



Privacy and data protection

What personal data is and how to handle it well, every day

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Contents

How to use this handout 3

1. What personal data is 3

1.1 Personal data 4

2. Who is who, and the basic rules 5

2.1 The principles in plain words 7

2.2 Why the law matters 9

3. Good practice in the office 9

3.1 Collect and use only the data you need 9

3.2 Documents in view and printers 9

3.3 Blind copy (Bcc) 10

3.4 Check before you send 11

4. Data breach and notifying the Garante 12

4.1 The 72 hours 13

4.2 What falls to you and what falls to the controller 14

Practical exercise 16

Questions that come up in class 17

Glossary 17

Further reading 18

How to use this handout

This handout gathers, in written and ordered form, everything covered in the lesson. You do not need to memorise it: it is there so you can find things again calmly, later, when the lesson is over and a question is left hanging.

> **GOAL**
>
> Understand what the GDPR and the Italian Privacy Code say, recognise personal data, adopt everyday good practice in the office, and know what to do in case of a data breach, including notifying the Garante within 72 hours.

What you will be able to do

- Recognise personal data and tell it apart from special-category data.
- Explain the basic principles of the GDPR in plain words.
- Apply good office practice: necessary data only, documents in view, printers, blind copy.
- Recognise a personal data breach and immediately warn the person who must decide.
- Know the 72-hour deadline for notifying the Garante and who is responsible for doing it.

1. What personal data is

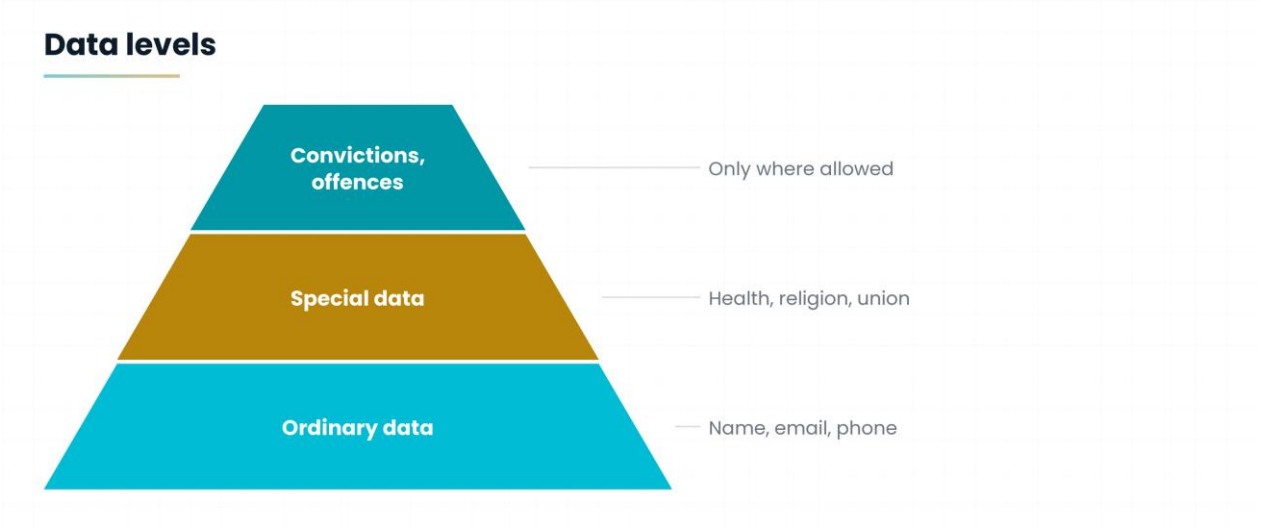
In an office, names, phone numbers, addresses, grades and certificates pass through every day. Every sheet of paper tells something about a real person.

Imagine Marta, who works in the office of Istituto Esempio, a fictional school. A family asks her to email a pupil's record. Marta is in a hurry and types the wrong address. A file with a name, a class and notes about health lands with a stranger. There was no cyberattack, but it is still a privacy breach.

In Europe, **privacy** (the right to confidentiality) is protected by two texts. The first is **Regulation (EU) 2016/679**, known as the **GDPR** (General Data Protection Regulation), valid in every EU member state and applied since 25 May 2018. The second is Italy's **Personal Data Protection Code**, legislative decree 196 of 2003, updated in 2018 to align it with the GDPR. In Italy they apply together.

1.1 Personal data

Personal data is any information about an identified or identifiable natural person. A name is not needed: it is enough that the information lets you work out who the person is.



Three levels of data sensitivity

Type of data	Examples	How to handle it
Ordinary data	Name, address, email, phone, tax code (codice fiscale), photo, number plate	Only what is necessary, with care
Special-category data	Health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sex life or sexual orientation, genetic data and biometric data used to identify a person	Stricter rules: maximum attention
Criminal convictions and offences	Information on criminal convictions and offences	Handled only in cases the law allows

The more sensitive the data, the stricter the rules.



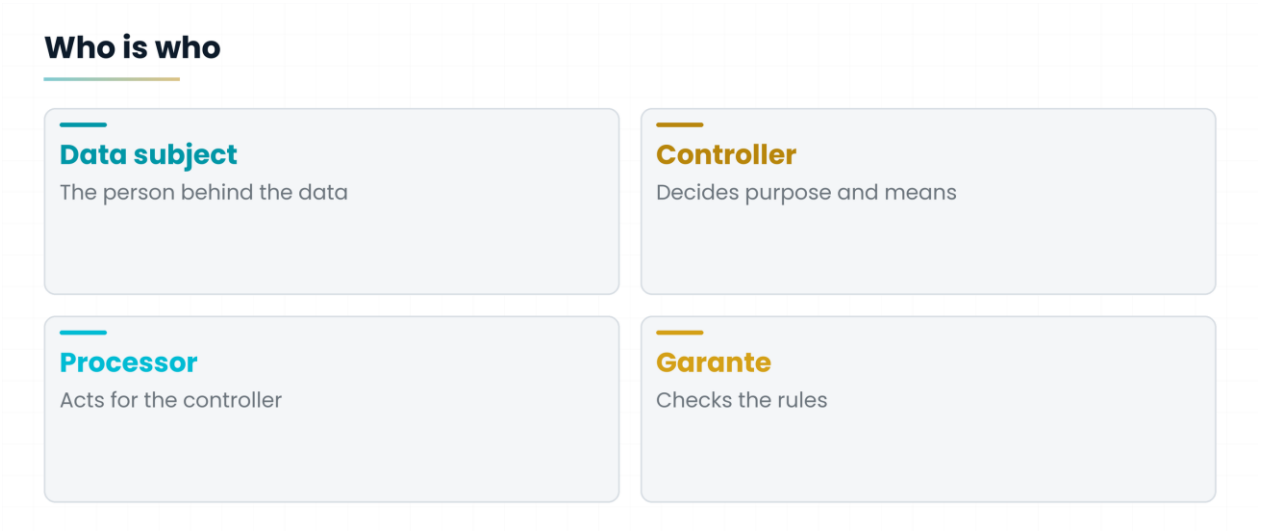
An identifiable piece of information is about a person.

THE IDEA IN ONE LINE

If a piece of information lets you tell who is being talked about, it is personal data and deserves care.

2. Who is who, and the basic rules

The law gives a name to each role. Knowing who is who tells you whom to turn to when something goes wrong.



The roles set out by the law

- **Data subject**: the person the data refers to (the pupil, the client, the patient);
- **Controller**: whoever decides why and how data is used, that is the school, the firm, the company. The controller answers before the law;
- **Processor**: whoever handles data on the controller's behalf, for example the provider of the management software or the cloud;
- **Authorised person**: you, when you work in the office and handle data following the instructions you received;
- **The Garante**: Italy's independent Data Protection Authority (Garante per la protezione dei dati personali), which checks that the rules are followed.



Different roles, different responsibilities.

2.1 The principles in plain words

The GDPR (Article 5) sets a few principles that you can turn into daily habits.

Principle	What it means in practice
Lawfulness, fairness, transparency	Data is used fairly and the person knows what you do with it (privacy notice)
Purpose limitation	You collect data for a specific purpose and do not use it for anything else
Data minimisation	You ask for and keep only the data that is really needed
Accuracy	Data is correct and up to date
Storage limitation	You do not keep it longer than necessary
Integrity and confidentiality	You protect it from unauthorised access, loss and misuse

The basic principles of the GDPR.



A precise purpose, only what is necessary, accuracy, storage time and security.

> **A PRACTICAL CASE: THE NOSY FORM**
>
> A sports club has people fill in a sign-up form that also asks for the parents' jobs and income, for no reason. To enrol a teenager in a course that data is not needed: under the minimisation principle it should not be asked. Removing two lines from the form lowers the risk and the workload.



Ask only for information that is relevant to the purpose.

2.2 Why the law matters

Anyone who ignores the rules risks administrative fines. For the most serious infringements, the GDPR (Article 83) allows fines of up to 20 million euros or, for companies, 4 percent of worldwide annual turnover, whichever is higher. For other infringements, such as those on security and notification duties, the ceiling is 10 million euros or 2 percent. But there is a more concrete reason: behind every piece of data there is a person who can be harmed.

3. Good practice in the office

Most privacy breaches do not come from an attack: they come from a moment of distraction.

3.1 Collect and use only the data you need

Before asking for a piece of data, ask yourself what it is for. If you cannot answer, you probably do not need it. The less data you hold, the less data you can lose.

3.2 Documents in view and printers

A file on the desk, seen by someone passing, is already a small breach. The same goes for sheets forgotten in the printer, which anyone can pick up and read.

- at the end of the day put files away in **locked** cupboards or drawers;
- when you stand up, **lock your screen** with the Windows key and L (we covered it in the lesson on devices);
- after printing, **collect the sheets at once**; if the printer has secure printing with a code, use it;
- for documents to throw away use the **shredder**, not the bin;
- do not leave passwords on sticky notes and do not leave sheets with data on the desk during visits.

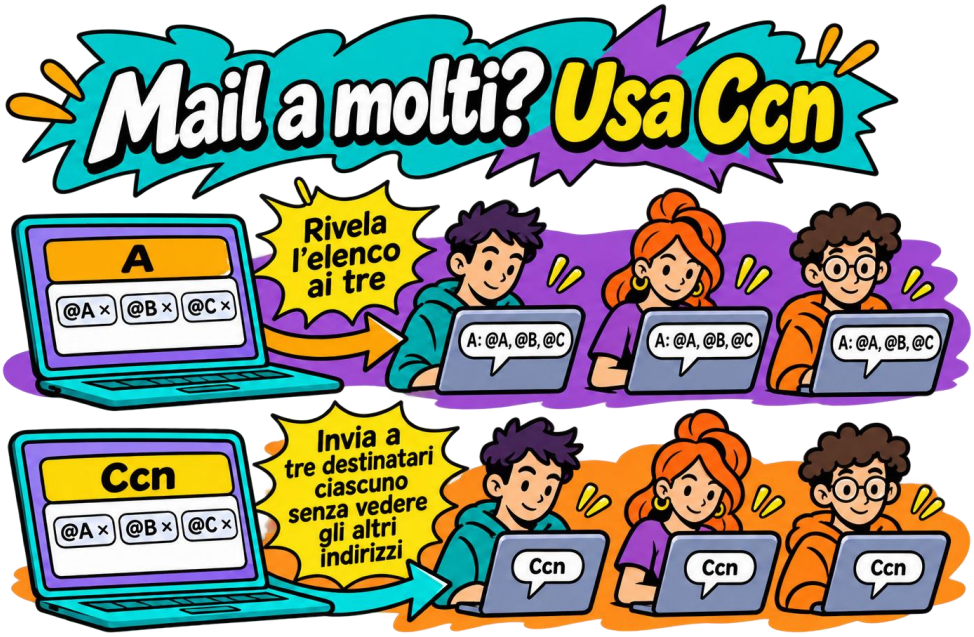


Locked cabinets, locked screens, printouts collected and waste disposed of safely.

3.3 Blind copy (Bcc)

When you email many people who do not know each other, their addresses are personal data. If you put them in the "To" or "Cc" (carbon copy) field, everyone sees everyone's address. Use the **Bcc** field (blind carbon copy; Italian mail programs call it Ccn), which hides recipients from each other.

> **BEFORE AND AFTER**
>
> **Before:** a notice sent to forty parents, with all addresses in the "To" field. Everyone sees everyone else's address.
>
> **After:** the same addresses in the Bcc field. Everyone receives the message, nobody sees the others.



Bcc avoids exposing the addresses of the other recipients.

3.4 Check before you send

Many breaches come from a wrong send: a similar-looking recipient, the wrong attachment. Before pressing send, reread recipient and attachment. For very sensitive documents, such as health records, consider protecting the file with a password, communicated separately by another channel.



Re-read recipient and attachment; for sensitive data protect the file and send the password separately.

> **WARNING**
>
> Taking a photo with your personal phone of a work document containing other people's data is itself handling data: do not do it unless the controller has explicitly allowed it.

4. Data breach and notifying the Garante

It can happen to anyone, even to the most careful. What matters is how you react.

The GDPR defines a **personal data breach** as any breach of security leading, accidentally or unlawfully, to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. You do not need a hacker.

- a **lost USB stick** with lists of people;
- an email with **attachments sent to the wrong person**;
- a **stolen computer** or a laptop left in a car;
- **ransomware** that encrypts the client archive;
- an **email account** taken over after phishing;
- a whole folder of files **thrown into the bin**.



A breach can also come from a mistake or a loss.

4.1 The 72 hours

Article 33 of the GDPR says the **controller** must notify the breach to the Garante **without undue delay and, where feasible, within 72 hours** of becoming aware of it. The duty applies unless the breach is unlikely to result in a risk to people's rights and freedoms. If the notification comes later, the reason for the delay must be given.



What happens after a breach

The clock starts when the controller has reasonable certainty that a breach occurred. So your job is just one: **tell them at once**, the controller or whoever the controller has appointed. Every delay on your side takes time away from the person who has to decide.

4.2 What falls to you and what falls to the controller

Who	What they do
You, when you find the problem	Stop what you are doing, warn the responsible person at once, tell the facts accurately, delete nothing
The controller	Assesses the risk to people, decides whether to notify and notifies the Garante through the online procedure on the Garante's website
The processor (supplier)	If the breach happens on its side, informs the controller without undue delay
The people involved	If the risk to them is high, the controller informs them without undue delay (Article 34)

Who does what in case of a breach.

Even when it does not notify the Garante, the controller must **document** every breach in an internal register, with the facts, the effects and the measures taken. So even a small incident should be reported: it is for the controller to decide what to do with it.



The controller assesses the risk and the obligations; every case must be documented.

A PRACTICAL CASE: THE WRONG EMAIL

Marta realises she sent a pupil's record to a wrong address. She does not wait or hope nobody notices: she tells the head teacher at once and gives her the facts, address included. The head teacher, who is the controller for the school, assesses the risk and decides the next steps, including asking the recipient to delete the message and, if needed, notifying the Garante.



Alert the person in charge right away and report precise facts.

WARNING

Hiding a breach is the worst mistake: it makes the harm worse and can aggravate the penalties. Reporting quickly and honestly protects you, the people and your organisation.

THE LINK TO THE NEXT LESSON

When it happens, you need a method. In the final lesson you will see the steps to follow in any incident, including reporting to the Polizia Postale e delle Comunicazioni (Italy's online-crime police unit).

Practical exercise

A short exercise on your own desk and your own mail, with what you already have.

1. Look at your desk and your screen as a visitor would: what personal data is visible?
2. Pick a form you use (sign-up, request, record) and mark the data that is not really needed for its purpose.
3. Open your mail and find the last message sent to several people: were the addresses in To, Cc or Bcc?
4. Write in three lines what you would do if you noticed you had sent an attachment to the wrong person.
5. Ask the right person who the controller is in your office and whom to report a breach to, and write the name somewhere you will find it.

FINAL CHECK

Do you know whom to warn in case of a breach?

Do you use Bcc when addresses must not be visible?

Are files locked away at the end of the day?

Do you ask only for the data you need?

Questions that come up in class

Are a name and a phone number also personal data?

Yes. Name, phone, email, address, a photo and even a number plate are personal data, because they allow you to trace a person.

Must I warn the Garante if I notice a breach?

No, that is for the controller, the organisation you work for. Your job is to warn them at once: they assess the risk and decide whether to notify the Garante within 72 hours.

Do the 72 hours count from when it happened?

They count from when the controller became aware of it. That is why warning at once matters so much.

Does the GDPR also apply to a small firm or an association?

Yes. It applies to anyone who handles people's data, whatever the size. In some cases the amount of paperwork changes, not the responsibility.

Can I send a client's documents over WhatsApp?

It depends on your organisation's rules and on how sensitive the data is. For special-category data, such as health, ask the controller which channel is authorised: do not decide alone.

What is the difference between the GDPR and the Privacy Code?

The GDPR is the European regulation, the same across the Union. The Code is the Italian law that completes it, updated in 2018 to align it with the regulation. They apply together.

Glossary

Term	What it means
Bcc	Blind carbon copy (Ccn in Italian): the mail field that hides recipients from each other.
Controller	Whoever decides why and how data is used: the school, the firm, the company.
Data breach	An event causing loss, destruction, alteration, unauthorised disclosure of, or access to, personal data.
Data minimisation	The principle of collecting and keeping only the data necessary for the purpose.

Term	What it means
Data subject	The person the data refers to.
Garante	Italy's independent authority for the protection of personal data.
GDPR	Regulation (EU) 2016/679 on the protection of personal data, applied since 25 May 2018.
Personal data	Any information about an identified or identifiable natural person: name, email, phone, tax code, photo, number plate.
Processor	Whoever handles data on the controller's behalf, for example a cloud service provider.
Special-category data	More sensitive data (health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sex life or sexual orientation, genetic data and biometric data used to identify a person) with stricter rules.

Further reading

Regulation (EU) 2016/679 (GDPR) - official text on EUR-Lex; in particular Articles 4, 5, 33, 34 and 83

Italian Personal Data Protection Code, legislative decree 196/2003 - as amended by legislative decree 101/2018

Garante per la protezione dei dati personali (Italian Data Protection Authority) - www.garanteprivacy.it: information sheets and the breach notification procedure

European Data Protection Board (EDPB) - guidelines on personal data breach notification

> **WATCH OUT**
>
> Information up to date as of October 2026. This lesson is general training and not legal advice: rules are evolving, always check the Garante's website; for specific cases, ask your controller or your organisation's data protection officer. The GDPR applies across the EU; Italian bodies are explained in brackets, and in other countries the national data protection authority plays the role of the Garante.