Making Sense of Data Act Access Rights Across Europe

IAPP European Privacy KnowledgeNet 2026



Your local KnowledgeNet chapter volunteers



Carolina Weber

Research Fellow

Max Planck Institute for Innovation and Competition

carolina.weber @ip.mpg.de



Dr. Christian Hamann

Partner

Gleiss Lutz

christian.hamann @gleisslutz.com



Ramon Baradat

Principal Associate

Cuatrecasas

ramon.baradat @cuatrecasas.com

Case 1 — Connected vehicles

A transport company owns a fleet of 500 connected trucks of the same model, bought new from a European truck manufacturer. Every truck constantly generates data from its onboard sensors: location, fuel use, engine effort, battery health, driver behaviour and fault codes (short digital messages the truck records whenever something is not working correctly). The transport company wants two things:

(i) to read all of that raw sensor data in real time on its own dashboard; and

(ii) to send the same live data to an independent provider of predictive-maintenance software (a company that uses the data to anticipate breakdowns before they happen) that competes directly with the manufacturer's own fleet-management product.

The manufacturer only offers a weekly summary report through its own online portal, and quotes a tariff for direct access that is three times what it charges its own authorised dealers. It also wants to prohibit the transport company from forwarding the data to the independent provider.

Case 2 — Wearables

An individual consumer buys a smart cardiac wearable (a small sensor patch worn on the chest, plus an app on her phone). The device constantly records heart rate, variations in heart rhythm and blood oxygen levels. The manufacturer is a two-year-old European start-up.

The consumer wants to export her raw data from the last 12 months and to have the manufacturer send a live feed to a not-for-profit research project working on early detection of arrhythmias. The manufacturer's app presents the user with a confusing choice: a prominent green button labelled "Share my health journey — recommended" (which routes the data only to the manufacturer's own commercial partners) and a dimmed, less visible link below labelled "Other options" (where the Data Act access and sharing rights are hidden). On top of that, the manufacturer tells the consumer that, because it is a small business, it does not have to comply with the Data Act at all.

Case 3 — The trade-secret regime

A European industrial manufacturer leases high-end factory robots (precision machines used in car production) to a car-parts supplier. The software embedded in each robot's controller contains two valuable assets built up over 20 years: the manufacturer's proprietary motion-planning algorithms, and an internal dictionary that translates raw fault codes into meaningful diagnostics.

The supplier accepts, in principle, the manufacturer's commercial terms on access, pricing, format and onward sharing. The dispute is narrower: the manufacturer refuses to disclose anything that touches the motion-planning algorithms or the fault-code dictionary, invoking the "exceptional damage" ground in Articles 4(8) and 5(11). It says that sharing would allow the supplier's engineers, or a future competitor hiring them, to reverse-engineer core know-how.

The supplier does not challenge that the two items are trade secrets. It challenges the refusal: either they must be shared with protection, or the manufacturer must give a documented, item-by-item justification for withholding.



Questions?

carolina.weber@ip.mpg.de | christian.hamann@gleisslutz.com | ramon.baradat@cuatrecasas.com