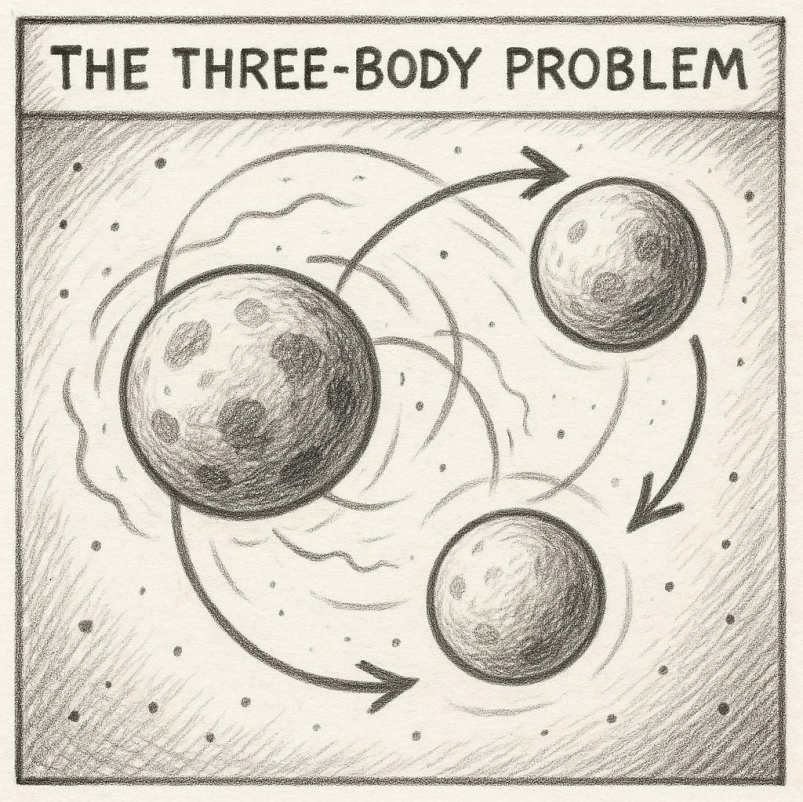
VISCHER

The Three-Body Problem of Digital Regulation.

Is Privacy No Longer King?

David Rosenthal, VISCHER AG
October 30, 2025



A physics problem:

A chaotic, unpredictable system is caused by three celestial bodies with their gravitational force pulling on each other …

The Old System: GDPR as the Sun

- Digital regulation had a **stable centre of gravity**: **GDPR** and other regulations of privacy and secrecy
- The primary force dictating **digital data processing**
  - The main goal was the protection of the rights and freedoms of the data subjects and those with business or professional secrets
- **Clear focus** and **clear rules**
  - Limit the processing of personal data as much as possible (e.g., purpose of use limitation and data minimisation, TOMS)
  - Give data subjects the control over their data (e.g., privacy notices, data subject rights)
  - Assess risks for individuals – if they cannot be identified, everything is (more or less) ok

Two New "Massive Bodies"

- **AI Regulation** (e.g., the EU AI Act) – pulling towards safety
  - Focuses on data quality, bias detection and correction, transparency and safety, which often requires processing large and varied datasets – it is *not* about privacy or data subjects
- **Data Sharing Regulation** (e.g., Data Act, Data Governance Act) – pulling towards data sharing and innovation
  - Aims at making data about the environment or usage of devices available as broadly as possible in order to increase competition and permit the creation of new applications or services
- Some **smaller "bodies"** interfering with them (e.g., copyright)
  - Protecting commercial interests of both rights holders and those who want to use third party works

The Central Conflict

- **Three powerful regulations** …
  - Pulling companies in different directions
  - Using different concepts to regulate the same digital activities
  - With minimal compatibility; making them work together is left to others …
- The **stable orbit** of privacy is **gone**
- A **chaotic**, unpredictable, and dangerous regulatory **space**
- Is privacy **no longer king**?

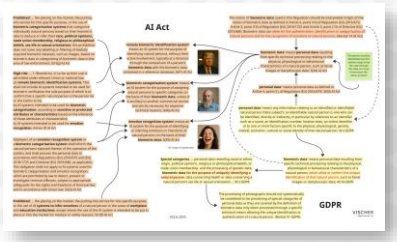
Recital 7, Data Act: "… **No provision** of this Regulation should be applied or interpreted in such a way as **to diminish or limit the right to the protection of personal data** or the right to privacy and confidentiality of communications. Any processing of personal data pursuant to this Regulation should comply with Union data protection law, including the requirement of a valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC. This Regulation does **not constitute a legal basis for the collection or generation of personal data** by the data holder."

Clash 1: Data Minimisation vs Bias Mitigation

- **GDPR:** Demands data minimisation (collect and process as little as possible)
- **AI Act:** Requires vast, high-quality datasets to detect and correct bias for high-risk AI systems
- **Example:** An AI recruitment tool needs sensitive demographic data to ensure fairness, conflicting with GDPR's strict limits
  - Art. 10(5) AI Act does provide a limited legal basis for processing special categories of data for detecting and correcting bias, but only for high-risk AI systems; data minimisation remains an issue
  - **Moreover:** Does not permit the training or validation of an AI marketing system to avoid, e.g., stereotypical targeting, exclusion and price discrimination, inference of sensitive data, or reinforcement using negative loops

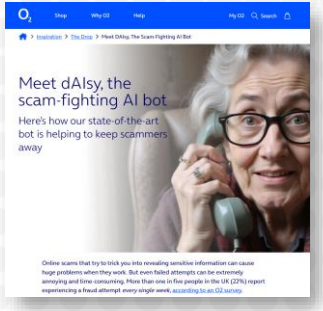
Clash 2: Concept Confusion

- **GDPR:** Treats biometric data as a special category only when used for the purpose of uniquely identifying a natural person
- **AI Act:** Treats biometric data as a special category irrespective of whether it is used for unique identification
  - Regulates other aspects such as "biometric categorisation", "emotion recognition" and "remote biometric identification"
- **Example:** Lawful Basis (GDPR) vs Risk Category (AI Act)
  - GDPR legal basis may be irrelevant (AI Act: No consent)
- **Further complication** when determining responsibility
  - Controller / Processor (GDPR) vs Provider / Deployer (AI Act)
  - Both, an AI Act provider and a deployer, can be a controller



Clash 3: AI Transparency Sabotaging GDPR

- **GDPR:** Requires measures to protect personal data
- **AI Act:** Requires transparency to anyone that they are dealing with an AI system and about how certain AI systems work
- **Example:** Transparency provides intel for evasion or poisoning attacks against protective measures, "canary trap" user accounts to detect attacks, the "Honeypot IT Support Chatbot"
- **Further complication** due to different concepts
  - Information about the data processing activity (controller) vs information about the AI system itself (provider)
  - Obligations split between different actors in the value chain
  - Example: Controllers (usually deployers) are dependent on the information on the AI system provided by the provider



Source: O2

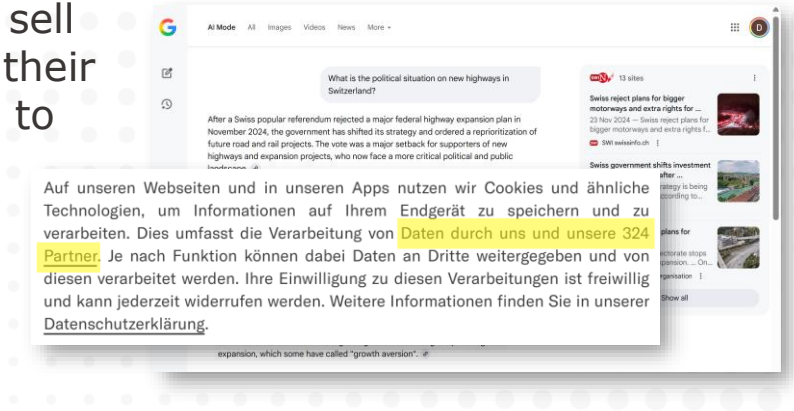
Clash 4: Purpose Limitation vs Data Sharing

- **GDPR:** Data collected for a specific purpose may not be reused for another
- **Data Act:** Grants users of connected products/related services a broad right to obtain and share "their" data for new purposes
- **Example:** A carmaker collects usage data for diagnostics, but the owner demands it be sent to an insurer for a new purpose
  - If personal data of others (e.g., drivers) is affected, the burden for GDPR compliance is upon the carmaker (Art. 4(12)/5(7) DA)
  - How shall the carmaker know? Is it personal data for the carmaker after all? Obligation to redact? Which proof is sufficient? Failure to produce is sanctioned, and production in violation of the GDPR is sanctioned, as well …

Art. 5(7) Data Act: "Where the user is not the data subject whose personal data is requested, any personal data generated … shall be made available by the data holder to the third party only where there is **a valid legal basis for processing** …"

Clash 5: Eyeballs vs Agents

- **GDPR:** Data subjects can protect themselves from being tracked by website operators by relying on AI agents to do research on the Internet
- **Copyright:** Motions to have AI agents prohibited or restricted from using third-party content to provide their services
- **Example:** Media publishers can no longer sell ads if only agents instead of humans visit their websites – and humans do no longer have to allow them to be tracked by their sites
- **Sidenote:** AI-based browsers (e.g., Comet, Atlas) may represent an even larger risk to privacy …



The Collision: A Health Device Scenario

- **Use Case:** A company producing an AI-powered continuous glucose monitor (a connected medical device)
- **GDPR Pull:** Minimize collection of health data, legal basis for processing, limit purpose of use, ensure security measures
- **AI Act Pull:** Maximize data collection and analyse data from many diverse users to ensure accuracy of the (high-risk) AI system and to avoid bias across different populations
- **Data Act Pull:** Make it easy to retrieve all data from the device and be ready to share it on user demand with third-parties (e.g., a wellness app, a research institution)
- **Result:** The company is pulled in three potentially conflicting directions

Navigating the Chaos: The Path Forward

- **For Companies**
  - Adopt interdisciplinary task forces (legal, IT, data science)
  - Move from only "Privacy by Design" to also include "Access and Sharing by Design" and "Risk Management by Design"
  - Enhance data mapping and governance (personal data, non-personal data, trade secrets, connected product data, etc.)
  - Revising contracts, privacy notices, and consent flows to navigate new complexities
- **For Regulators**
  - Need for harmonized guidance
  - Develop (practical) model clauses balancing data protection, data sharing and information required to understand the complexities

Conclusion: A New Paradigm

- **Privacy** is no longer the sole monarch, but part of a power balance
  - E.g., the GDPR may prevail in a direct conflict with the Data Act, but the system is designed to force data to flow
- **Focus shifts** from pure protection to a more complex balancing act (protection vs innovation vs risk management)
  - Chaotic orbit as the new reality
- The "Three Body Problem" is **not** a problem **to be solved**, but a new environment to be understood and navigated
  - Success depends on the ability to navigate these three gravitational pulls simultaneously

VISCHER

Thank you for your attention!

david.rosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Esplanade Pont-Rouge 9C
Postfach
1200 Genf 26, Schweiz
T +41 58 211 35 00

More materials:
www.rosenthal.ch
vischer.com/ai
vischer.com/redink