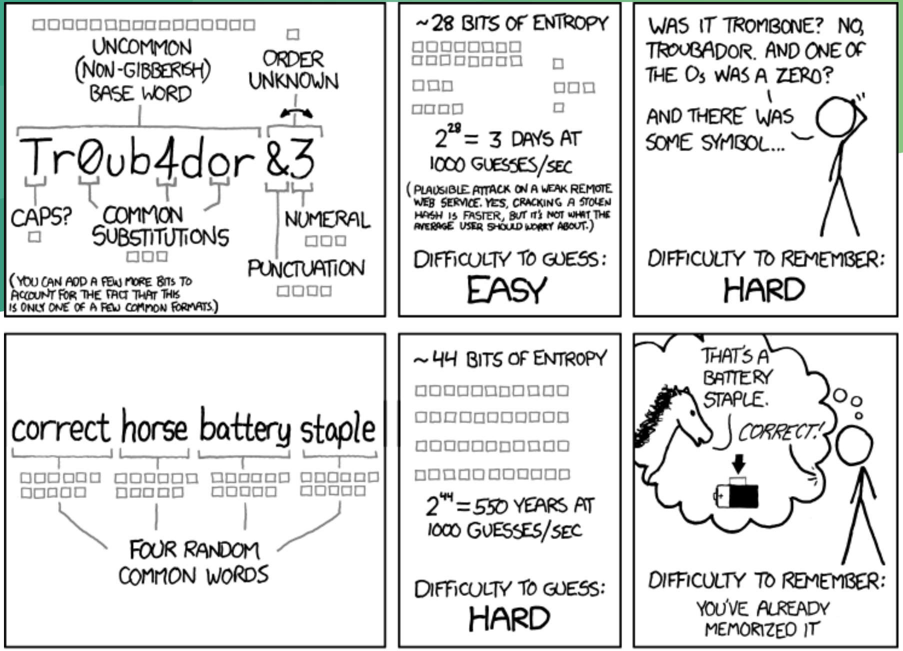
Virtual city: products and stock transactions

Danger: e-mails and bank account can be hacked, loss of money

3. Security measures and control

Insecure passwords?

- Reduce unnecessary passwords.
- Avoid short passwords that can be obtained easily (your pet's name, dates, postal codes, ...)


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44} = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

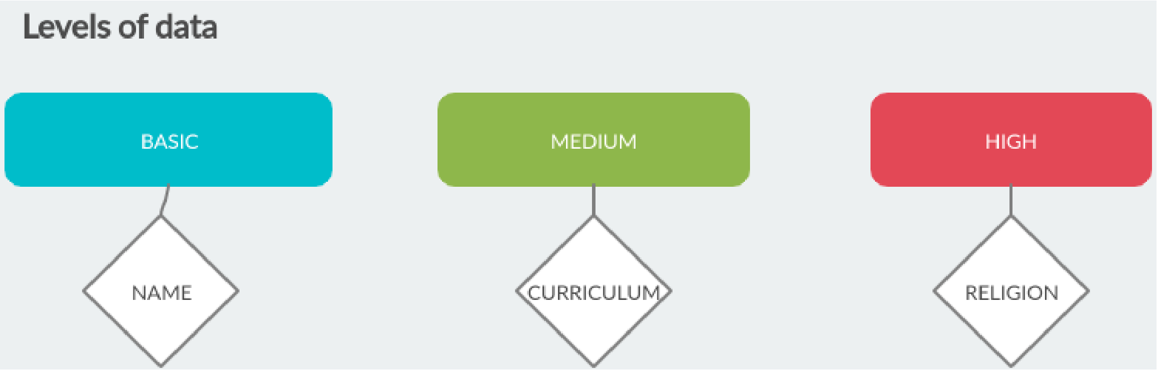
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Easy to remember but difficult to guess.

How can we prevent data loss?

- Make regular backup copies:
  - different devices
  - media
- Use robust encryption systems: to prevent others from reading it.

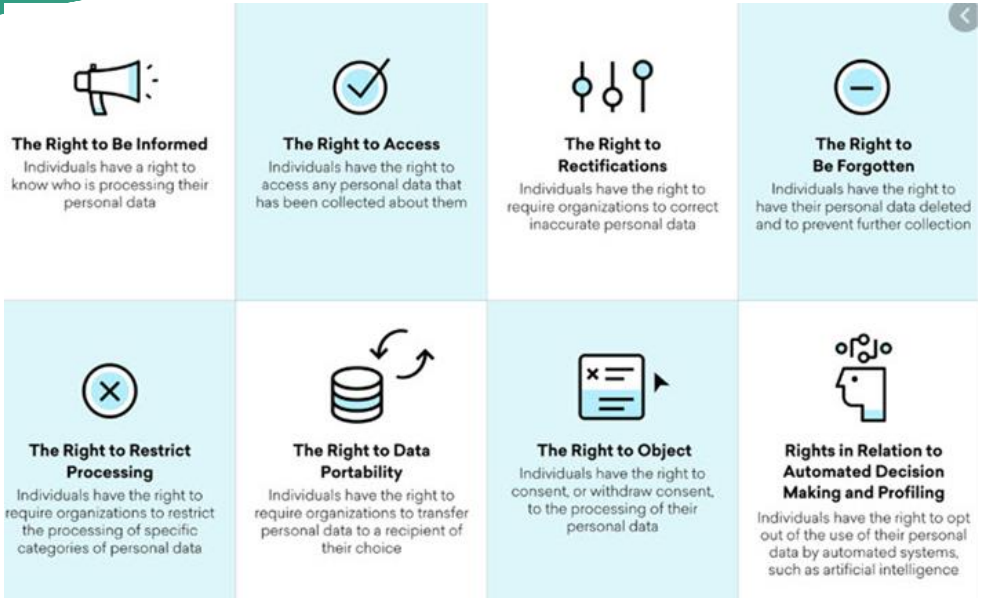
How can we manage our data?



Levels of data

GDPR
General Data Protection Regulation

Users rights by the GDPR?



The Right to Be Informed
Individuals have a right to know who is processing their personal data

The Right to Access
Individuals have the right to access any personal data that has been collected about them

The Right to Rectifications
Individuals have the right to require organizations to correct inaccurate personal data

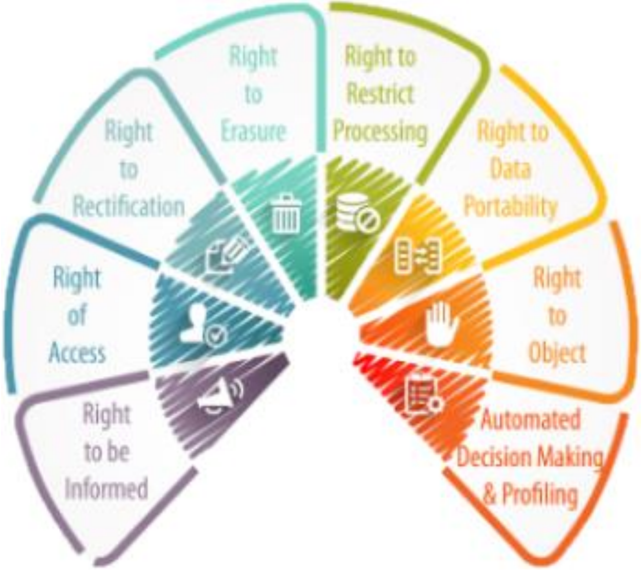
The Right to Be Forgotten
Individuals have the right to have their personal data deleted and to prevent further collection

The Right to Restrict Processing
Individuals have the right to require organizations to restrict the processing of specific categories of personal data

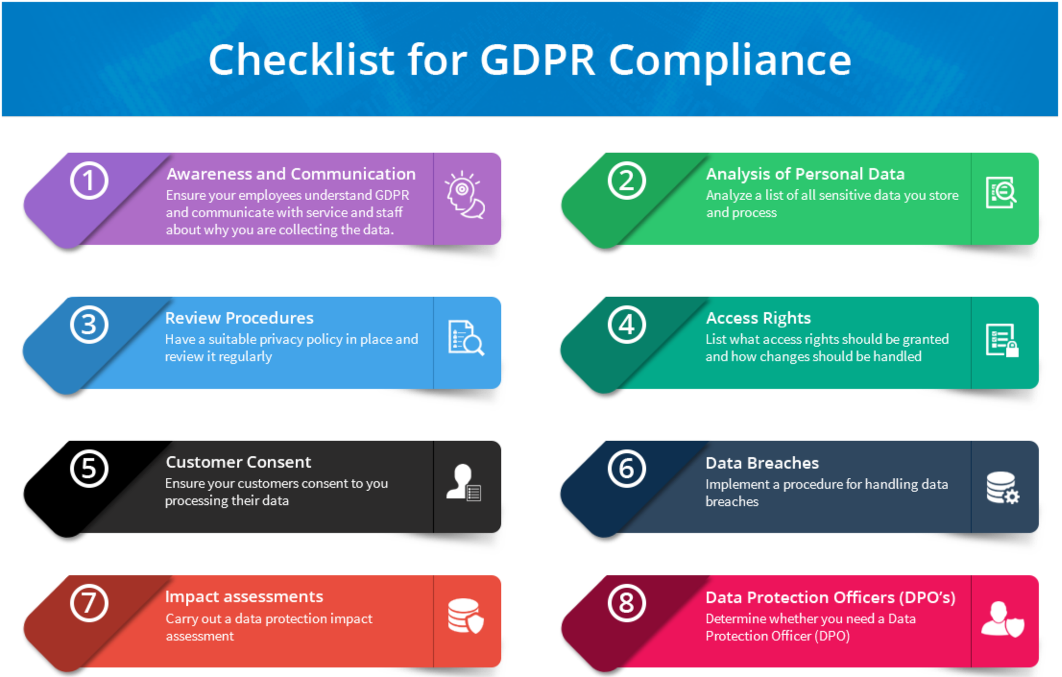
The Right to Data Portability
Individuals have the right to require organizations to transfer personal data to a recipient of their choice

The Right to Object
Individuals have the right to consent, or withdraw consent, to the processing of their personal data

Rights in Relation to Automated Decision Making and Profiling
Individuals have the right to opt out of the use of their personal data by automated systems, such as artificial intelligence

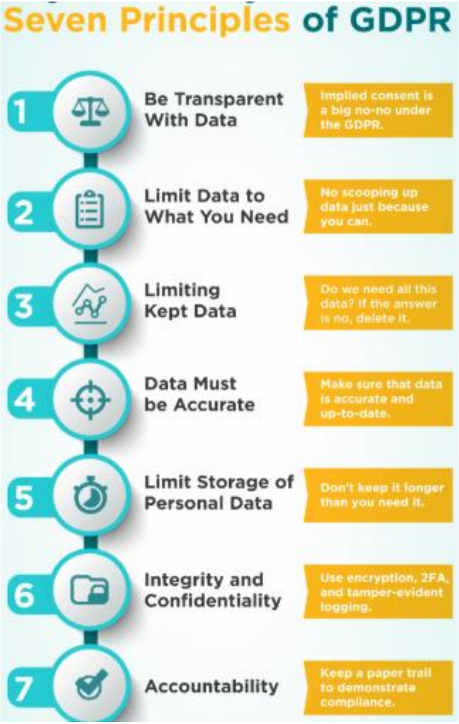

Right to Erasure
Right to Restrict Processing
Right to Rectification
Right to Data Portability
Right of Access
Right to Object
Right to be Informed
Automated Decision Making & Profiling

GDPR?



Checklist for GDPR Compliance

1. **Awareness and Communication** Ensure your employees understand GDPR and communicate with service and staff about why you are collecting the data.
2. **Analysis of Personal Data** Analyze a list of all sensitive data you store and process
3. **Review Procedures** Have a suitable privacy policy in place and review it regularly
4. **Access Rights** List what access rights should be granted and how changes should be handled
5. **Customer Consent** Ensure your customers consent to you processing their data
6. **Data Breaches** Implement a procedure for handling data breaches
7. **Impact assessments** Carry out a data protection impact assessment
8. **Data Protection Officers (DPO's)** Determine whether you need a Data Protection Officer (DPO)



Seven Principles of GDPR

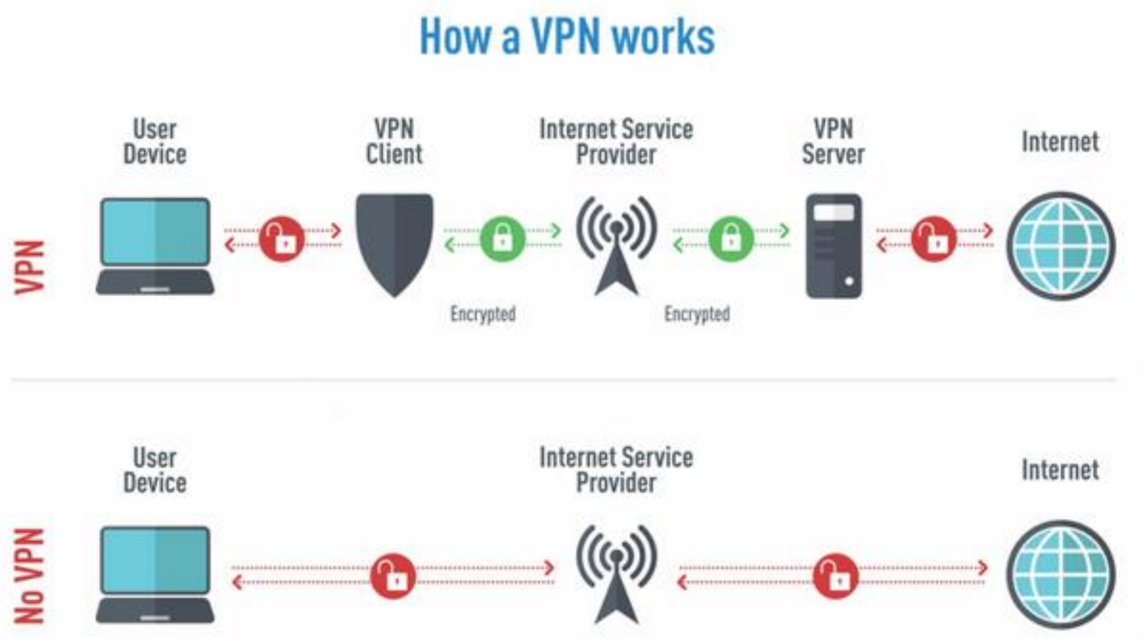
1. **Be Transparent With Data** Implied consent is a big no-no under the GDPR.
2. **Limit Data to What You Need** No scooping up data just because you can.
3. **Limiting Kept Data** Do we need all this data? If the answer is no, delete it.
4. **Data Must be Accurate** Make sure that data is accurate and up-to-date.
5. **Limit Storage of Personal Data** Don't keep it longer than you need it.
6. **Integrity and Confidentiality** Use encryption, 2FA, and tamper-evident logging.
7. **Accountability** Keep a paper trail to demonstrate compliance.

Protect our devices

- Install antivirus software

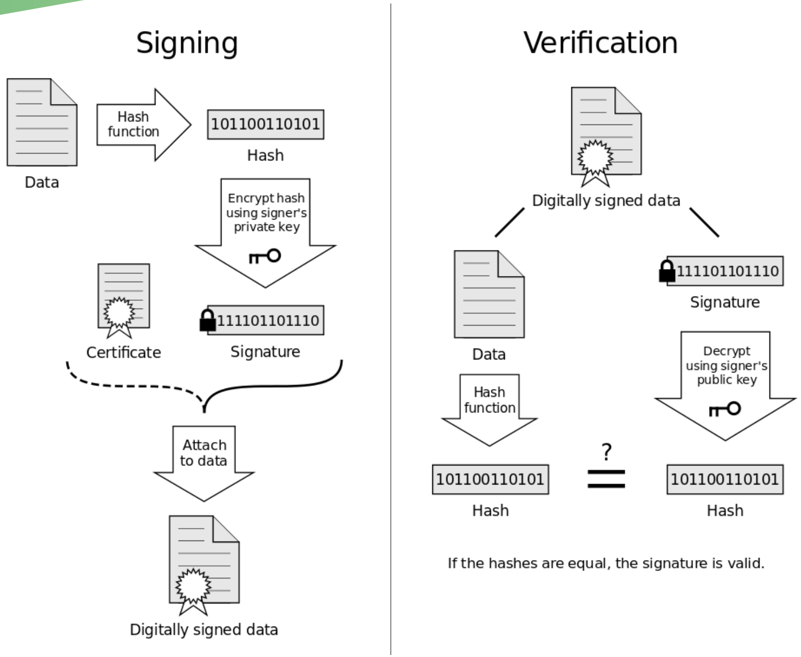
Secure connections

- Create VPN for secure connection
- Use more strict rules on firewall



Digital certificates

- Protect our data bank
- Authenticate our identity



- 95

“ THANKS FOR YOUR ATENTTION!!!

E+

Security in ICT

Erasmus+