Advantages and sovereignty

Where is your Classroom homework right now: in Madrid, in Ireland, in Iowa? Who decided it, you or the school? And if a judge in another country asked the provider for it, would the provider have to hand it over?

Most people never ask. A company has to. When a hotel chain in Palma puts its guests' passports and card details in the cloud, it is still legally responsible for them, wherever they end up. Today you weigh what the cloud really brings to a connected company, what it risks, and you do the research a careful IT team does before signing: find out where a real service keeps its data and which law applies.

What you will learn

- Identify the **advantages** the cloud brings to **connected systems**, and its main risks
- Explain **data sovereignty**: knowing and controlling where data are, who can reach them and which law applies
- Recognise the rules that decide it: the **RGPD** and its transfer rules, the US **CLOUD Act** and the EU **Data Act**
- Find out, with public sources, where a real service keeps its data and whether they leave the EU
- Avoid the trap: "the IP address of a website tells you where the data are stored"

What the cloud brings to connected systems

> A **connected system** is a set of devices, applications and people that exchange data over a network: the sensors and SCADA of Unit 1, the IoT of Unit 2, the wind turbines of the last lesson.

Advantage	What it means	Example
One common point for data	Every device and site sends its data to the same place.	The data of all the hotels of a chain, together and comparable
Scalability and elasticity	Grow from ten devices to ten thousand without buying servers; shrink when they are not needed.	More capacity in August, less in January
Access from anywhere	Data and applications are reachable from any device with a connection.	The manager checks the wind farm's production on her phone
Cost that follows use	No big initial investment: spending follows activity (your estimate from lesson 2).	Opening a new hotel without a server room
Availability and copies	Providers have several data centres and let you replicate data between them.	If one server fails, bookings continue from another
Remote management	Devices are controlled and updated from a distance, all at once.	Updating the software of every door lock without visiting them one by one
Power to analyse	Computing capacity for big data and artificial intelligence.	Predicting breakdowns from years of vibration data

Advantage	What it means	Example
Integration	Services from different companies connect easily through APIs.	Bookings linked to travel agencies and a payment gateway

And the risks to keep an eye on:

Risk	What it means	How it is reduced
Depending on the connection	No internet, no cloud.	Edge processing for what cannot stop (last lesson)
Vendor lock-in	Moving to another provider becomes so hard or expensive that you are stuck.	Open formats, multicloud, and the EU **Data Act** (below)
Costs that grow	Paying per use also means paying for what is left switched on.	Budgets, alerts, reviewing the bill every month
Shared security	The provider protects the infrastructure; the configuration and the data are the customer's job.	Know which layers are yours (lesson 1)
Where the data are and who can reach them	Another country, another law.	The rest of this page

Data sovereignty

> **Data sovereignty** means that data are subject to the laws of the place where they are stored and of the company that holds them. Having sovereignty over your data means knowing and controlling **where they are, who can reach them and which law applies**.

In the city-builder game, renting electricity is comfortable. But before signing you want to know where the power station is, which country the company belongs to, and whether you can switch to another one without paying a fine. Four questions, four answers:

Question	What you need to know
Where are they?	Providers group their data centres in **regions**, and the customer chooses the region. The three big ones have regions in Spain: AWS in Aragon (`eu-south-2`, opened in 2022), Google Cloud in Madrid (`europe-southwest1`, 2022) and Microsoft Azure in Madrid (`Spain Central`, 2024). Hetzner, a German provider, has its data centres in Germany and Finland, plus the USA and Singapore.
Can they leave the EU?	The **RGPD** (Regulation (EU) 2016/679, Chapter V, articles 44 to 49) only lets personal data leave the European Economic Area with safeguards: an **adequacy decision** of the European Commission (the destination protects data as well as the EU), **standard contractual clauses**, or specific exceptions. For the United States there is the **EU–US Data Privacy Framework**, an adequacy decision of 10 July 2023, upheld by the EU General Court on 3 September 2025; an appeal is pending before the Court of Justice.
Whose is the provider?	A US company is subject to US law even if its data centre is in Europe. The **CLOUD Act** (2018) obliges it to hand over data under its control when US authorities request them through legal process, wherever the data are stored. That is why "sovereign" offers exist, such as the **AWS European Sovereign Cloud**, whose first region opened in Brandenburg, Germany, in January 2026, run by companies set up in the EU.
Can I switch provider?	The EU **Data Act** (Regulation (EU) 2023/2854) has applied since 12 September 2025. It obliges cloud providers to make switching to another provider possible, and from **12 January 2027** they may no longer charge **switching charges**. It is Europe's answer to vendor lock-in.

The company that collects personal data stays **responsible** for them even if a provider stores them. Choosing a provider and a region is a **legal** decision, not only a technical one. The rules on personal data are studied in depth in Unit 5.

> **Careful: "switching is now free"**
> The Data Act bans the **switching charges** themselves. The provider can still bill the normal service while you use it, and some costs of running two clouds in parallel. Read it as "they cannot fine you for leaving", not "everything is free".

Where does a website answer from?

There is a quick technical check you can do from the browser, with no account: look up a domain's IP address and ask who owns that address.

Tool	What it does
Google Admin Toolbox Dig	Asks the **DNS** (the internet's phone book) for a domain's address. Choose the `A` record and copy the IP
ipinfo.io	Opening `ipinfo.io/<IP>` shows the organisation that owns the address and an approximate city

Try it with your own GitHub Pages site. On 25/10/2026, a `github.io` address showed the organisation **Fastly** (a CDN), the city **San Francisco**, and the label `anycast: true`. Yet the page reached Mallorca in milliseconds. **Anycast** means the same address is announced from many places at once, and you are served by the closest copy: the CDN of the last lesson, which is edge.

> **Careful: the IP address is not where the data live**
> A website is often served from a CDN or an anycast address, so the IP points to a nearby cache or to the CDN company's head office, not to where the data are stored. If ipinfo says "Madrid", it does **not** prove the data are in Madrid. What the provider **writes** in its privacy policy and contracts is what counts; the IP check only tells you who delivers the page.

In class: where do the data live?

Individually. Research **two services**: one you use in class (Kahoot, Google Classroom or GitHub) and one your company uses or that you proposed in D3 (the provider of your estimate, the company's website...). **No generative AI**: this activity is assessed (class work, 30%). **Passive only:** you only read what any visitor can see; never test passwords or scan anything.

Step	Do this	Where to look
1	**Who is the provider**, and in which country is its head office?	The legal notice or privacy policy
2	**Where does it say it stores the data**: country, region or data centre?	Privacy policy, "data location" or "data residency" page, list of **subprocessors** (other companies that handle data for it)
3	**Do data leave the EEA**, and with which safeguard (adequacy, Data Privacy Framework, standard clauses)?	The "international transfers" section of the privacy policy

Step	Do this	Where to look
4	**Where does the website answer from?** Look up the domain in Dig (`A` record), copy the IP and open `ipinfo.io/<IP>`. Note the organisation and city	Dig and ipinfo.io
5	**Conclusion** in three sentences: is it a good option for your company's data? Which region or provider would you choose, and why?	What you found

For every step, the citation: link, date consulted, and the sentence copied in quotation marks. If the policy does not say, write "it does not say" and where you looked: that is also a finding.

Then: your group's website

Then, in your project group, the **Technician** sets up the site where the group will publish Deliverable 3. Everybody watches and takes part.

Step	Do this	You should see
1	The Technician creates a **public** repository called `dossier-<company>` (no spaces or accents), with **Add README**	The new repository
2	**Settings** → **Collaborators** → **Add people**: invite the other members by username. Each one accepts the invitation (email or GitHub notification)	Everybody can edit
3	Create `index.md` with the skeleton of D3: title, company name, one heading per section (A, B, C, D) and one for the group part. Each member writes one line under their heading and commits it	The history shows who wrote what
4	**Settings** → **Pages** → **Deploy from a branch** → `main`, `/ (root)` → **Save**	The site at `https://<technician-username>.github.io/dossier-<company>/`

GitHub Pages turns `.md` files into web pages by itself, so you can write in Markdown. Mermaid diagrams are **not** drawn on the published site: add the architecture diagram as an **image** (PNG). The repository is public: no personal data, first names only if you prefer. The Coordinator hands in the two links on Classroom. If nobody in the group has a GitHub account, make a Google Sites site with your school accounts.

For your project

This lesson closes the research for Deliverable 3 · Cloud architecture, due **Monday 8 February 2027 at 23:59**, the same day as your defence in session 14.

Today's work	Becomes	Criterion
Where the data of your company's provider live, and your choice of region	Section D: deployment model and sovereignty (with 3 members, group part)	e
Advantages and risks for your company	Sections B and D, and the group's conclusions	e
The group's repository and site	The published dossier (group part)	Group part

Key takeaways

- For **connected systems**, the cloud brings one common point for data, elasticity, access from anywhere, cost that follows use, availability, remote management, analysis power and integration.
- Its risks: depending on the connection, **vendor lock-in**, growing costs, shared security, and where the data are.
- **Data sovereignty** is knowing and controlling where data are, who can reach them and which law applies. The customer stays responsible for its data.
- The **RGPD** only lets personal data leave the EEA with safeguards such as an **adequacy decision**; the US **CLOUD Act** reaches US providers wherever their data centres are.
- The EU **Data Act** obliges providers to allow switching, with no switching charges from 12 January 2027.
- An IP lookup tells you who **delivers** a page (often a CDN with **anycast**), not where the data are **stored**.

Quick check

1 What is data sovereignty?

A The provider's right to use its customers' data
B Knowing and controlling where data are, who can reach them and which law applies
C Storing all data on the company's own servers
D Encrypting data so that nobody can read them

2 A hotel chain moves its guest records to a cloud provider. Who is responsible for those personal data?

A Only the provider, from the moment it stores them
B The hotel chain, which remains responsible even though a provider stores them
C Nobody, because the data are in the cloud
D The guests themselves

3 Under the RGPD, when can personal data be sent to a country outside the European Economic Area?

A Never, in any case
B Always, if the provider is a large company
C Only with safeguards, such as an adequacy decision of the European Commission or standard contractual clauses
D Only if the data are less than one year old

4 A US provider keeps a company's data in a data centre in Madrid. Which statement is true?

- **A** Only Spanish law applies, because the data centre is in Spain
- **B** US law can also reach those data, because the CLOUD Act applies to US providers wherever the data are stored
- **C** No law applies to data in the cloud
- **D** The data automatically move to the United States

5 What does the EU Data Act change for a company that wants to leave its cloud provider?

- **A** Nothing: it only covers mobile phones
- **B** It forbids companies from changing provider more than once a year
- **C** Providers must make switching possible, and from 12 January 2027 they cannot charge switching charges
- **D** It makes every cloud service free of charge

6 ipinfo.io says a website's IP address is in Madrid. What can you conclude?

- **A** The website's data are stored in Madrid
- **B** The company is Spanish
- **C** Only who delivers the page and roughly from where; the data could be stored somewhere else, so you must read the privacy policy
- **D** The website does not use a CDN

7 A small dental clinic in Manacor wants online appointments for its patients. Which choice protects its patients' data best, with the least effort?

- **A** The cheapest service found, whatever the country, without reading its policy
- **B** A SaaS whose policy says it stores data in the EU, after checking its transfers section
- **C** Its own server in the waiting room, so that nobody else sees the data
- **D** A spreadsheet shared publicly so patients can book themselves

You now have everything for your cloud architecture: what to rent, from whom, at what cost, what stays local and where the data live. Put it together in Deliverable 3 · Cloud architecture.

Solutions

1. B · **Data sovereignty** is about **location, access and law**. Encryption and own servers can help, but they are tools, not the definition.

2. B · Under the **RGPD** the company that collects the data stays **responsible**. The provider processes them on its behalf, under contract.

3. C · **Chapter V** of the RGPD allows transfers outside the EEA only with safeguards: an **adequacy decision**, **standard contractual clauses** or specific exceptions.

4. B · Location matters, but so does **who the provider is**. The **CLOUD Act** obliges US providers to hand over data under their control when legally requested, wherever they are stored.

5. C · The **Data Act** (Regulation (EU) 2023/2854) attacks **vendor lock-in**: switching must be possible and, from 12 January 2027, without switching charges. The normal service is still paid.

6. C · Many sites are served through a **CDN** or an **anycast** address. The IP tells you who **delivers** the page, not where data are **stored**: the provider's written policy is the evidence that counts.

7. B · A **SaaS** saves the clinic administration work, and checking the **region** and **transfers** in the provider's policy is the sovereignty homework. A server in the waiting room is not safer just because it is close.