CLARITY LAYER

DATA STRATEGY & GOVERNANCE

The EU Data Act
Definitions

Easy-to-read glossary for the EU Data Act (Regulation (EU) 2023/2854), written for business people

www.clarity-layer.com

01

Connected Product

A physical device that collects or sends data through the internet or another network.

Examples: smart cars, tractors with sensors, fitness trackers, smart fridges.

Not: a traditional fridge or an old car with no sensors or connectivity.

02

Related Service

A digital service that uses or adds value to data from a connected product.

Examples: a mobile app showing your car's fuel use, a smart home dashboard, a fleet management platform.

Not: a call center or physical repair service.

03

Data Holder

The company or organization that *controls* access to the data from a product or service — even if they didn't create it.

Examples: a car manufacturer that stores vehicle performance logs, a smart device company keeping usage data.

Not: the customer using the product, or a data broker with no control over access.

04

User

The person or business that uses a connected product or its related service. They can be a consumer or a company.

Examples: a driver using a smart car, a farmer operating a connected tractor, a factory running IoT sensors.

Not: the manufacturer or service provider who made or sells the product.

05

Data Recipient (Third Party)

A company or person that gets data from a user or data holder, *with permission*, for a specific reason.

Examples: an independent repair shop, a research team analyzing energy use, a data analytics startup.

Not: a company taking or buying data without the user's consent.

06

Data Sharing

Giving access to data to someone else (like a third party or public body) — securely, fairly, and for an agreed purpose.

Examples: a car owner letting a repair shop access engine data; a company sharing machine data with a partner.

Not: secretly collecting or selling data, or giving partial/locked data to competitors.

07

Access in a Timely Manner

Providing data fast enough for it to still be useful — not weeks or months later.

Examples: real-time access to sensor data for maintenance; 24-hour access through an API.

Not: long approval chains or slow, manual data exports.

08

Public Authority

A government or public organization that can ask for data in emergencies or public-interest cases.

Examples: a city government during a flood, a health ministry during a pandemic.

Not: commercial companies, even if they are state-owned.

09

Data Owner (Informal Term)

The entity that has the *legal right or control* over how data is used — often overlaps with "data holder."

Examples: a manufacturer owning machine performance data; a company owning employee system logs.

Not: cloud providers or IT vendors that only store data for others.

10

Processing

Doing *anything* with data — collecting, storing, analyzing, sharing, or deleting it.

Examples: recording sensor readings, analyzing fuel consumption, uploading to the cloud.

Not: unopened or anonymized data sitting in storage.

11

Pseudonymization

Replacing real identifiers (like names or IDs) with fake codes so you can't directly identify a person.

Examples: replacing "Maria Popescu" with "User_00123" in datasets.

Not: true anonymization (where re-identification is impossible).

12

Personal Data

Any data that can identify a person directly or indirectly.

Examples: name, address, email, GPS location, vehicle ID tied to an owner.

Not: data that's completely anonymized or purely technical (like engine oil temperature, without owner link).

13

Business Data

Non-personal data about how a company or machine performs.

Examples: production rates, sensor logs, equipment downtime data.

Not: employee or customer personal data.

14

Interoperability

The ability for systems or platforms to exchange and use data smoothly and automatically.

Examples: being able to move data from AWS to Azure, or connecting a smart thermostat with a different app.

Not: closed systems where data stays trapped in one vendor's ecosystem.

15

Data Portability

The right to easily move your data from one system or provider to another.

Examples: downloading your fitness tracker data to use in another health app.

Not: needing to manually copy/paste or losing your data when you switch providers.

16

Trade Secret

Confidential business information that gives a company an advantage and must be protected when sharing data.

Examples: manufacturing formulas, machine calibration settings, internal algorithms.

Not: general or public data, or data that belongs to the user.

17

Fair, Reasonable, and Non-Discriminatory (FRAND) Terms

A legal principle that means access to data should be fair to everyone — no hidden costs, favoritism, or unfair conditions.

Examples: offering the same API access to all authorized third parties at a fair price.

Not: charging competitors extra or delaying their data access.

18

Data Breach (Contextual Term)

When data is accessed, shared, or lost without authorization.

Examples: a cloud leak exposing machine logs tied to owners.

Not: planned data deletion or access by authorized parties.

19

Switching Provider

Moving your data and services from one cloud or edge provider to another without obstacles.

Examples: migrating from AWS to Azure within days and keeping all your logs intact.

Not: being forced to stay due to hidden costs, delays, or lost data.

20

Data Altruism

Voluntarily sharing data for public good — like science, health, or environment — without expecting payment.

Examples: farmers donating soil data for climate research.

Not: commercial data sales or sharing for advertising.

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