research institute

Technical University Vienna (TU Wien)

Digital Humanism Initiative

DIGHUM Lecture

International Data Transfer and Sovereignty from a European Perspective

Ing. Dr. iur. Christof Tschohl

13. May 2025, 17:00 - 18:00h

research institute

Dr. iur. Christof Tschohl

- Since 2012: Scientific Director and Partner of the Research Institute AG & Co KG - *Centre for Digital Human Rights*
- Communications engineer (HTL, Ericsson, Kapsch) and lawyer
- Until 2012 at the Ludwig Boltzmann Institute of Human Rights (BIM) and at the University of Vienna
- Research and organisational consulting - interface between technology, law and organisation
- Teaching: Research Institute Academy; TÜV Austria Academy; University of Vienna; University of Applied Arts Vienna; University of Malta; Education of Austrian Judges.
- Memberships:
  - Austrian Computer Society (OCG), Head of the "Forum Privacy" working group
  - Austrian Association of Judges, Section for Fundamental Rights, extraordinary member
  - Member of the CERT Advisory Board of the Austrian Federal Chancellery
  - NOYB (Non Of Your Business) - Association for Data Protection Law Enforcement, founding member and board member together with Max Schrems and Petra Leupold
  - President (retired) of the Austrian Chess Federation (ÖSB) 2021-2022

Research Institute AG & CO KG-
Digital Human Rights Centre

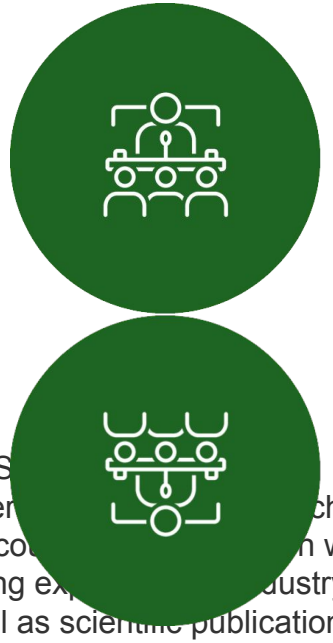
Florianigasse 55/10
1080 Vienna

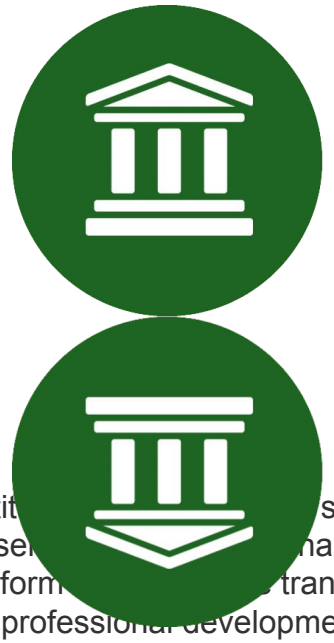
www.researchinstitute.at

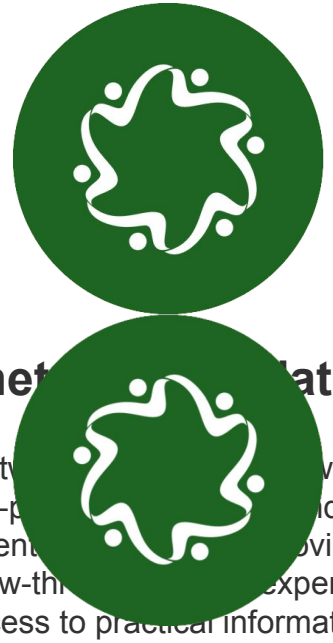
Research Institute

Research

Scientific research at the interface of technology, law and society. Questions concerning fundamental rights as well as social consequences and ethical aspects of new technologies.







Institut… sees itsel… nary platform… transfer and professional development in the fields of technology, law, administration and ethics.

net… …ata

net… …work of non-p… …d social ent… …ovides low-thr… …expensive access to practical information on data protection with regard to NPOs.

Introduction and overview

European Fundamental Rights and EU Regulation a claim of sovereignty in a globalized digital world

research institute

Data protection, information security, AI regulation, product safety, liability, data spaces, etc.

The risk-based approach and the human rights-based approach as guard rails for digitalisation

Cybersecurity

- **European cyber security strategy**
- **Main objectives**:
  - Resilience, technological sovereignty and leadership;
  - operational capability to prevent, deter and respond;
  - Working together to promote a global and open cyberspace.
- **Data strategy** Teil of the Security Union Strategy
- **Six legal acts in the cluster:**
  - Network and Information Security Directive (NIS2-RL)
  - Critical Entities' Resilience Directive (CER Directive)
  - Digital Operational Resilience Act (DORA)
  - Cyber Resilience Act (CRA)
  - Cyber Solidarity Act
  - Cyber Security Act (CSA)

European Commission

Further information:

- https://wiki.atlaws.eu/index.php/Cybersecurity

Cybersecurity

Legal acts at a glance

NIS2 Directive (Network and Information Security Directive)

- Objective: To ensure a high common level of security for network and information systems in the EU. Organisations in the sectors concerned must introduce strict risk management measures and report security incidents.

CER Directive (Critical Entities' Resilience Directive)

- Regulates **physical security and prevention** of critical infrastructures in a focussed manner. The target group is narrowly defined. The Commission will issue **guidelines** that further specify the CER Directive measures. Starting points for the implementation of the NIS2 Directive.

DORA (Digital Operational Resilience Act)

- Covers **the financial sector** and sets out detailed requirements for IT risk management. Guidelines published under DORA (RTS/ITS) Starting points for the implementation of the NIS2 Directive.

Cyber Resilience Act (CRA)

- Introduce cyber security requirements for products with digital elements. Addressees must carry out **certifications**. Should make it easier to secure supply chains in the long term.

Cyber Solidarity Act

- European cyber security shield Analysis of collected data using AI and data analytics Detection of cyber threats and incidents by networked SOCs (national/sectoral level: ASOC) Ausgabe Cross-border alerts for identified threats

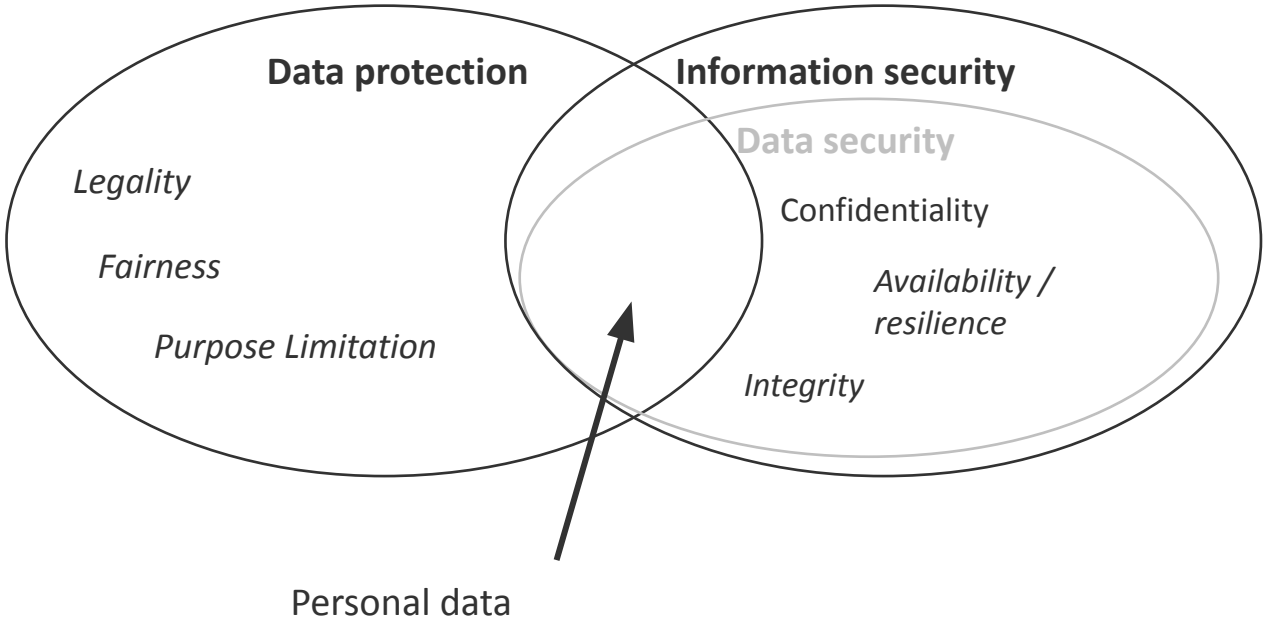
Cyber Security Act (CSA)

- The CSA established an EU-wide certification system for ICT products and strengthened the mandate of the European Cybersecurity Agency (ENISA). CRA

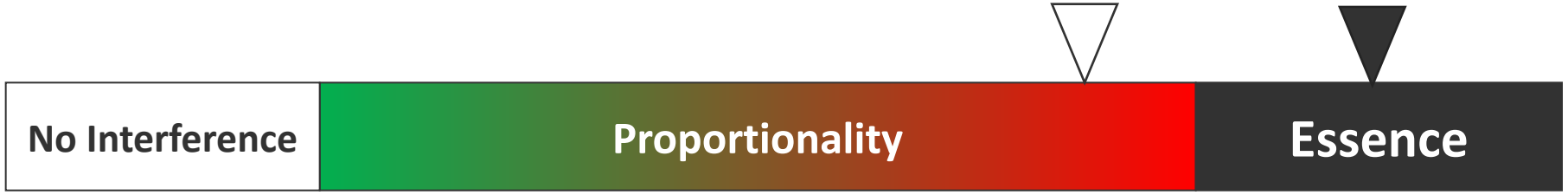
Data protection and information security inseparable siblings

Strict earmarking
Compulsory justification

"need to know" principle
Authorisation concept



The “Essence” of a fundamental rights guarantee



1. Legitimate aim for the measure
2. Measure suitable to achieve the aim
3. Measure must be necessary to achieve the aim (Less onerous way?)
4. Measure must be reasonable, considering the competing interests of different groups at hand

Slide provided by Max Schrems ©

Democratic legitimation of technical standards?

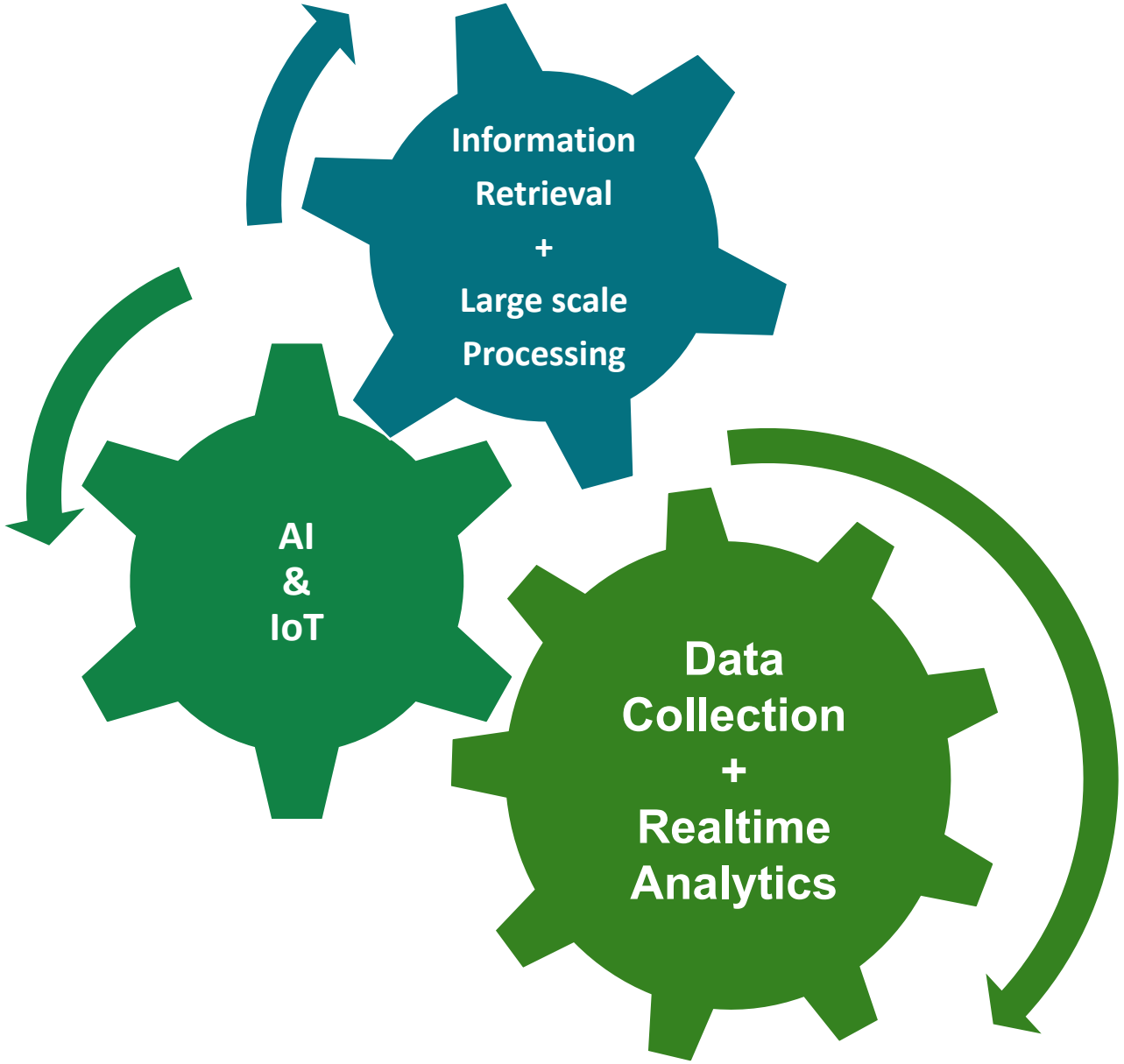
Who defices the standards?

IEEE, ITU, ETSI,… ?!
Who is who defines "The Net" ?

How are Standards legitimized?

The "normative power of facts" (compare "RFCs")

- The "Market" ?!
- The community ?!
- …… ?!



Digital Human Rights – Background and Concept

Data protection is not covering "digital" human risks fully

See e.g. „computer-fundamental-right" in Germany

UN Human Rights Counsel, Resolution A/HRC/20/L.13 (2012):

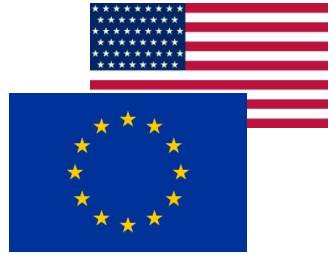
All "classical" human rights do also apply "online"

EU new legislative framework

Fundamental Rights Impact Assessment (Art 27 AI Act)

Data Protection Impact Assessment (Art 35 GDPR)

Safe Harbor and EU-US Privacy Shield a historic review…



Problem:

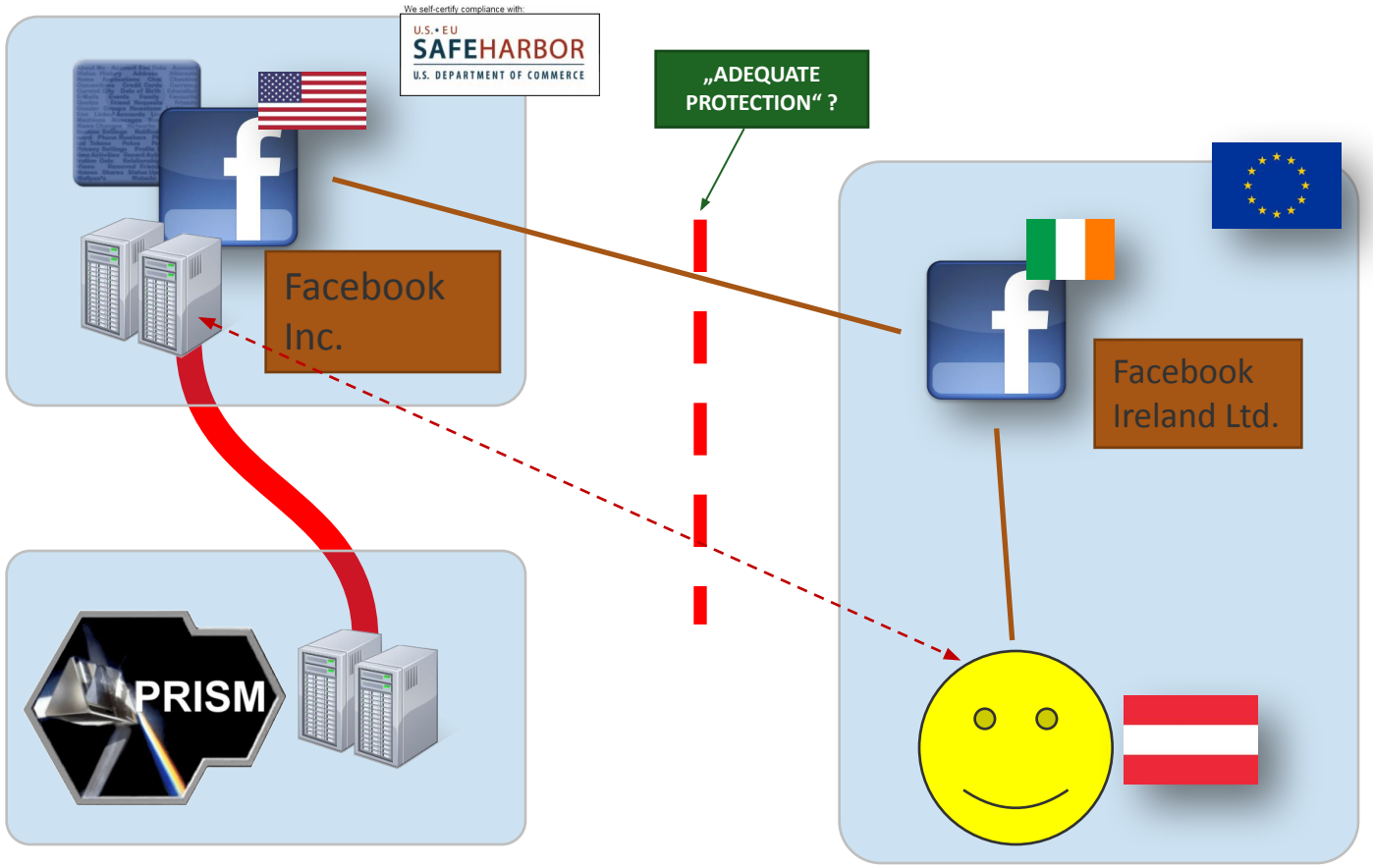
- Directive 95/46/EC
- No general data protection law in the US

Solution:

- „Self-Certification“ to „EU-Principles“
- Executive Decision 520/2000 of EU Comission

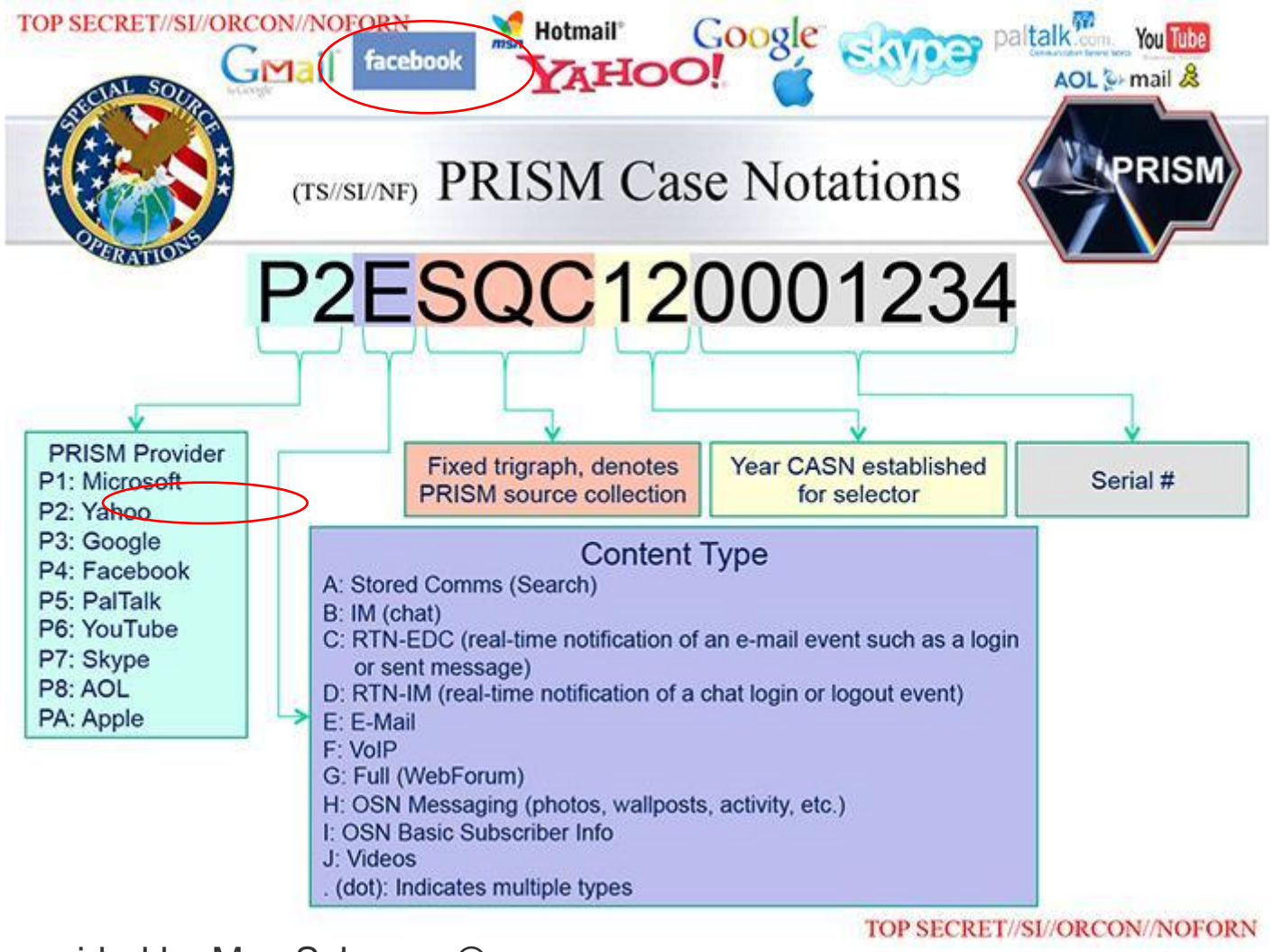
„Europe vs Facebook“ (Max Schrems) and Safe Harbor

The „Safe Harbor“ Decision of ECJ („Schrems I“)



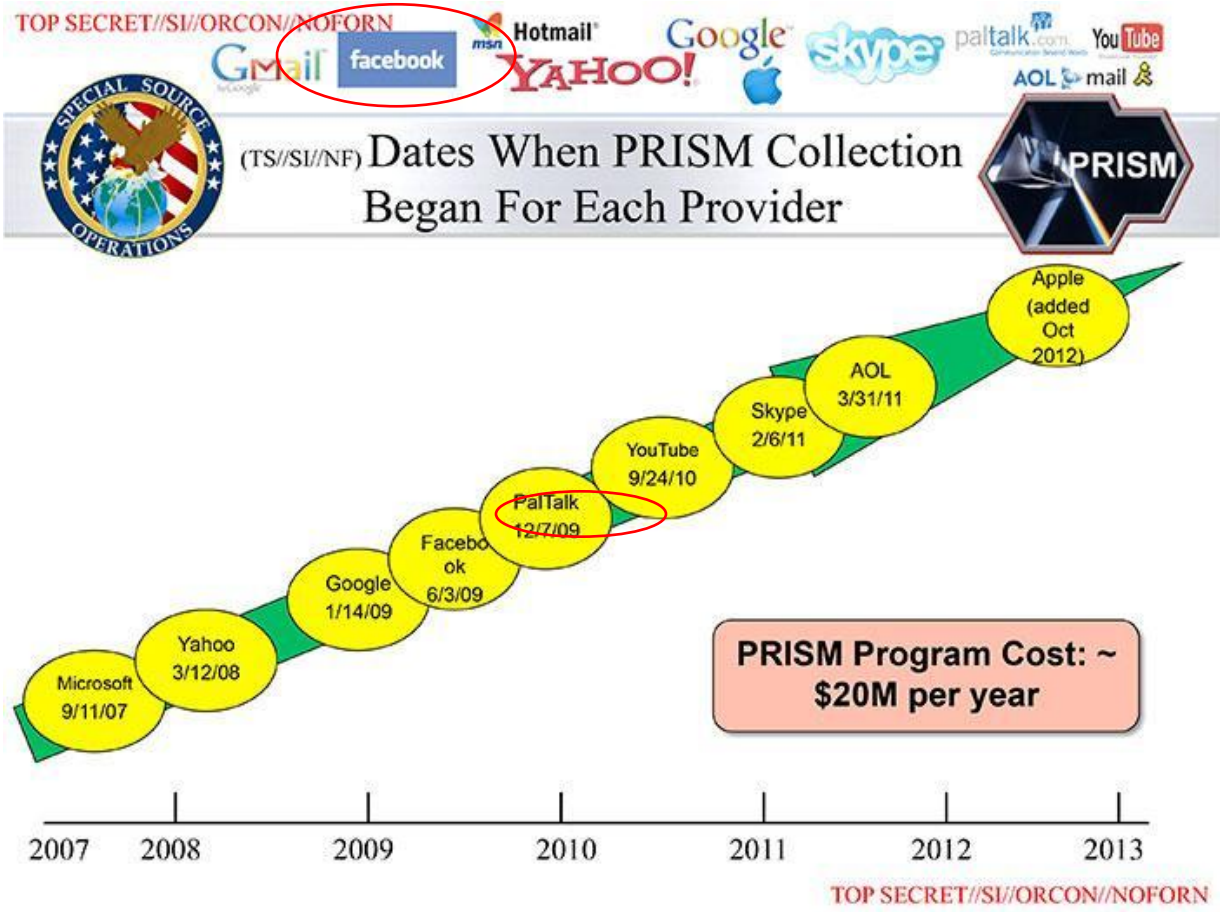
Slide provided by Max Schrems ©

What we learned from Edward Snowden…
…while the ECJ was negotiating „data retention“



Slide provided by Max Schrems ©

…and in April 2014 ECJ abolished „Data Retention Directive“ due to a Violation of Article 7 CFR



Slide provided by Max Schrems ©

Judgement of the European Curt of Justice on „Safe Harbor“ („Schrems I“ C-362/14)

- Court finds „Save Harbor“ Decision invalid
  - Mass Surveillance **violates “essence” of Art 7 CFR**
  - Legal Redress in the US **violates “essence” of Art 47 CFR**

- Also required but not provided by „Safe Harbor“ according to ECJ:
  - “Essentially Equivalent” protection in 3rd country
  - Effective detection and supervision mechanisms
  - Legal redress in line with Art 47 CFR

- „Solution“ from 2016-2020:
  „EU US Privacy Shield“

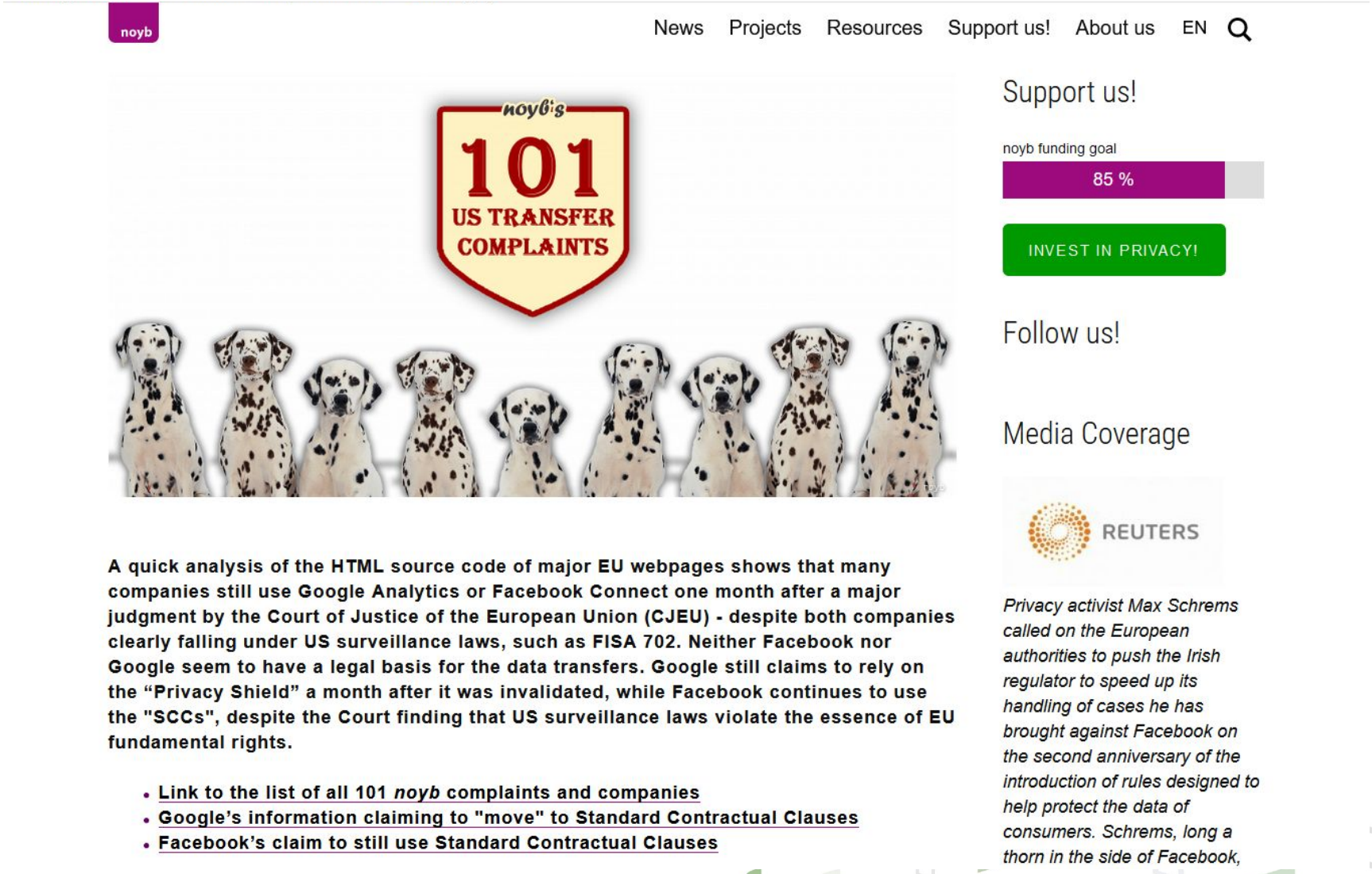
Some smaller improvements
but basically „more of the same“

research institute

The end of EU-US-Privacy Shield
EJCs „Schrems II“ decision

- Transfer of personal data to countries with an in-adequate level of data protection is only permitted in exceptional cases by GDPR
- One exceptional case **was** the EU-US Privacy Shield, an agreement between the USA and the EU for data transfers to the USA
- Transfer of personal data was often justified on the basis of EU-US Privacy Shield
- ECJ declared "EU-US Privacy Shield" invalid on 16 July 2020, ECJ C-311/18 “Schrems II”-Decision (without any transition period!)
- Concerns, amongst others, all US based “hyper scaler” services: Google, Facebook, Amazon, Microsoft, Apple,...

Strategic Litigation by NOYB on international data transfer: targeting „Google Analytics“ & Co



noyb

News Projects Resources Support us! About us EN

noyb's 101 US TRANSFER COMPLAINTS

A quick analysis of the HTML source code of major EU webpages shows that many companies still use Google Analytics or Facebook Connect one month after a major judgment by the Court of Justice of the European Union (CJEU) - despite both companies clearly falling under US surveillance laws, such as FISA 702. Neither Facebook nor Google seem to have a legal basis for the data transfers. Google still claims to rely on the “Privacy Shield” a month after it was invalidated, while Facebook continues to use the "SCCs", despite the Court finding that US surveillance laws violate the essence of EU fundamental rights.

- **Link to the list of all 101 *noyb* complaints and companies**
- **Google’s information claiming to "move" to Standard Contractual Clauses**
- **Facebook’s claim to still use Standard Contractual Clauses**

Support us!

noyb funding goal

85 %

INVEST IN PRIVACY!

Follow us!

Media Coverage

REUTERS

Privacy activist Max Schrems called on the European authorities to push the Irish regulator to speed up its handling of cases he has brought against Facebook on the second anniversary of the introduction of rules designed to help protect the data of consumers. Schrems, long a thorn in the side of Facebook,

Source: https://noyb.eu/en/101-complaints-eu-us-transfers-filed

Important decisions of the ECJ
End of the EU-US Privacy Shield, Schrems II

- Transfer of personal data to countries with a "low" level of data protection is therefore only permitted in exceptional cases
- One exceptional case was the EU-US Privacy Shield (adequacy decision)
- Transfer of personal data was often justified by organizations on the basis of this EU-US Privacy Shield
- ECJ declared "EU-US Privacy Shield" invalid on July 16, 2020 (ECJ C-311/181) (no transition period!)
- Concerns among others: Google Analytics, Facebook pages, YouTube, various newsletter services, etc
- Backup-Path: other legal justification (in particular standard contractual clauses "SCCs", contract performance, consent for certain cases)

research institute

Important decisions of the ECJ
End of the EU-US Privacy Shield, Schrems II

- Critical here are transfers to US companies that fall under a US "mass surveillance" law such as FISA 702 (also known as 50 USC §1881a)
- Concerns so-called "Electronic Communication Service Providers".
- Includes most IT and cloud providers
- Examples: Amazon (AWS), Apple, Cloudflare, Dropbox, Facebook, Google, Microsoft, Verizon media (known as Oath & Yahoo) or Verizon.
- Concerns typical "outsourcing" situations (i.e. when an organization transfers its data to a US company, which in turn processes its data)

Standard Contractual Clauses (SCC)

- Standard Contracting Clauses (SCCs) are the most important legal basis for US data transfers following the repeal of the EU-US Privacy Shield.
- SCCs are model contracts concluded between controllers or processors and recipients of the data (especially when using US services).
- In certain cases, SCCs must be supplemented by so-called "additional guarantees", i.e. those responsible may have to take additional measures to ensure compliance with an equivalent level of protection.

Austrian DPA decision on "Google Analytics„ I Decision of the data protection authority D155.027 GA

- online published at (German only): https://www.dsb.gv.at/dam/jcr:c1eb937b-7527-450c-8771-74523b01223c/D155.027%20GA.pdf
- Website of an Austrian provider uses Google Analytics.
- This is a Google tool with which a website operator can create detailed reports on the usage behavior of website visitors. By using the IP address or certain browser data, it is possible to assign a unique digital footprint to a person.
- If this person is logged into their Google account while accessing the website, the information about the website visit can be clearly assigned to the respective account.
- The "digital footprint" is transmitted to servers of Google LLC based in the USA - without anonymization of the IP addresses.
- Measures implemented in addition to SCC are not effective against monitoring.
- level of protection was not sufficiently established and Google Analytics was therefore not used in accordance with the GDPR.

Austrian DPA decision on "Google Analytics" II
Decision of the data protection authority D155.027

- published online at https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf
- Website of an Austrian provider uses Google Analytics in the variant with anonymization of the IP address.
- The anonymization of the IP address does not change the result in comparison to the first decision of the DSB, as the anonymization only takes place after the transmission to the USA.
- NEW in this decision, however, are the statements on the risk-based approach of the GDPR in relation to the provisions on third country transfers in Art 44 ff GDPR.
- Provisions on the requirement of an "adequate level of protection" do not themselves recognize a risk-based approach - regardless of other provisions of the GDPR
- This means that a low risk alone - and one that is acceptable from the perspective of the controller - is not sufficient to legitimize the transfer of data to a third country without an adequate level of protection.
- Measures within the meaning of the instruments of Art. 44 ff GDPR are therefore always required to justify an appropriate level.
- See now also the confirmation by the Federal Administrative Court in the appeal proceedings, BVwG 12.05.2023, W245 2252208-1; W245 2252221-1 https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20230512_W245_2252208_1_00/BVWGT_20230512_W245_2252208_1_00.pdf

Other relevant decisions in the EU noyb initiative on Google Analytics

- **France + Italy:**

- In addition to the French data protection authority (CNIL), the Italian DPA has also ruled that the transfer of data to Google Analytics is unlawful. The authorities prohibit website operators from using Google Analytics.
- Both decisions are based on the 101 model complaints filed by noyb following the ECJ's ruling on the invalidity of the Privacy Shield. noyb expects similar decisions from other authorities.
  - https://noyb.eu/de/update-cnil-entscheidung-eu-us-datenuebermittlung-google-analytics-illegal
  - https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9782874#english

- **EDPS:**

- At the beginning of 2021, the European Data Protection Supervisor published a decision in a complaint by noyb confirming that the European Parliament had violated the GDPR by using Google Analytics on its COVID test website.
  - https://noyb.eu/de/edsb-sanktioniert-parlament-wegen-eu-us-datenuebermittlung-google-und-stripe

Recent Developments in EU Data Protection

- Facebook Pixel: DPO March 2023
  - Use of Facebook Pixel without express consent to data transfer to a third country unlawful
  - https://noyb.eu/de/datenschutzbehoerde-meta-tracking-tools-rechtswidrig (with download link to the DSB decision)
- Schrems vs Facebook: € 1.2 billion record fine against Meta in Ireland for unlawful EU-US data transfers
  - After 10 years of proceedings by Max Schrems against Facebook, there are finally consequences for the meta-corporation
  - EDPB largely overturns Irish data protection authority's decision, imposes record fine and calls for data already transferred back to the EU
  - https://noyb.eu/de/edsa-entscheidung-zu-facebooks-datenuebertragung-die-usa

„Transatlantik Privacy Framework“ and Biden's Executive Order 14086 (10/2022)

- "Enhancing Safeguards for United States Signals Intelligence Activities"
  - https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/
- **Internal directive** of the US President with validity within the US government, which regulates **the areas of proportionality of data transfer to US intelligence services** as well as a **complaints office** and is intended to increase the level of data protection and improve legal certainty for US data transfers
- This should eliminate the criticism of the ECJ that there are no restrictions on surveillance and, above all, no legal protection for non-US citizens Problem: the "regulation" (according to Austrian legal terminology) is not above US law:
- Cf. further differentiated criticism by Max Schrems: https://noyb.eu/de/executive-order-zur-us-ueberwachung-reicht-wohl-nicht
- European "implementation" by means of an **adequacy decision** by the Commission Draft published in December 22, consultation of the European Data Protection Board (EDPB) and consultation of the Member States completed, valid since 10.07.2023

ECJ „Schrems III“?
One way or another: DPF will fail (again)…

- Fundamental Critics: the same old problem remains…
  - Proportionality has a different meaning within the executive order
  - it is only an executive order easily to be overruled by the Trump-administration
  - As an executive order it is unlikely to actually change intelligence services behaviour (FISA 702 is the law and their measurement)
- "Privacy and Civil Liberties Oversight Board" (PCLOB): the key US oversight authority
  - that Democratic members of the PCLOB got removed and their email accounts shut down. This brings the number of appointed Members below the threshold to have the PCLOB operate.
  - The fact that the US President simply removed people from an (allegedly) independent authority, question the independence of all other executive redress bodies in the US.
  - https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal
  - This might be sufficient for EU Commission to revoke the adequacy decision
  - Otherwhise „Schrems III“ is going to be decided soon by ECJ…

research institute

Artificial Intelligence (AI) and other EU Regulation

Data Protection and AI Act

killjoy for the market or humanistic survival?

EDPB Opinion on data protection aspects

- EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024 https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf
- "For an **AI model** to be considered **anonymous**, both
  - (1) the likelihood of direct (including probabilistic) extraction of personal data regarding individuals whose personal data were used to develop the model and
  - (2) the likelihood of obtaining, intentionally or not, such personal data from queries, should be insignificant, taking into account 'all the means reasonably likely to be used' by the controller or another person."
- **List** of methods that may be used by controllers in their demonstration of anonymity
- If it is not documented/cannot be demonstrated that effective measures were taken to anonymise the AI model, although this is claimed, the controller has potentially failed to meet its accountability obligations under Article 5(2) GDPR.

research institute

Artificial Intelligence Act (AI Act)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Artificial Intelligence Act

Subject matter and objectives:

Improve the functioning of the ***internal market***
Promotion of human-centred and ***trustworthy AI***
ensure a ***high level of protection in terms*** of health, safety and the fundamental rights enshrined in the Charter from the harmful effects of AI systems
Support for ***innovation***

Area of application:

Substantial:
- AI systems
- GPAI models

Spatial:
- providers placing on the market or putting into service AI systems in the Union
- deployers of AI systems established or located in the EU
- Providers or distributors established in a third country if the output is used in the Union

Affected institutions / sectors:

Cross-sector
State and ***private*** AI providers and users (as well as dealers, importers, etc.)

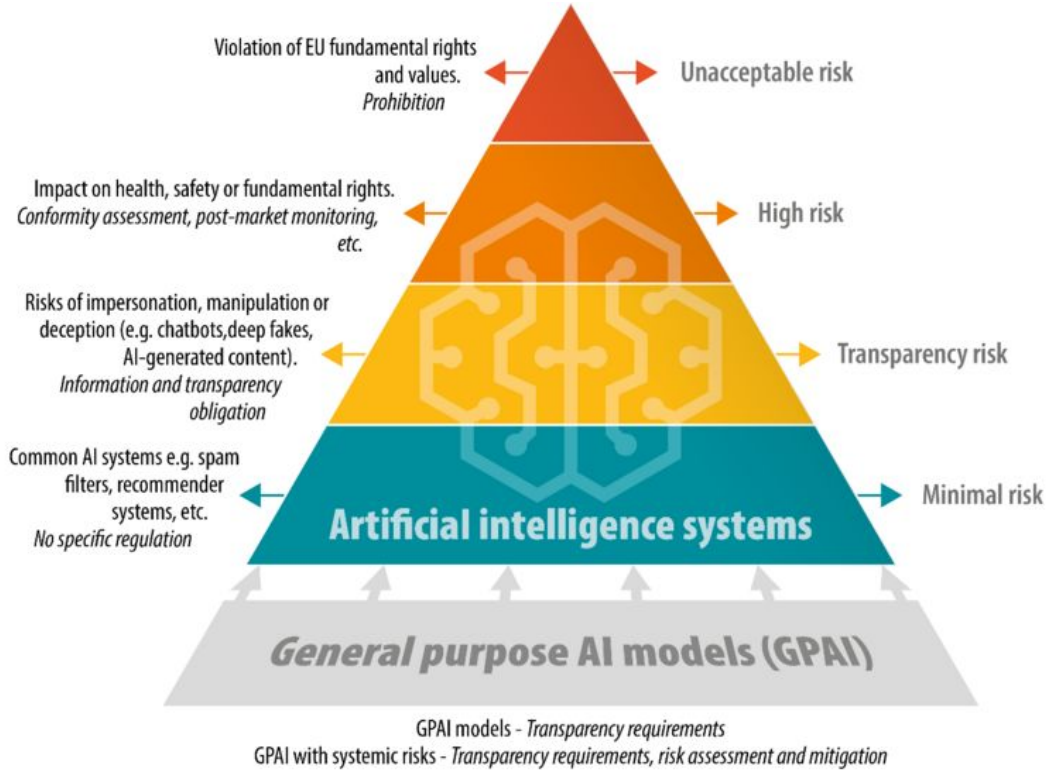
Relief for SMEs
Exceptions, e.g. in the area of open source and research

research institute

AI Act

Risk-based approach:

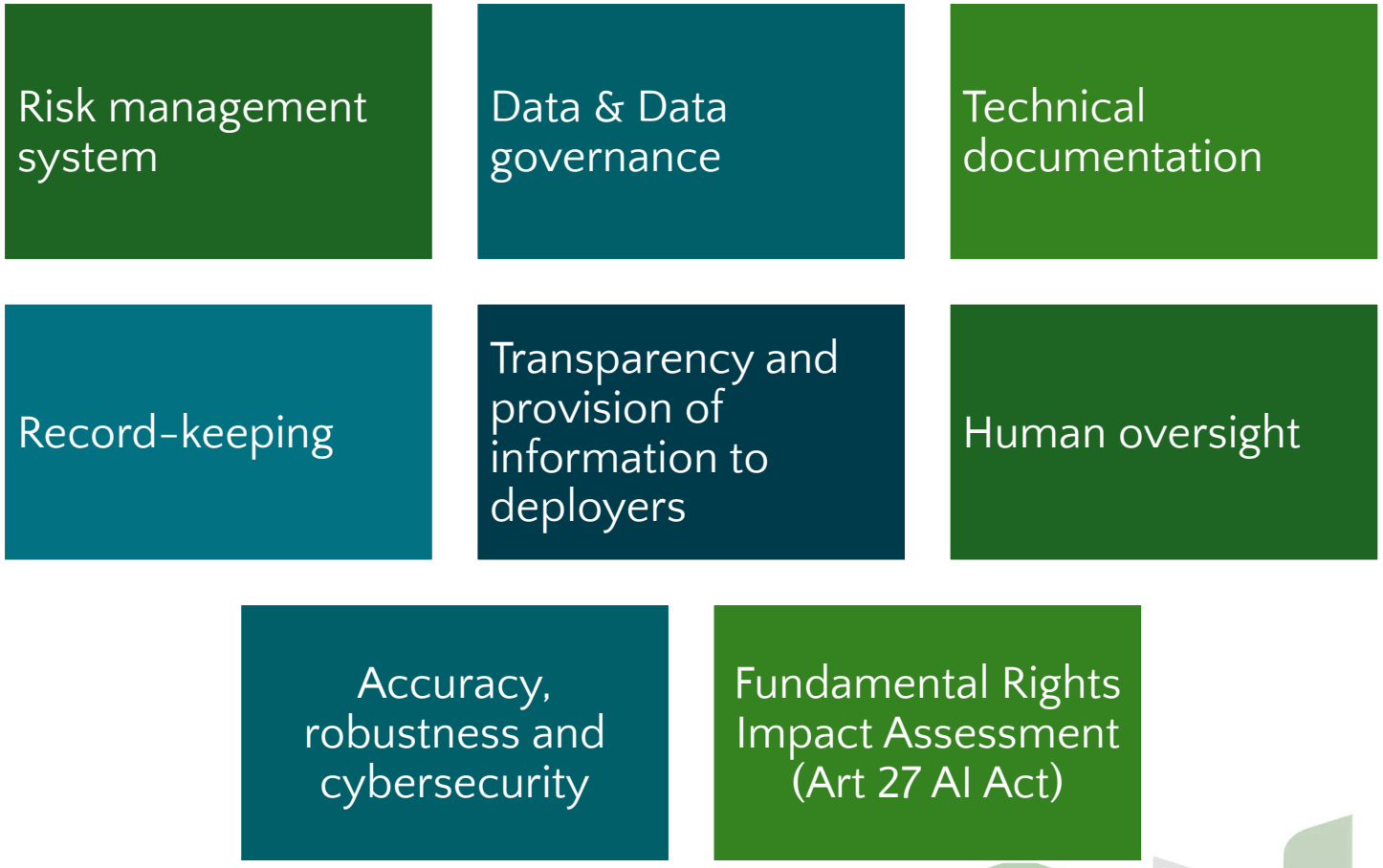
- **Horizontal regulation** (i.e. regardless of the sector) of AI systems and general-purpose AI (GPAI) models
  - mainly rooted in product safety law (compare medical device regulation) +
  - elements concerning the protection of human rights (e.g. fundamental rights impact assessment)
- **Applicability**: August 2026 (prohibited practices/AI literacy since February 2025)
- **Exemptions,** e.g.:
  - national security/military
  - sole purpose of scientific research and development
  - research, testing or development activity
  - open source



Source: European Commission https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

AI Act: Requirements for High-risk AI Systems

(Articles 8-15 and 27 AI Act)



Transparency obligations (Art 50 AI Act)

- Providers of AI systems "intended to **interact directly with natural persons**" (e.g. Chatbot) have a duty to inform about the nature of this interaction
- Providers of AI systems **generating "synthetic audio, image, video or text content**" must ensure that the outputs are marked in a machine-readable format and detectable as artificially generated or manipulated
- Deployers of an **emotion recognition system** or a **biometric categorisation system** have a duty to inform about the operation

- Duties to inform about **artificially generated/manipulated content**
  - Deployers of "Deep Fake" AI systems
  - Deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest

Transparency obligations (Art 50 AI Act)

- Duties to inform about **artificially generated/manipulated content**
  - Deployers of "Deep Fake" AI systems
  - Deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest

research institute

Human oversight (Art 14)

- High-risk AI systems must be designed and developed in such a way that they can be **effectively overseen by natural persons**
  - oversight measures must be commensurate with the risks, level of autonomy and context of use of the high-risk AI system
- **Goal:**
  - prevent or minimise the risks to health, safety or fundamental rights
- Shall **enable** oversight to
  - properly **understand the relevant capacities and limitations** of the high-risk AI system and be able to duly **monitor its operation** (e.g. anomalies, dysfunctions, unexpected performance)
  - remain aware of the possible tendency of automatically relying or over-relying on the output (**automation bias**)
  - **correctly interpret** the high-risk AI system's output (including interpretation tools and methods)
  - **decide not to use** the high-risk AI system or to otherwise disregard, override or reverse the output
  - **intervene** in the operation of the high-risk AI system or interrupt the system

research institute

Accuracy, Robustness and Cybersecurity (Art 15)

- High-risk AI systems must be designed and developed in such a way that they achieve
  - an appropriate level of accuracy, robustness, and cybersecurity
  - they perform consistently in those respects throughout their lifecycle
- **Accuracy: Levels of accuracy/accuracy metrics** must be declared in the instructions of use
- **Robustness**: as **resilient** as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates
- **Technical and Organizational Measures** (TOMs): e.g. redundancy solutions like backup or fail-safe plans
- **Continuous learning** requires special considerations regarding possible feedback loops and resulting bias

research institute

Cybersecurity (Art 15)

- Resilience against attempts by unauthorized third parties **exploiting system vulnerabilities** to alter
  - the use of the high-risk AI system,
  - outputs or
  - performance
- Requires **technical solutions appropriate** to the relevant circumstances and risks
- Technical solutions must include measures to **prevent, detect, respond to, resolve and control** for
  - attacks trying to manipulate the training data set (**data poisoning**)
  - attacks trying to manipulate pre-trained components used in training (**model poisoning**)
  - inputs designed to cause the AI model to make a mistake (**adversarial examples or model evasion**)
  - **confidentiality attacks**
  - **model flaws**

Excursus - ATLAWS

Overview of the regulation of digitalisation in the EU

as Wiki

https://wiki.atlaws.eu

For now only in German, first English Version will be online from 4th June 2025

https://atlaws.eu/

https://wiki.atlaws.eu

- **Basic problem**:
  - (Unmanageable) multitude of EU digital legal acts
  - This makes it difficult to understand the interplay between legal acts
  - Constant change through delegated acts, guidelines, case law
- **Solution approach:**
  - Publicly accessible ATLAWS wiki, which provides an initial "mapping" of the legal acts (e.g. scope of application, core obligations, consequences)
  - Facilitating access to justice
  - enriched with practical examples, references to literature, standards and guidelines
  - Elaboration of synergies with other legal acts
  - Co-creation approach, quality assurance through interdisciplinary workshops
- **4 thematic "clusters", 17 legal acts**
  - Digital services & markets
  - Data strategy
  - Artificial intelligence
  - Cybersecurity

In a nutshell

- ✔ Technology needs to be „Human Centered“(„Human Dignity by Design“)
- ✔ Balance of security and freedom needs an open societal dialog
- ✔ Legal framework needs to consider technological aspects
- ✔ Technology needs to respect limits of human rights („Privacy by Design“)
- ✔ EU shall safeguard and export regulation achievements (DSA, DMA, AI Act, ect)

Human Rights Based Approach: building on the main achievement of 20th century - International Human Rights

research institute

Thank you very much!

Subscribe to our newsletter and

visit us at: www.researchinstitute.at

Questions and discussion

Backup Slides

research institute

AI system

'**AI system**' means

- a machine-based system
- that is designed to operate with **varying levels of autonomy** and
- that may exhibit **adaptiveness** after deployment, and
- that, for explicit or implicit **objectives**,
- **infers**, from the input it receives,
- how to **generate outputs** such as predictions, content, recommendations, or decisions
- that can **influence physical or virtual environments**

Definition of an **AI system** includes

- machine learning and
- logic- and knowledge-based systems
- Guidelines on "AI systems" (February 2025)
  - some "well established" techniques like linear regression, classical heuristics are outside the scope

research institute

Main operators of the AI Act

- **Provider** [=manufacturer]: "a natural or legal person, public authority, agency or other body that **develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed** and **places it on the market or puts the AI system into service under its own name or trademark**, whether for payment or free of charge" (Art 3 (3) AI Act)
- **Deployer** [= professional user]: "a natural or legal person, public authority, agency or other body **using an AI system under its authority** except where the AI system is used in the course of a personal non-professional activity" (Art 3 (4) AI Act)

Beware: "Change if the Role" (Art 25 (1) AI Act)

Any operator is "considered to be a provider of a high-risk AI system [....] in any of the following circumstances:

1. they put their **name or trademark** on a high-risk AI system already placed on the market or put into service, [...];
2. they make a **substantial modification** to a high-risk AI system [...] in such a way that it remains a high-risk AI system [...]
3. they **modify the intended purpose** of an AI system, [...] which has not been classified as high-risk [...] in such a way that the AI system concerned becomes a high-risk AI system [...]

Result: operator becomes new provider; affected by the obligations concerning providers

AI literacy (Art 4)

- measures to ensure **a sufficient level of AI literacy** of staff and other persons dealing with the operation and use of AI systems
- **taking into account**
  - technical knowledge
  - experience
  - education
  - training
  - context the AI systems
  - considering the persons or groups of persons on whom the AI systems are to be used

EDPB Opinion on data protection aspects

- List of methods/elements that may be used by controllers in their demonstration of anonymity of a model:
  - Context of deployment/direct acces to the model
  - AI model design
    - Selection of **sources**
      - appropriateness of the selection criteria
      - relevance and adequacy
      - whether inappropriate sources have been excluded
    - **Data Preparation and Minimisation**
      - Anonymisation/pseudonymisation or reasoning why not
      - Data minimisation
      - Remove irrelevant personal data
    - Methodological choices regarding the **training**
      - regularisation methods to improve model generalisation and reduce overfitting
      - appropriate and effective privacy-preserving techniques (e.g. differential privacy)
  - AI model analysis
  - AI model testing and resistance to attacks
  - Documentation

EDPB Opinion on data protection aspects

- Can controllers rely on **legitimate interest** as an appropriate legal basis for processing conducted in the context of the development and the deployment of AI models?
- **Three-step test**:
    1. Identifying the legitimate interest(s), which shall be
        1. lawful
        2. clearly and precisely articulated
        3. real and present (i.e. not speculative)
    2. Analysing the necessity of the processing for the purposes of the legitimate interest(s)
        1. Suitability
        2. No less intrusive way of pursuing this interest
        3. Proportionality
    3. Assessing that the legitimate interest(s) is (are) not overridden by the interests or fundamental rights and freedoms of the data subjects,
        1. taking into account the specific circumstances of each case and
        2. data subjects' reasonable expectations

Product Liability Directive (PLD)

Subject matter and objectives:

Extension of the ***product concept***: inclusion of "software"
Concretisation of the ***concept of damage***
Extension of ***liability addressees***
Easing the burden of proof
Disclosure obligation

Entry into force: 9 December 2024
24 months implementation period

Area of application:

Objectively:
- movable, defective products (including software and construction documents)
- Exceptions for open source

Spatial:
- National implementation necessary (directive)
- Greater harmonisation in the EU

Institutions concerned:

Sector-independent:
Manufacturers - end manufacturers, parts manufacturers, importers, quasi-manufacturers, suppliers, fulfilment service providers, online platforms

Product Liability Directive (PLD)

Product liability for a digital age

- **Definitions**:
  - "Product" refers to all movable items, even if they are integrated into or connected to another movable or immovable item. This also includes electricity, digital ***construction documents***, raw materials and ***software***.
  - "***Manufacturer***" means any natural or legal person who a) develops, manufactures or produces a product, b) has a product developed or manufactured or acts as a manufacturer by affixing its name, trade mark or other distinguishing features to that product, or c) develops, manufactures or produces a product for its own use.
- **Central contents:**
  - Specification of the ***concept of damage***: death or physical injury; damage to or destruction of property (with an exception); destruction or falsification of data that is not used for professional purposes
  - Specification of the ***defectiveness*** of a product: e.g. effects on the product of the ability of the product to ***continue learning*** or ***acquire new functions*** after it has been placed on the market or put into service; the relevant safety requirements of the product, including safety-related ***cybersecurity requirements***

Product Liability Directive (PLD)

Product liability for a digital age

- **Central contents:**
  - ***Disclosure of evidence:***
    - Obligation of disclosure
    - Evidence of plausibility required
  - ***Burden of proof***
    - ***Assumption of defectiveness*** if
      - Refusal of disclosure
      - Product does not fulfil mandatory product safety requirements
      - Damage due to obvious malfunction
    - ***Assumption of defectiveness/connection between defectiveness and damage*** (or both) in the case of
      - ***Detection difficulties*** due to technical or scientific complexity
      - Proof that the product is probably defective

Product Liability Directive (PLD)

Relationships with other legal acts

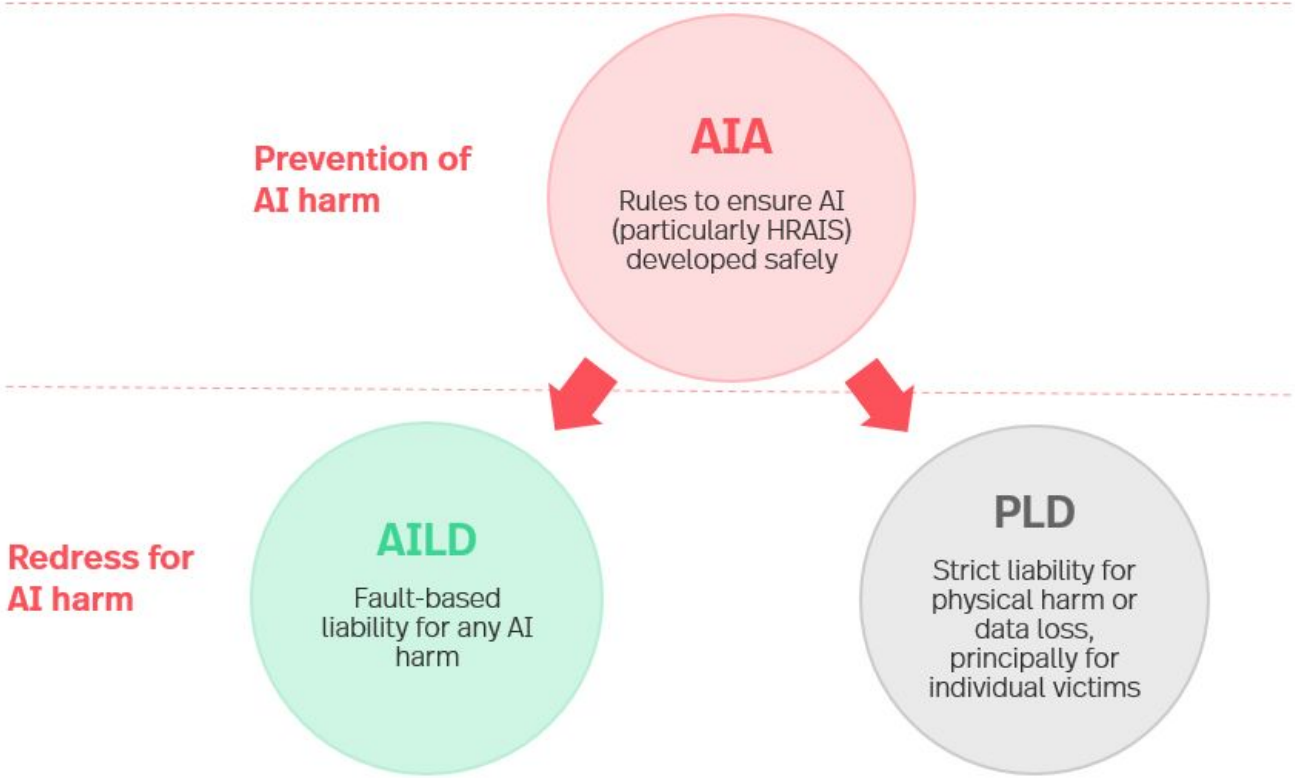


Image source: https://www.simmons-simmons.com/en/publications/cla2fpkgw5uj20a94oaegyszn/what-is-the-new-eu-ai-liability-regime-

Legal information

This document serves as a presentation document for lecturing at University. It was created and edited by Christof Tschohl and the Research Institute team (https://researchinstitute.at/team/)

Disclaimer:

Although the contents of this presentation have been prepared with the utmost care, all information is provided without guarantee, also due to the condensed presentation of the contents, and any liability of the authors and the RI is excluded. The presenters recommend that individual advice be sought prior to the realisation of such projects.

Contact: kontakt@researchinstitute.at