CLARITY LAYER

DATA STRATEGY & GOVERNANCE

The EU Data Act
Simple Summary

www.clarity-layer.com

Contents

What It is

The **EU Data Act** sets rules for how data from connected products and related digital services should be shared, accessed, and protected in the EU.

Its goal is to make data fairly accessible, securely shared, and used for innovation, without letting big players lock others out.

Who is Affected

Group	What They Do	Real-World Examples
Manufacturers of connected products	Make devices that generate or collect data.	Smart cars, tractors, medical devices, IoT sensors, smart home tech.
Providers of related services	Offer digital services linked to those products.	Vehicle fleet apps, fitness dashboards, industrial monitoring tools.
Users	People or companies using those products.	A farmer using a connected tractor, a driver using a smart EV.
Data holders	Control or store access to the data.	A carmaker keeping vehicle performance logs.
Third parties (data recipients)	Businesses or researchers who get access to the data (with permission).	Independent repair shops, analytics startups, insurers, researchers.
Cloud and edge service providers	Host and process the data.	AWS, Azure, Google Cloud, local hosting firms.
Public authorities	Can request access *only* in emergencies or for public interest reasons.	National statistics offices, disaster response agencies.

Main Obligations and Rights

1 Manufacturers & Data Holders

- Must make data from connected products **available to users** easily and free of charge.
- Must share data **securely** and **without discrimination** with third parties chosen by the user.
- Must provide **clear, plain-language information** on what data is generated and how to access it.
- Must **protect trade secrets but** cannot use them as an excuse to block data sharing.
- Must offer APIs or other tools for **timely and continuous access**.

Example:
A carmaker must let a customer or an authorized garage access vehicle sensor data — not just keep it locked in their own app.

Not OK:
Charging huge fees or giving competitors' data slower access.

2 Users (Individuals or Companies)

- Have the **right to access** and **share** the data their devices generate.
- Can tell manufacturers to share that data with a third party (like a repair service).
- Have a right to **clear explanations** of what data is collected and for what purpose.

Example:
A farmer can tell the tractor manufacturer to send the machine's soil data to an independent agritech company for analysis.

Main Obligations and Rights

3 Third Parties (Data Recipients)

- Can receive data **only with user permission** and must use it **for the agreed purpose only**.
- Must **keep the data secure, not resell or combine** it to identify users without consent.
- Must delete it when no longer needed.

Example:
A repair service can access a car's diagnostic data to fix it but cannot use it for marketing or sell it to insurers.

4 Cloud and Edge Service Providers

- Must ensure **easy switching** between providers (no vendor lock-in).
- Must provide **data portability** — users can move their data freely.
- Must store and process data securely and protect it from non-EU government access (unless legally required).

Example:
A business using AWS can move its data to Azure without hidden fees or long delays.

Main Obligations and Rights

5 Public Authorities

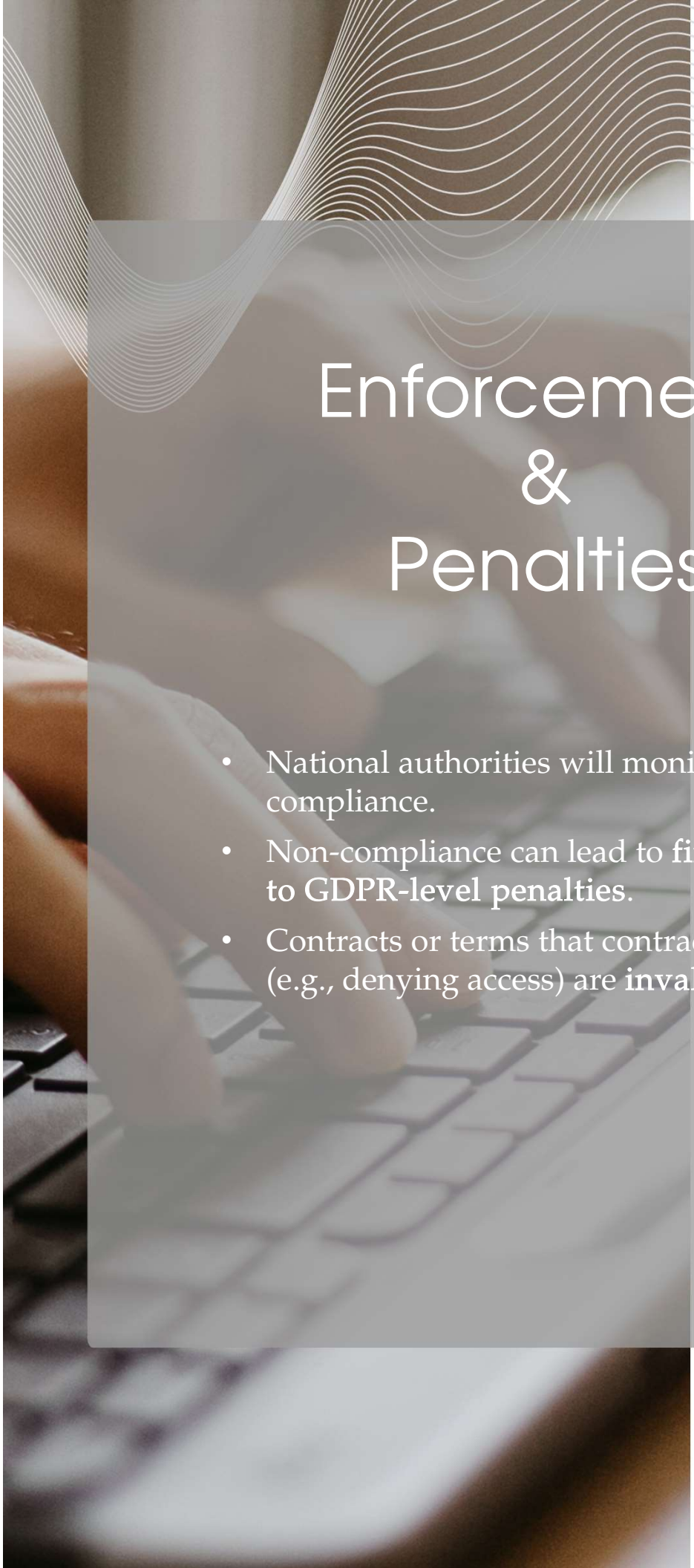
- Can request data **only in exceptional cases** — like emergencies or to respond to public needs (e.g., natural disasters, pandemics).
- Must delete it when no longer needed and **cannot use it for commercial purposes**.

Example:
During a flood, a local government can request real-time bridge sensor data to coordinate evacuations.

6 Statistical Institutes & Researchers

- May access anonymized or pseudonymized data for **public interest research**.
- Must ensure **no re-identification** of individuals or businesses.
- Must keep data handling **transparent and secure**.

Example:
A national statistics office using mobility data to plan public transport — without identifying drivers.



Enforcement & Penalties

- National authorities will monitor compliance.
- Non-compliance can lead to **fines similar to GDPR-level penalties**.
- Contracts or terms that contradict the Act (e.g., denying access) are **invalid by law**.

In Short

Stakeholder	Main Right	Main Duty
User	Access and share their data	Use it responsibly, authorize access clearly
Manufacturer /Data Holder	Keep fair control	Provide access, transparency, and security
Third Party	Get data for specific use	Use it only as agreed, protect confidentiality
Cloud Provider	Host data securely	Allow switching and avoid lock-in
Public Authority	Access for emergencies	Respect proportionality and privacy

Our Team

Alexandra Popa

Chief Data Officer

Paulina Marinos

Chief Operating Officer

THANK YOU

Have questions? Reach out.

info@clarity-layer.com

CLARITY LAYER

DATA STRATEGY & GOVERNANCE