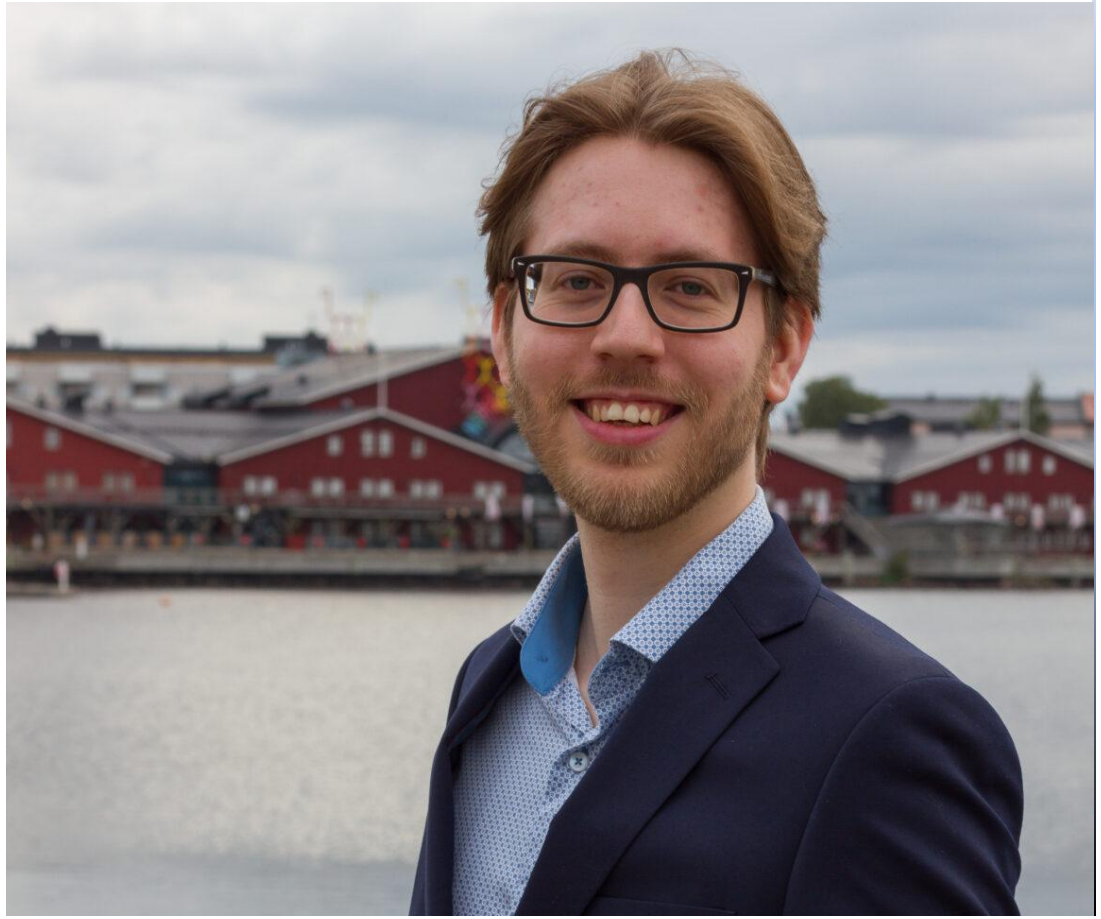
Q&A about GDPR

Ask your questions!

Mattias Gotthold

- **Legal professional with almost 10 years experience of data protection.**
- **Senior Legal Counsel, Data Law Center**
- **Vice-chairman, Swedish Data Protection Forum**

Previously worked at a law firm, govermental agencies and municipality as lawyer.

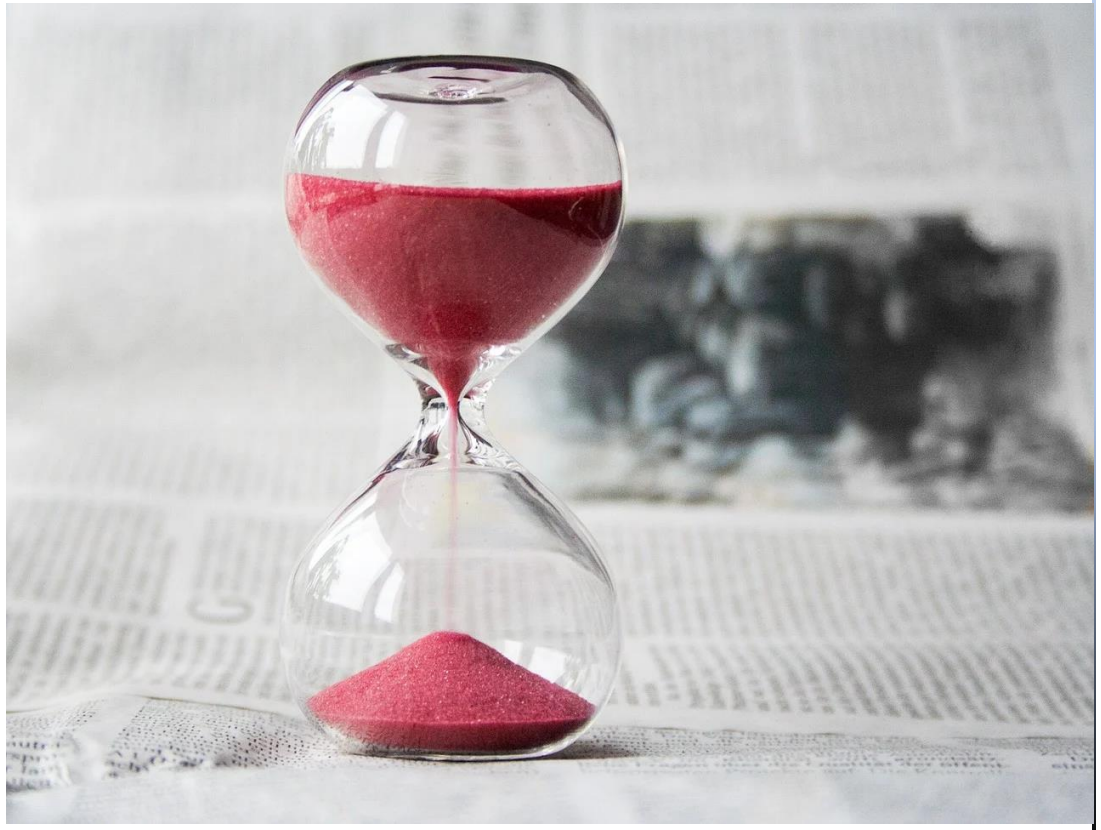


Agenda/questions asked

- **Questions in relation to EU-US data transfers.**
- **Questions in relation to what is personal data.**
- **Questions in relation to AI and personal data.**
- **?**

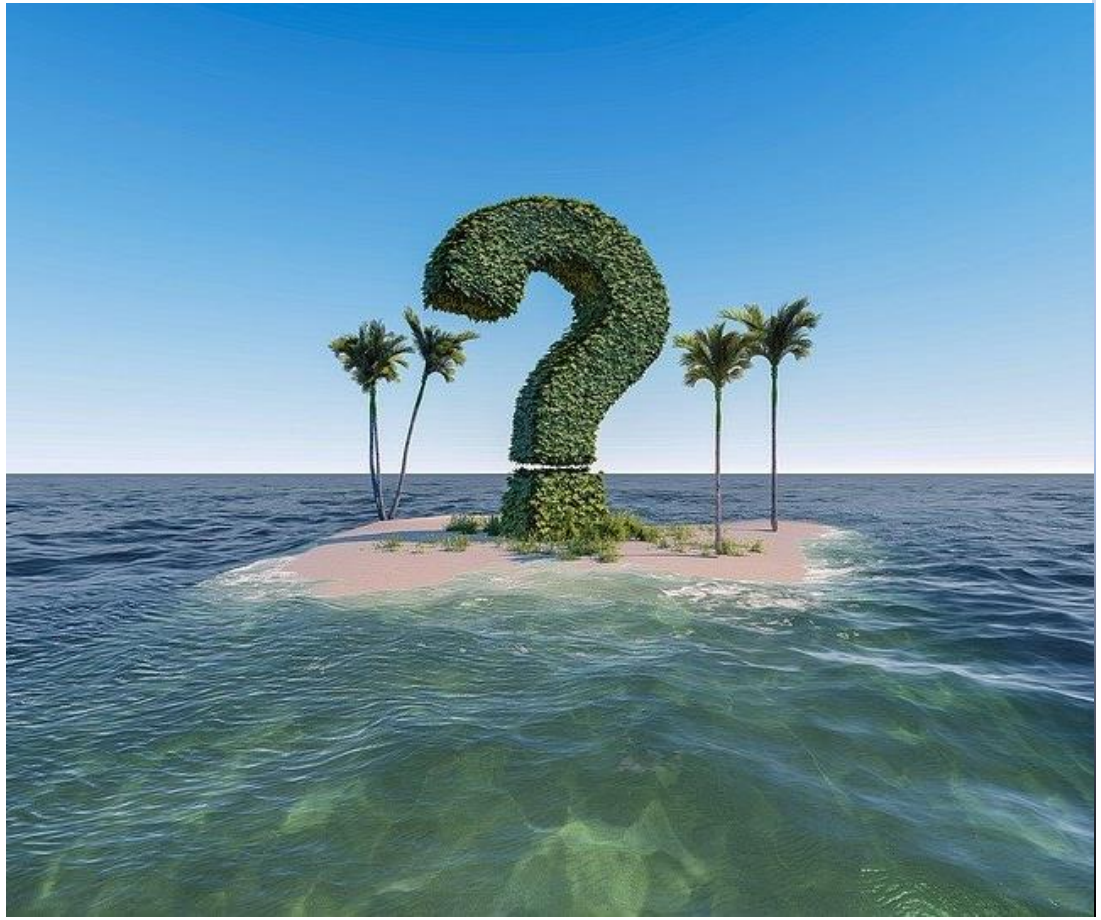
What is personal data?

- **(What is personal data?)**
- **When does personal data stop being personal data (anonymization)?**



Personal data (article 4.1 GDPR)

'personal data' means ***any information*** *relating to an* ***identified*** *or* ***identifiable natural person*** *('data subject'); an identifiable natural person is one who can be identified,* ***directly or indirectly****, in particular by reference to an* ***identifier*** *such as a* ***name****, an* ***identification number****,* ***location data****,* ***an online identifier*** *or to* ***one or more factors*** *specific to the* ***physical, physiological, genetic, mental, economic, cultural*** *or* ***social identity*** *of that natural person*

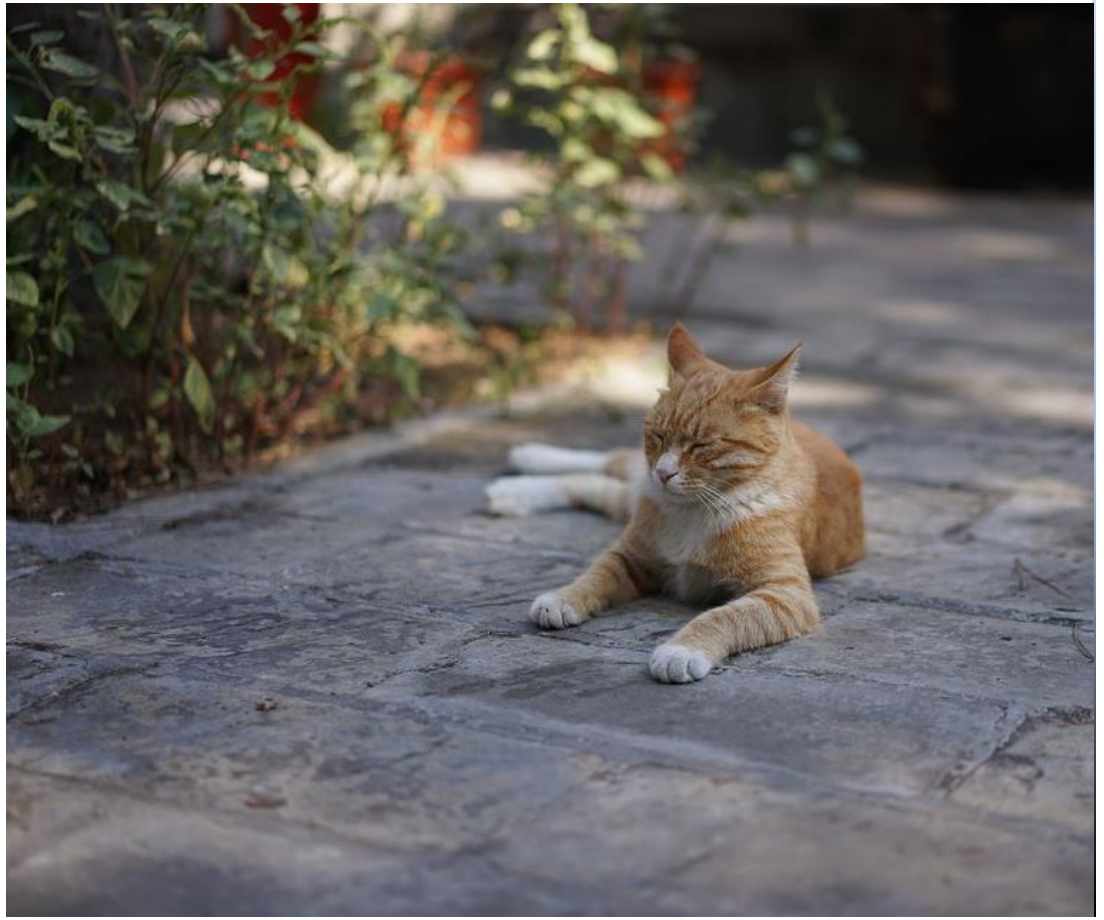


Personal data article 4.1 cont.

Personal data:

any information** about **identifiable natural person** **directly or indirectly** by such as **identifiers (name, identification number, location data, an online identifier)

OR one or more factors** such as **physical, physiological, genetic, mental, economic, cultural** or **social identity



Examples of personal data general/tech

- Name (e.g., John Doe)
- Address (e.g., 123 Main Street, City)
- Email address (e.g., john.doe@example.com)
- Phone number (e.g., +1234567890)
- Identification number (e.g., passport number, social security number)
- Biometric data (e.g., fingerprints, facial recognition data)
- Location data (e.g., GPS data, IP address)
- Cookies and online identifiers (e.g., device IDs, user IDs)
- Banking and financial information (e.g., bank account details, credit card numbers)
- Health data (e.g., medical history, health records)
- Employee ID (e.g., E12345)
- Customer purchase history (e.g., items bought, dates, quantities)
- Server log data (e.g., timestamp, request URL, response status)
- Sensor readings (e.g., sensor activation, timestamp)
- User login credentials (e.g., username, hashed password)
- Transaction records (e.g., date, amount, transaction ID)
- Personal API keys and access tokens (e.g., API_KEY_ABC123)
- Software version data (e.g., app version, update timestamps) – not by its own

Example of personal data

Customer of company X

Customer name: John Doe

Customer ID: 01x

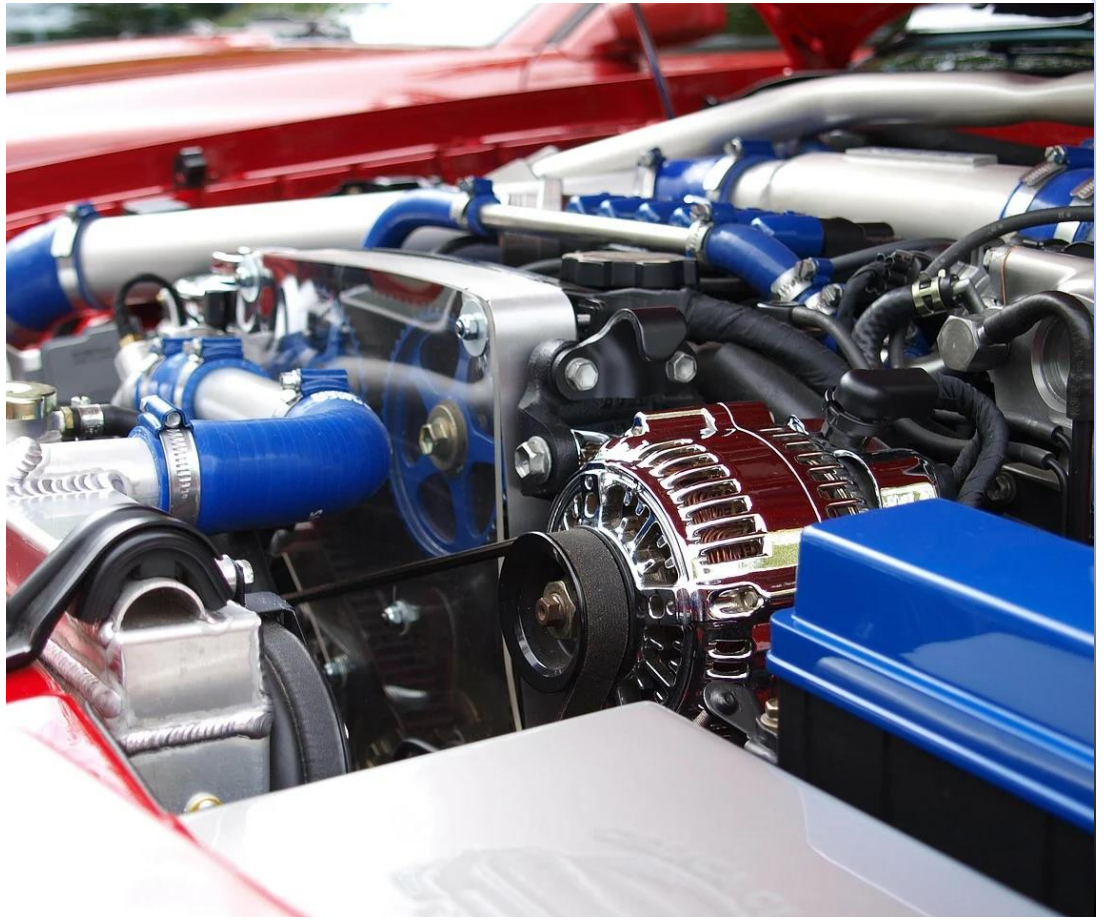
Username: Doe-90

Hashed password: 5e884898d…

Last login: 2025-01-01 23:59

User_Background: Teal-Blue

User_UI_Layout:4



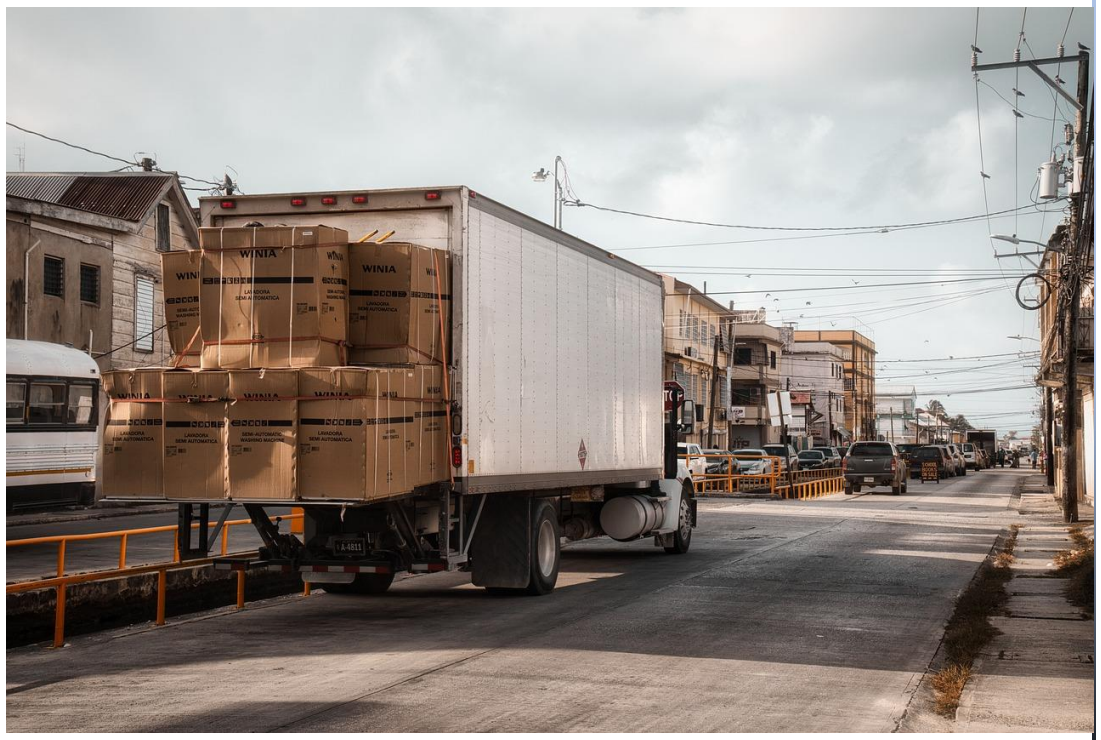
Enough data about user means...

That everything becomes personal data (eventually only 1 possible identifiable person):

Country, Sex, Data 1, Data 2, Data 3, Data 4…

->

the dataset becomes personal data



How to make personal data stop being personal data?

Use anonymization techniques:

- **Aggregation (changing data total)**
- **Data generalization (changing individual data)**

Almost never enough by its own:

- **Purge some datapoints (-)**
- **Data obfuscation (J*** D**)**
- **Data masking (replace data with fictional data)**

Reidentification must be ‘impossible’!

Established methods:

- **K-Anonymity (ensure that records are indistinguishable from others)**

Example: Modifying data so that at least 5 records share the same combination of age range, ZIP code, and gender.

- **L-Diversity (ensure diverse sensitive attribute values**

Example: In a group of anonymized records, ensuring that disease diagnoses are diverse enough to prevent inference.

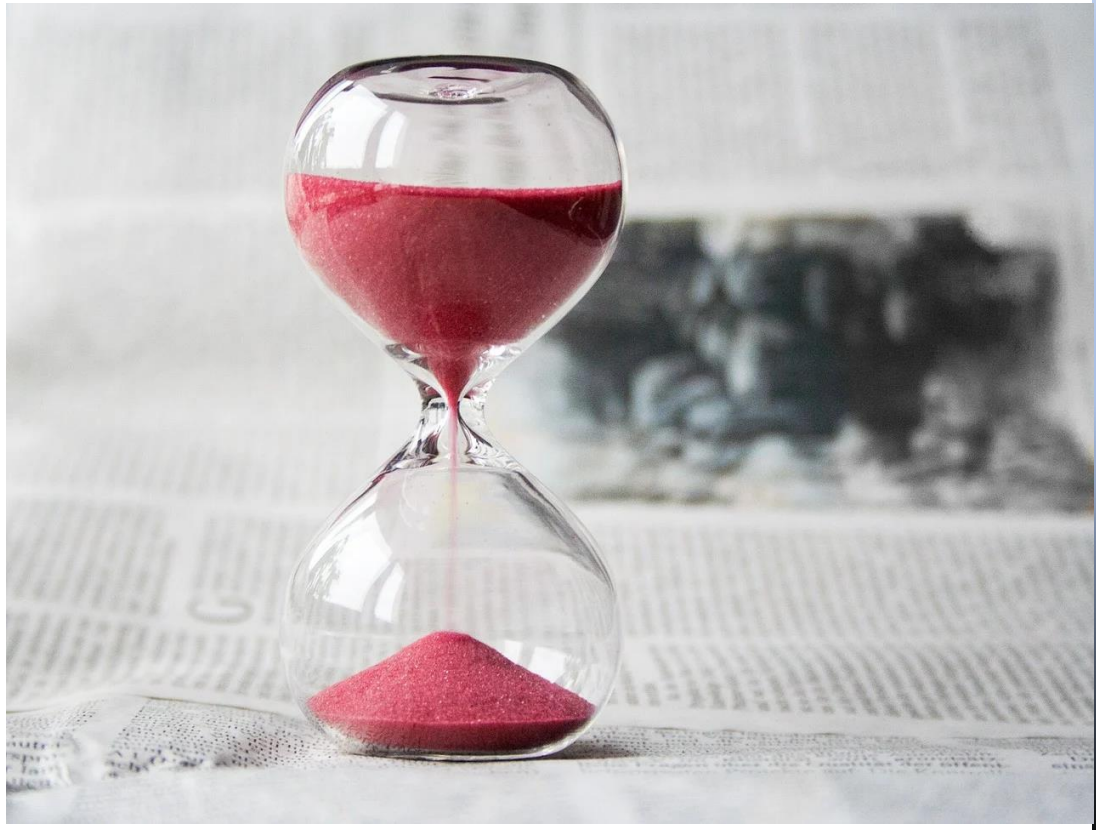
- **T-Closeness (ensure that no data outliers)**
- **Differential Privacy (add data noice)**

Necessity of anonymization?

Often harder to archive anonymization that just following GDPR. Usually only recommended when a high level of security is nessecary or impossible to comply with GDPR.

Data transfers in general and EU/US

- **(When are transfers possible?)**
- **What is actually required when using US companies as providers?**
- **What is the future for transfers to USA?**
- **Are data transfers affected by the Trump administrations policies?**



By standard transfers out of EU/EEA prohibited

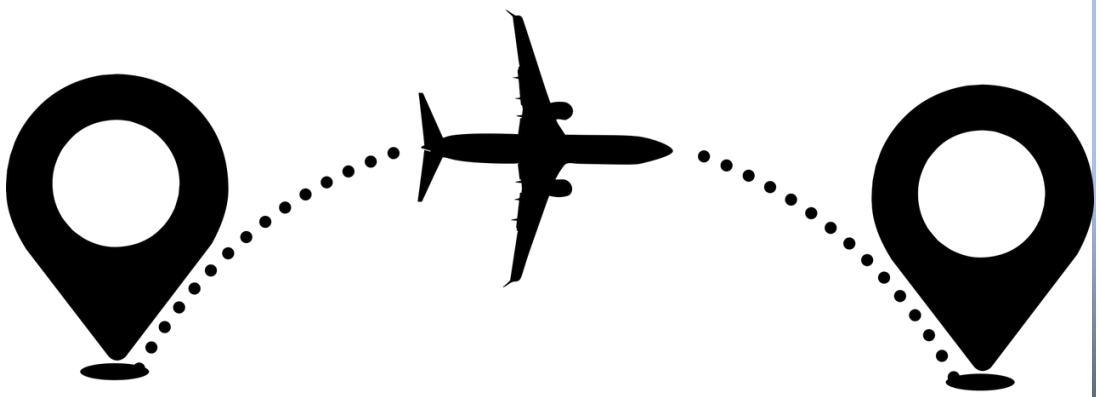
Transferring personal data outside the EU/EEA (the scope of GDPR) **is generally prohibited. This is because the right to privacy is considered a human right based on:**

- **the protection of private and family life** (Article 7 of Charter of Fundamental Rights of the European Union),
- **the protection of personal data** (Article 8 of the Charter),
- **and the right to effective remedies, such as courts** (Article 47 of the Charter).

Exceptions

There are exceptions that allow personal data to be transferred to third countries if adequate protection is in place, including

- adequacy decisions
- the European Commission's Standard Contractual Clauses (SCC)
- Legally binding and enforceable instruments between authorities and public bodies
- Approved codes of conduct
- Contractual clauses or provisions specifically approved by the supervisory authority in the individual case



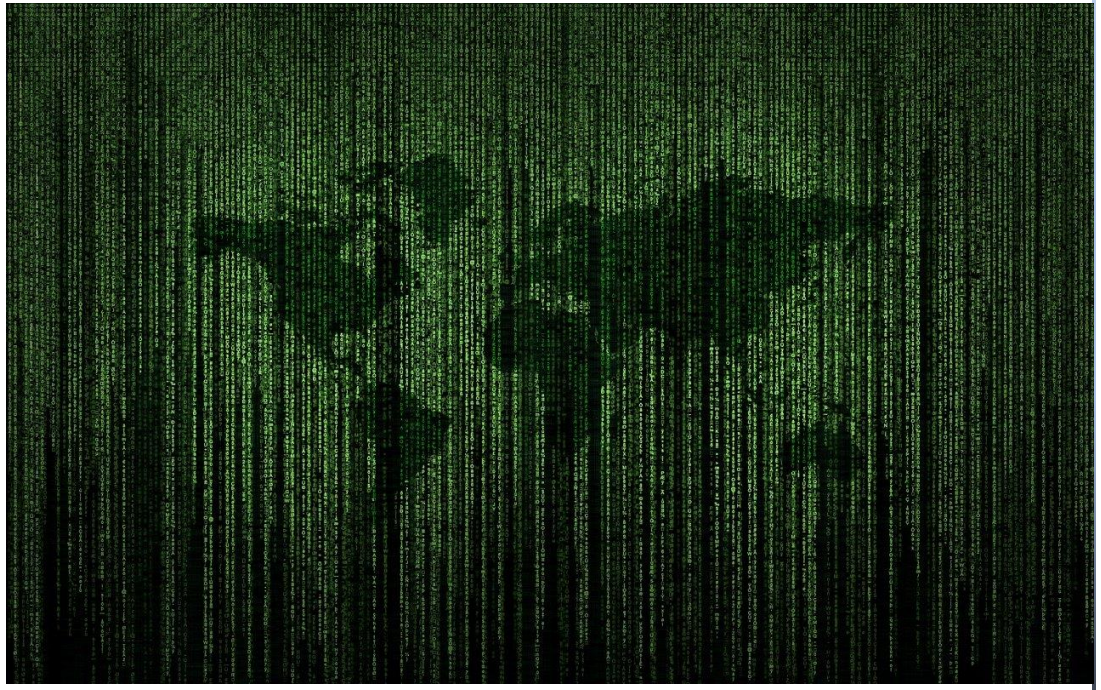
Most common transfer mechanisms

The most common transfer mechanisms are:

- **Adequacy decisions** by the European Commission
- Standard Contractual Clauses (**SCC**)

In the case of **adequacy decisions**, **no specific measures are required** for the transfer to be legal.

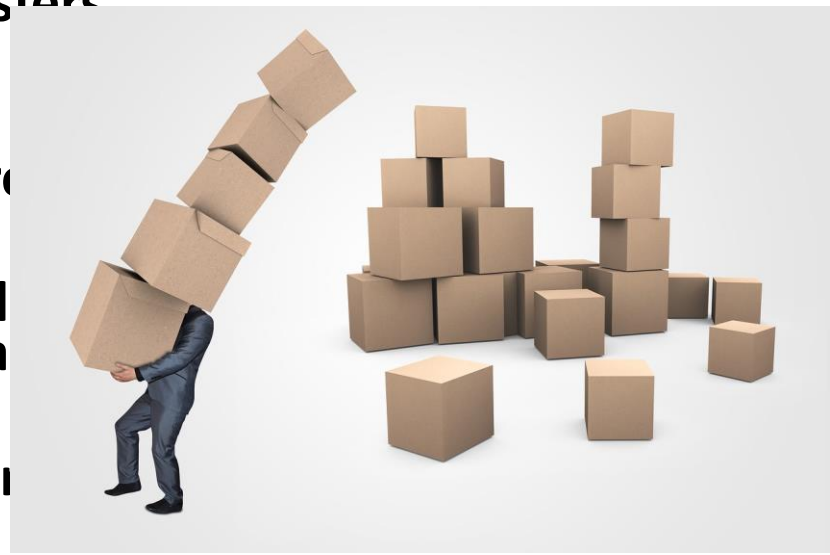
Standard contractual clauses normally **require extensive measures** to be legal.



Transfers are subject to obligations

EDPB six-step process for transfers:

1. **Know your transfers.**
2. **Know which mechanism of the GDPR the transfers are based on.**
3. **Assess whether there are any obstacles in the recipient country that affect the safeguards pr by the mechanism**
4. **Implement safeguards to achieve an acceptabl of protection of personal data based on the ga 3.**
5. **If necessary, take formal steps to make measu 4 binding.**
6. **Periodically assess the adequacy of the safeguards and monitor changes in relation to 3.**



USA specific

Previous transfer mechanisms:

- **Safe harbor**
- **Privacy shield**

“New” framework (since 2023):

- **EU-US Trans-Atlantic Data Privacy Framework (TADPF)**

- **Standard contractual clauses (SCC)**
- **Binding corporate rules**

Timeline

- **Safe harbor introduced**, July 26, 2000
- **Schrems I** (Safe Harbour repealed), 6 October 2015
- **Privacy shield introduced**, July 12, 2016
- **Schrems II** (Privacy shield repealed), July 16, 2020
- **EU-US Data Privacy Framework** (TADPF) enters into force, July 10, 2023
- Philippe Latombe requests interim decision to pause the TADPF, September 6, 2023 (denied, but appeal processes ongoing)
- US administration **dismisses 3 judges from TADPF court** (one judge remains, but see last note), January 27, 2025
- US administration bans Microsoft from providing services to parts of ICC:s staff, February 2025.
- NOTE! Just the last few days a court invalidated 2 of the judge dismissals, but the administration has appealed the invalidation so case pending, May 2025.

Problems with transfers to the US

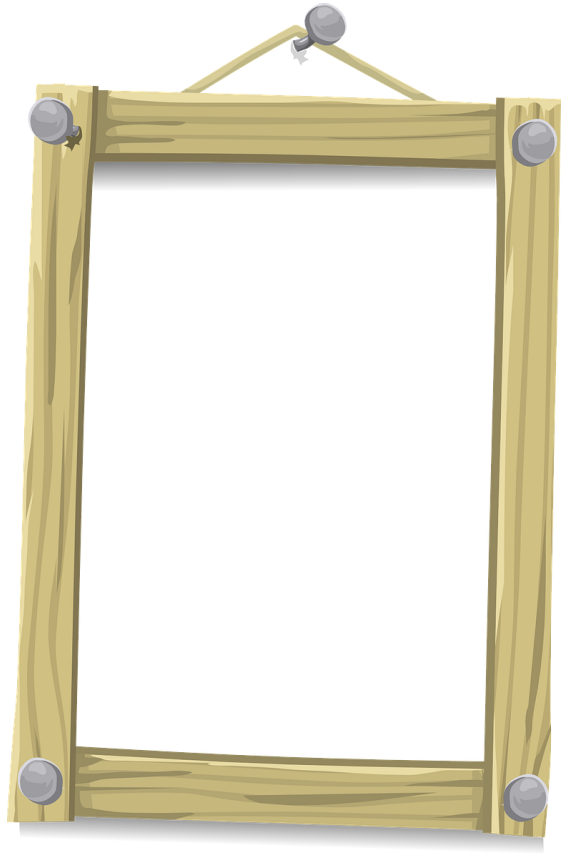
Based on Schrems I-II, two main problems with transfers to the US:

1. **That US authorities can get access to the data. This is because the surveillance measures etc. that are implemented are not necessary and proportionate in a democratic society.**
2. **The lack of effective complaint mechanisms for individuals who believe that their data has been mishandled.**

What is new/required to join TADPF?

Companies self-certify to the TADPF (**cost $50**). By this, they **promise to comply** with rules, mainly the following (GDPR-lite):

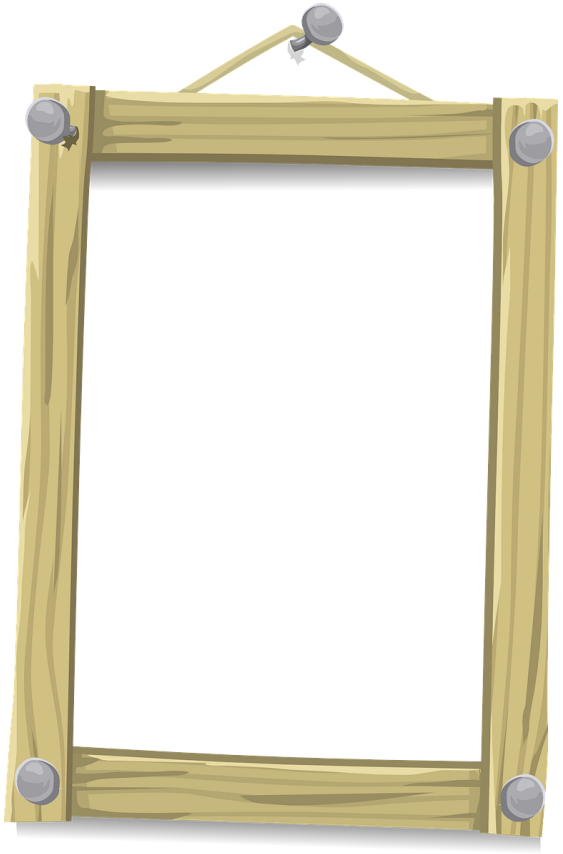
- Inform about processing.
- Meet security requirements.
- Delete personal data when it is no longer necessary for the purpose for which it was collected.
- Ensure continuity of protection when personal data is shared with third parties.
- Submit to judicial review so that EU citizens can access legal remedies.



What is new/required on the US side?

A critic would say that TADPF does not address:

- **US surveillance legislation (e.g. FISA 702).**
- **EU citizens are not given the same (constitutional) rights to privacy as US citizens.**
- **TADPF has an incorrect “proportionality concept” cf. EU law.**
- **The court in the new framework is not a court but an executive body.**
- **…**



TADPF:s future?

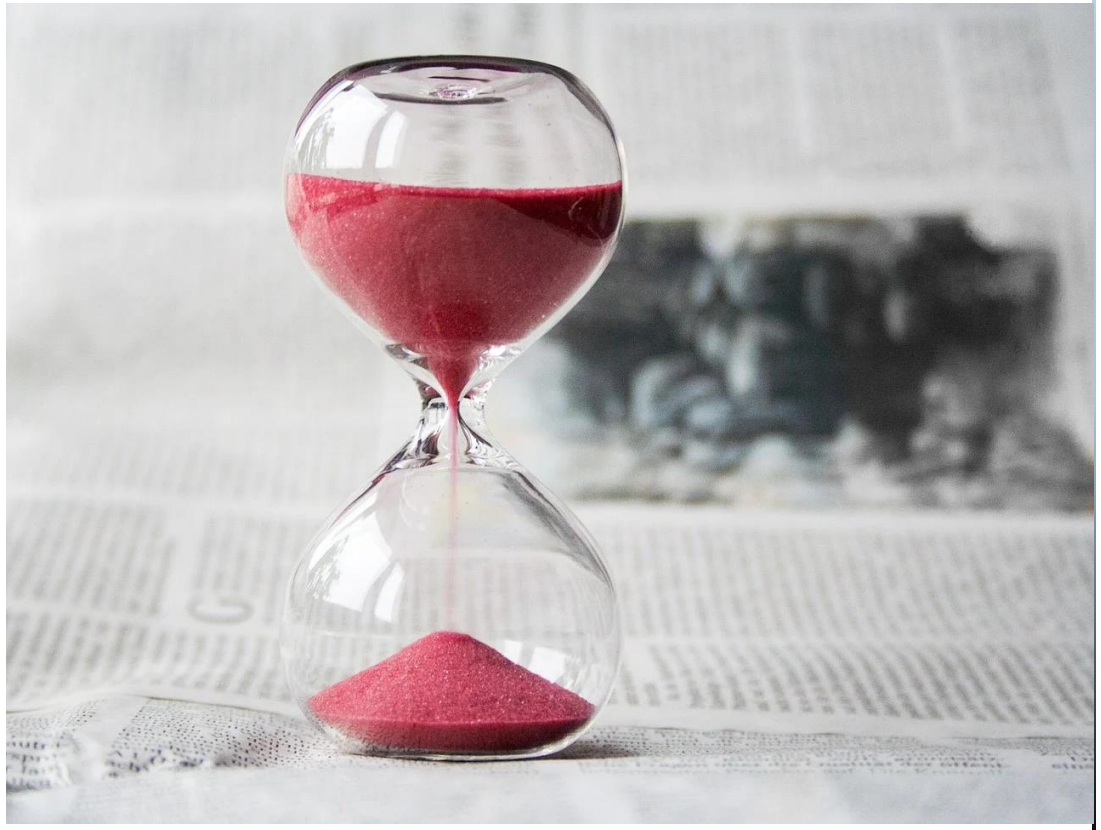
- **Unless EU rule of law is set out of order TADPF will not, under any circumstances, hold unless new judges appointed.**
- **Can still be challenged on cause of breach with EU law.**
- **Possible that Trump administration will repeal the TADPF.**

Max Schrems:

"*We now had 'Harbors', 'Umbrellas', 'Shields' and 'Frameworks' - but no substantial change in US surveillance law. The press statements of today are almost a literal copy of the ones from the past 23 years. Just announcing that something is 'new', 'robust' or 'effective' does not cut it before the Court of Justice. We would need changes in US surveillance law to make this work - and we simply don't have it.*"

AI and personal data

- **(What is AI Act? (simplified view))**
- **What GDPR-compliance issues can you meet when using AI?**



Introduction to the AI Act

- **Adopted in 2024**
- **Applies to providers, deployers, importers, and distributors of AI systems in the EU market**
- **Risk-based classification: unacceptable, high, limited, and minimal risk AI systems (more on this next slide)**

Providers: Organizations or individuals who develop or supply AI systems, responsible for their design, creation, and offering in the EU market.

Deployers: Entities that implement or operate AI systems in real-world settings, ensuring proper integration and use within specific applications.

Importers: Parties bringing AI systems into the EU market from outside the EU, responsible for ensuring compliance with regulations before sale or distribution.

- **Distributors:** Businesses that distribute AI systems within the EU, facilitating access to the market while ensuring adherence to regulatory requirements.

Main parts of the AI Act

1. **Risk-Based Approach**: The Act categorizes AI systems into different risk levels—unacceptable, high, limited, and minimal—regulating each accordingly.
2. **Prohibition of Unacceptable Risk AI**: AI systems that pose a clear threat to safety, fundamental rights, or are considered unacceptable (e.g., social scoring by governments, exploitation of vulnerabilities) are prohibited.
3. **Strict Requirements for High-Risk AI**: High-risk AI systems (such as those used in critical infrastructure, employment, law enforcement, and biometric identification) must meet strict standards, including:
    1. Risk management systems
    2. Data governance and quality measures
    3. Transparency obligations
    4. Human oversight
    5. Robustness and accuracy

1. **Transparency Obligations**: Certain AI systems, especially those interacting with humans or used for biometric identification, must provide clear information to users about their functioning.
2. **Governance and Oversight**: The establishment of national competent authorities and a European AI Board to oversee implementation, compliance, and enforcement.
3. **Conformity Assessments**: High-risk AI systems need to undergo conformity assessments before being placed on the market or used.
4. **Innovation Facilitation**: Provisions to support innovation, including regulatory sandboxes to test AI systems under controlled conditions.
5. **Penalties for Non-Compliance**: Significant fines and penalties for violations, potentially up to 6% of global annual turnover.

Key Obligations for High-Risk AI Systems

- **Subject to conformity assessments before market placement**
- **Mandatory risk management, data governance, and technical documentation**
- **Human oversight, transparency, and cybersecurity requirements**

Requirements for Limited and Minimal Risk AI Systems (limited to AI Act)

Limited Risk AI:

- **Must incorporate appropriate transparency measures (e.g., informing users they are interacting with AI).**
- **Developers should provide clear instructions to ensure safe and responsible use.**
- **Monitoring and documentation to mitigate potential risks.**

Minimal Risk AI:

- **Generally, no specific regulatory obligations.**
- **Allowed to be freely developed and used.**
- **Encouraged to follow existing standards and best practices to promote safe AI deployment.**

NOTE! All AI:s have to conform to other legalisation applicable (e.g. GDPR).

Introduced in steps

Entry into force: 2024-05-21. Main parts applicable from 2026-05-21. Some exceptions:

- **6 months after entry into force**
  - **Prohibited AI practices are banned.**
- **12 months after entry into force**
  - **Obligations for providers of general AI models.**
- **18 months after entry into force**
  - **Commission implements aftermarket surveillance.**
- **24 months after entry into force**
  - **Obligations for high-risk AI systems listed in Annex III, such as AI systems in biometrics, critical infrastructure and law enforcement**
  - **Member States must implement rules on penalties and administrative charges.**
  - **At least one national AI regulatory sandbox must be established.**
- **36 months after entry into force:**
  - **Obligations for high-risk AI systems listed in Annex II.**
- **By 2030 at the latest:**
  - **Obligations for certain AI systems that are components of large-scale IT systems established by the EU in the area of freedom, security and justice.**

AI Act and GDPR – Intersection with Personal Data

- **AI systems often process personal data, triggering GDPR obligations.**
- **Controllers must ensure lawful basis, transparency, and purpose limitation.**
- **Now to the question: What compliance issues exists?**

Issues with AI in relation to compliance

Data Minimization and bias/discrimination: ML models often require large amounts of data to train effectively minimize risk of bias/discrimination. Collecting and using vast amounts of data can violate the GDPR's principle of data minimization.

Purpose Limitation: The use of ML models may lead to secondary uses of personal data that were not explicitly stated at the time of data collection, which leads to conflicts with the principle of purpose limitation.

Transparency: When using personal data organizations are required to be able to describe what is done. Many ML models are opaque (often referred to as "black box" models), making it difficult to explain how personal data is used and processed.

Issues with AI in relation to compliance p2

Individual Rights: According to EU law individuals has rights such as access to their data, the right to rectification, and the right to explanation regarding automated decision-making. Ensuring these rights can be challenging with complex ML models.

Legal basis for processing personal data: Legal basis under GDPR poses challenges for ML because individuals can withdraw consent or object to processing, and then data being required to be removed from the ML model (underlying training datasets), which can disrupt the entire model.

Issues with AI in relation to compliance p3

Hallucinations / incorrect data: AI hallucinations pose risks to GDPR compliance by generating incorrect data. Additionally, hallucinations can contain erroneous information as part of eg customer service which can lead to contractual or civil liability for organizations.

Data leakage: Data leakage in machine learning models poses a compliance risk as it can lead to unauthorized access or inadvertent exposure of sensitive information or personal data.

Contact

Data Law Center

Mattias Gotthold

Mattias.gotthold@datalawcenter.se

+46 (0)70 288 27 74