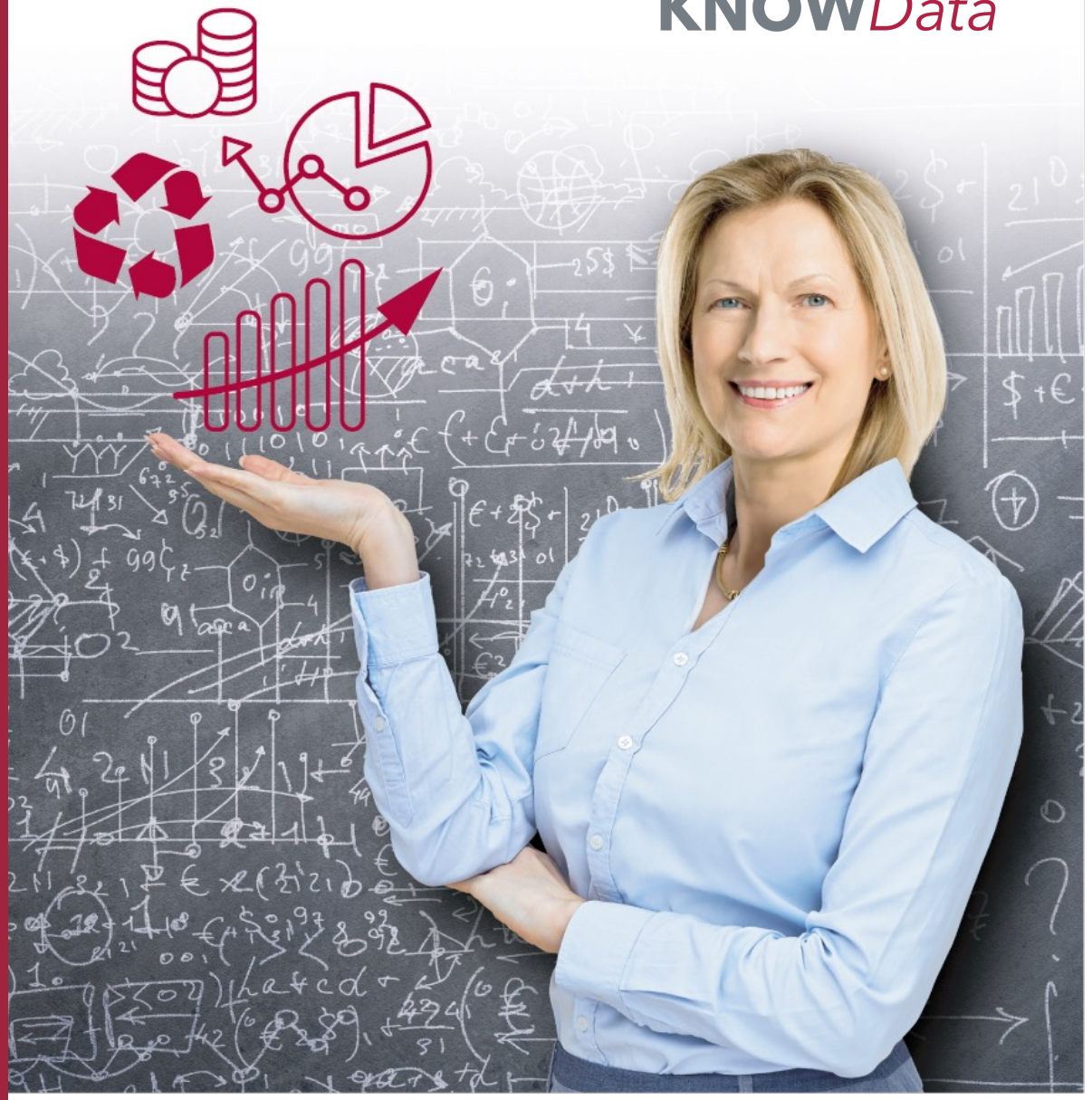
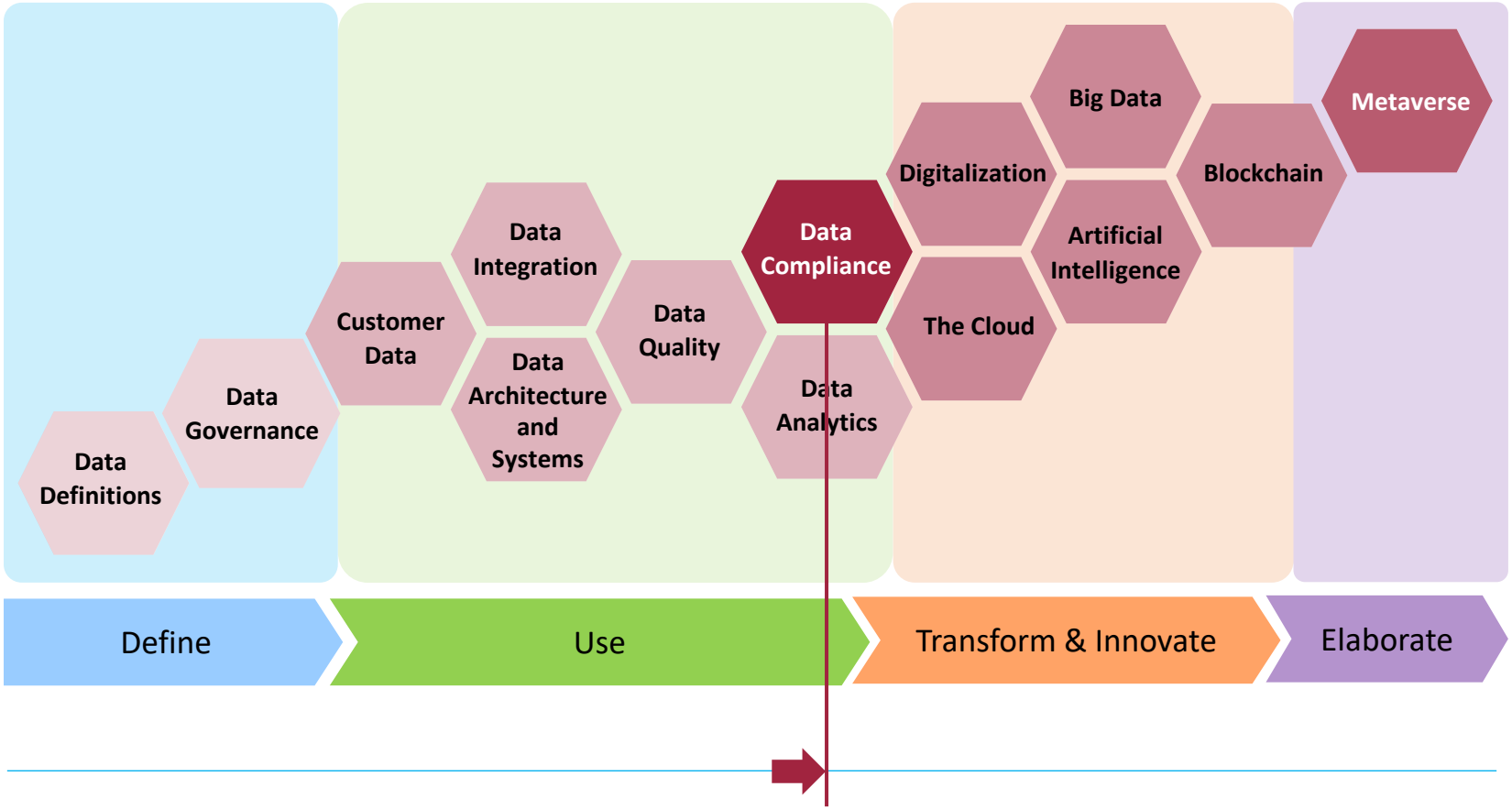
Data Compliance

KNOWData

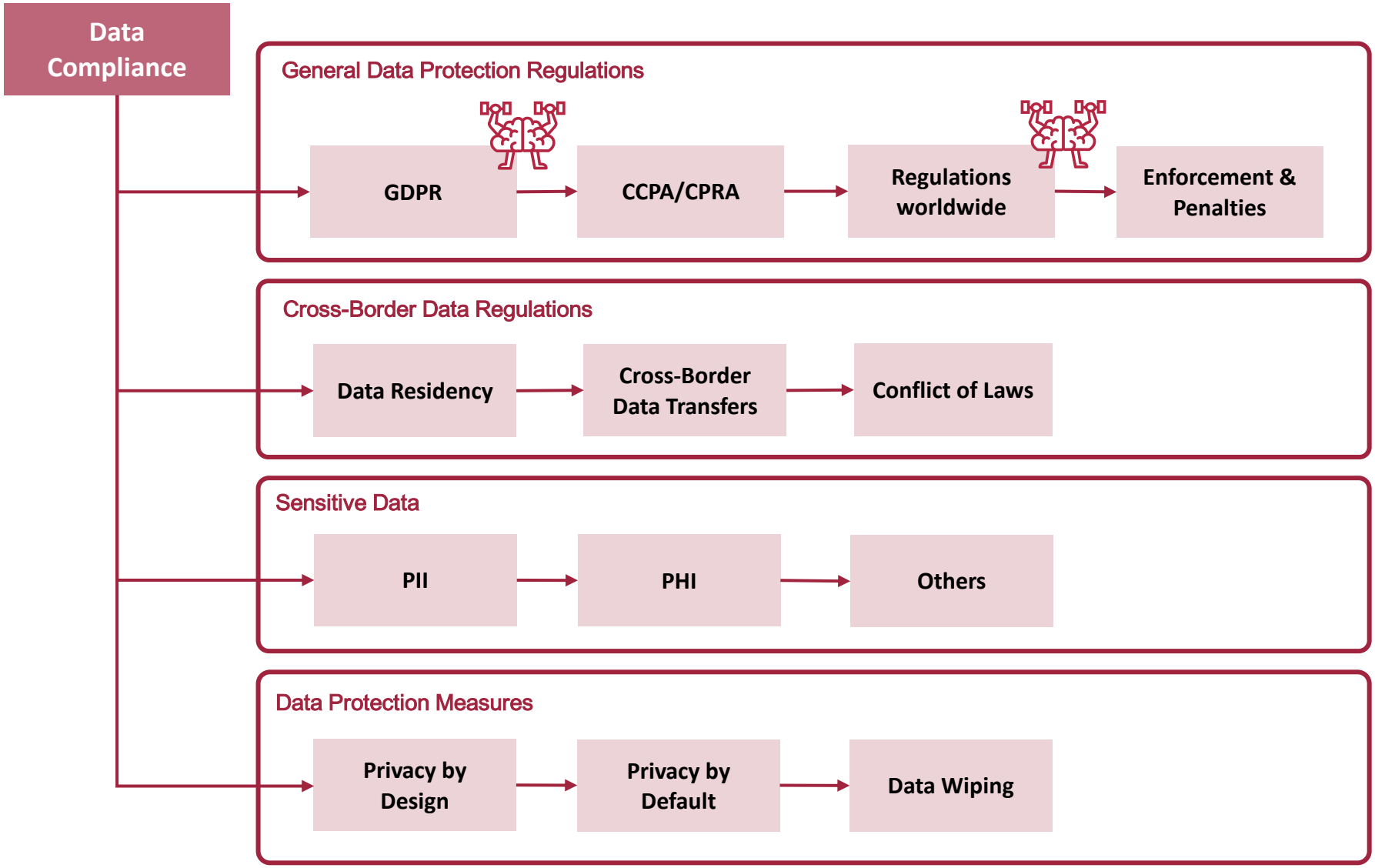


August 04, 2026

Lionel Pilorget


Data Definitions
Data Governance
Customer Data
Data Integration
Data Architecture and Systems
Data Quality
Data Compliance
Data Analytics
Digitalization
The Cloud
Big Data
Artificial Intelligence
Blockchain
Metaverse
Define
Use
Transform & Innovate
Elaborate

Structure of the presentation



What is Data Compliance and Why Is It Important?

Data Compliance is the practice of ensuring that data is handled according to legal, regulatory, and ethical standards.

Data Compliance is a "digital code of conduct".

It's important because it …

- Protects individuals' privacy
- Builds trust between people & organizations
- Avoids legal penalties & fines for businesses
- Provides Market Access as Compliance is often a requirement for doing business in certain regions or industries.

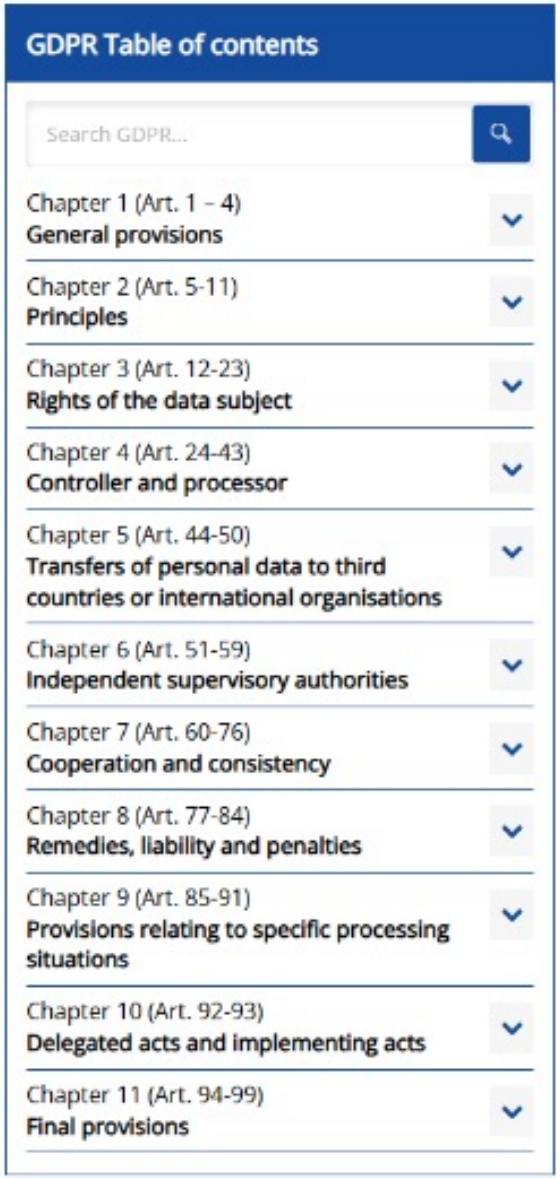
What is GDPR?

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

Source: gdpr.eu/what-is-gdpr/

11 Chapters and 99 Articles



Source: gdpr.eu/tag/gdpr/

173 Recitals of the Regulation

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	**69**	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173							

Recital 69

Right to object

Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

Source: gdpr.eu/Recital-69-Right-to-object/

Key Definitions

The GDPR defines an array of legal terms at length. Below are some of the most important ones that we refer to in this article:

Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.

Data processing — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing... so basically anything.

Data subject — The person whose data is processed. These are your customers or site visitors.

Data controller — The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. These could include cloud servers, like Google Drive, Proton Drive, or Microsoft OneDrive, or email service providers, like Proton Mail.

Source: gdpr.eu/what-is-gdpr/

Processing of Personal Data

Art. 5 GDPR
Principles relating to processing of personal data

1. Personal data shall be:

   a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

   b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

   c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

   d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

   e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

   f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Individual Rights

The information obligations and rights of data subjects listed below must be respected and guaranteed, bearing in mind that restrictions remain possible:

- Transparency of information and communications and arrangements for exercising the data subject's rights (art. 12 GDPR)
- Information to be provided when personal data is collected from the data subject (art. 13 GDPR)
- Information to be provided when personal data has not been obtained from the data subject (art. 14 GDPR)
- Data subject's right of access (art. 15 GDPR)
- Right of rectification (art. 16 GDPR)
- Right to erasure ("right to be forgotten") (art. 17 GDPR)
- Right to limit processing (art. 18 GDPR)
- Obligation to notify rectification or erasure of personal data or restriction of processing (art. 19 GDPR)
- Right to data portability (art. 20 GDPR)
- Right to object (art. 21 GDPR)
- Right to object to a decision based solely on automated processing (including profiling) producing legal effects concerning or significantly affecting the data subject in a similar way (art. 22 GDPR)
- Communication to the data subject of a personal data breach (art. 34 GDPR)

Rights to erasure

Art. 17 GDPR
Right to erasure ('right to be forgotten')

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) or point (a) of Article 9(2), and where there is no other legal ground for the processing;

c. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

d. the personal data have been unlawfully processed;

e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

   a. for exercising the right of freedom of expression and information;

   b. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

   c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

   d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

   e. for the establishment, exercise or defence of legal claims.

Data Protection by Design and by Default

From now on, everything you do in your organization must, "by design and by default," consider data protection. Practically speaking, this means you must consider the data protection principles in the design of any new product or activity. The GDPR covers this principle in Article 25.

Suppose, for example, you're launching a new app for your company. You have to think about what personal data the app could possibly collect from users, then consider ways to minimize the amount of data and how you will secure it with the latest technology.

Source: gdpr.eu/what-is-gdpr/

Consent

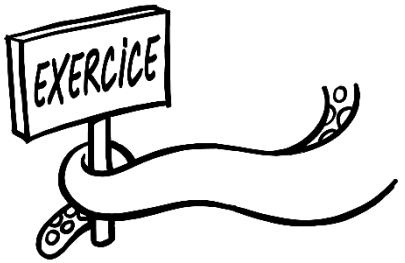
There are strict new rules about what constitutes consent from a data subject to process their information.

- Consent must be “freely given, specific, informed and unambiguous.”
- Requests for consent must be “clearly distinguishable from the other matters” and presented in “clear and plain language.”
- Data subjects can withdraw previously given consent whenever they want, and you have to honor their decision. You can’t simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parent.
- You need to keep documentary evidence of consent.

Source: gdpr.eu/what-is-gdpr/

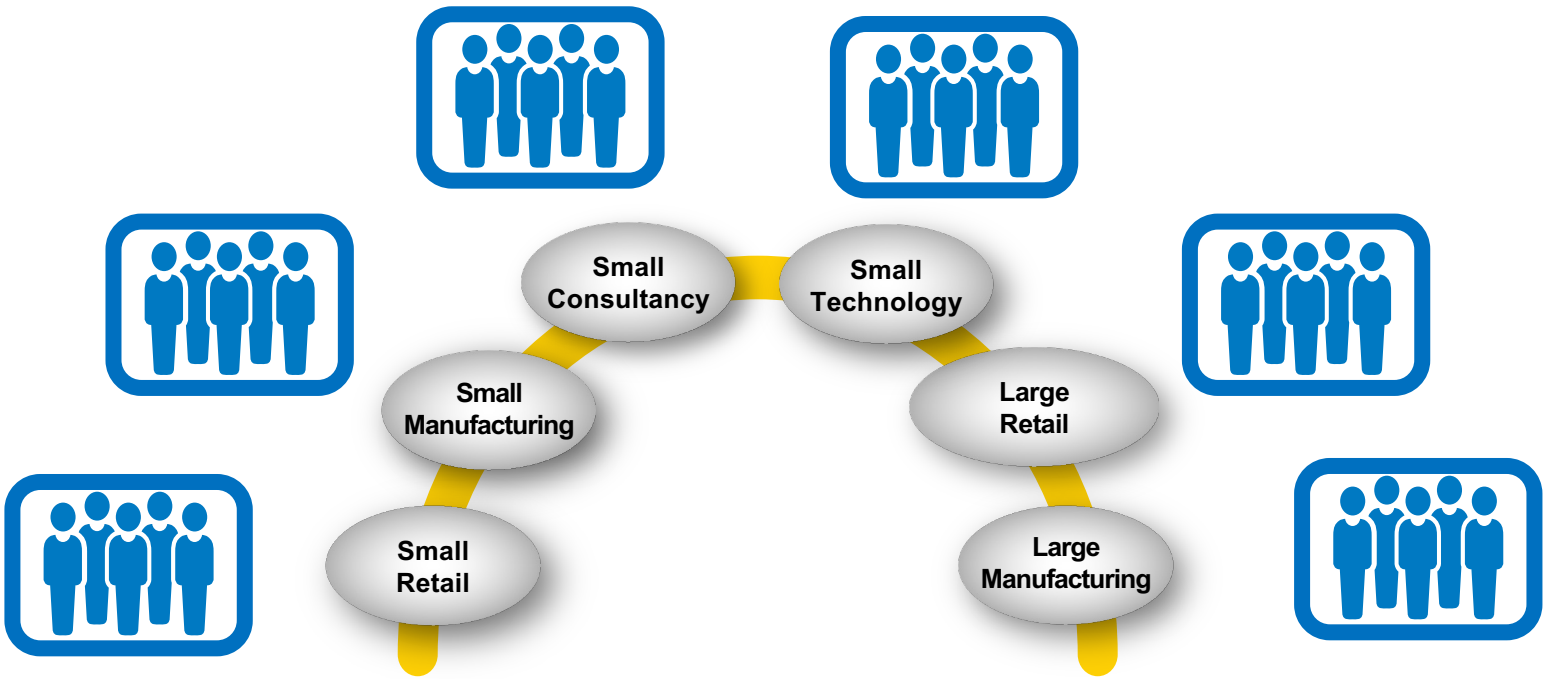
What Does GDPR Mean

For the following organizations ?



Type of data? What needs to be done?

- Small Retail Business
- Small Manufacturing Business
- Small Consultancy Business
- Small Technology Business
- Large Retail Business
- Large Manufacturing Business



California Consumer Privacy Act

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale or sharing of their personal information including via the GPC;
- The right to non-discrimination for exercising their CCPA rights.

Businesses that are subject to the CCPA have several responsibilities, including responding to consumer requests to exercise these rights and giving consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers.

Source: oag.ca.gov/privacy/ccpa

California Privacy Rights Act

In 2020, California voters approved Proposition 24, the California Privacy Rights Act. The CPRA amended the CCPA by adding additional consumer privacy rights and obligations for businesses. It also established this Agency and tasked it with responsibilities including implementing and enforcing the law and educating the public on their rights and obligations under the law. The CPRA amended the CCPA; it did not create a separate, new law. As a result, the Agency typically refers to the law as "CCPA" or "CCPA, as amended." The CPRA amendments to the CCPA went into effect on January 1, 2023.

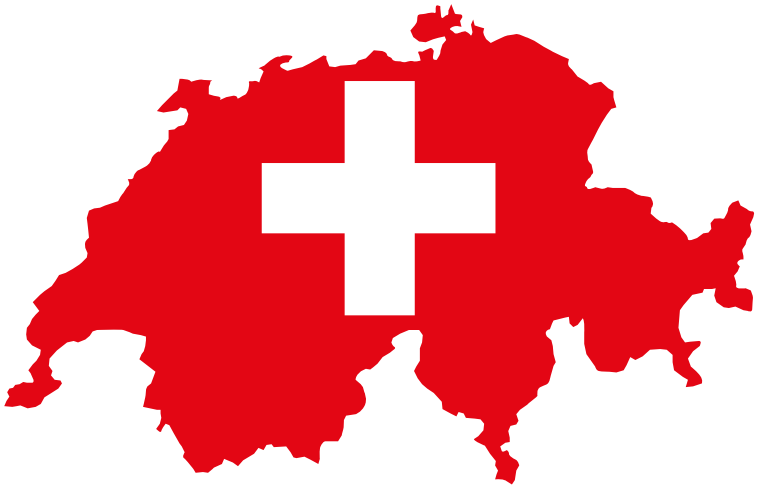
As of January 1, 2023, California residents have the following rights:
L - Right to LIMIT the use and disclosure of sensitive personal information collected about them.
O - Right to OPT-OUT of the sale of their personal information and the right to opt-out of the sharing of their personal information for cross-context behavioral advertising.
C - Right to CORRECT inaccurate personal information that businesses have about them.
K - Right to KNOW what personal information businesses have collected about them and how they use and share it.
E - Right to EQUAL treatment. Businesses cannot discriminate against consumers for exercising their CCPA rights.
D - Right to DELETE personal information businesses have collected from them (subject to some exceptions).

Source: cppa.ca.gov/faq.html

CCPA versus CPRA versus GDPR

Feature	CPA (2020)	CPRA (2023)	GDPR (2018)
Sensitive Info Regulation	❌ Not specifically defined	✅ Yes - Special category with right to **limit use/disclosure**	✅ Yes - **Special category data** with strict protection rules
Right to Correct Data	❌ No	✅ Yes	✅ Yes
Data Sharing Opt-Out	❌ Only applies to **selling**	✅ Applies to **selling + sharing** (e.g., targeted advertising)	✅ Individuals can object to sharing without consent
Data Retention Limits	❌ Not specified	✅ Yes - Data must be **kept only as long as necessary**	✅ Yes - Data **must not be kept longer than needed**
Enforcement Body	🏛️ CA Attorney General only	🏛️ **California Privacy Protection Agency (CPPA)** + Attorney General	🏛️ Independent **Data Protection Authorities (DPAs)** in each EU country
Maximum Fine	💰 $2,500 per violation (or $7,500 if intentional)	💰 Same, but with **dedicated enforcement agency**	💰 Up to **€20 million or 4% of global annual turnover**

Swiss Federal Act on Data Protection (FADP / nFADP)



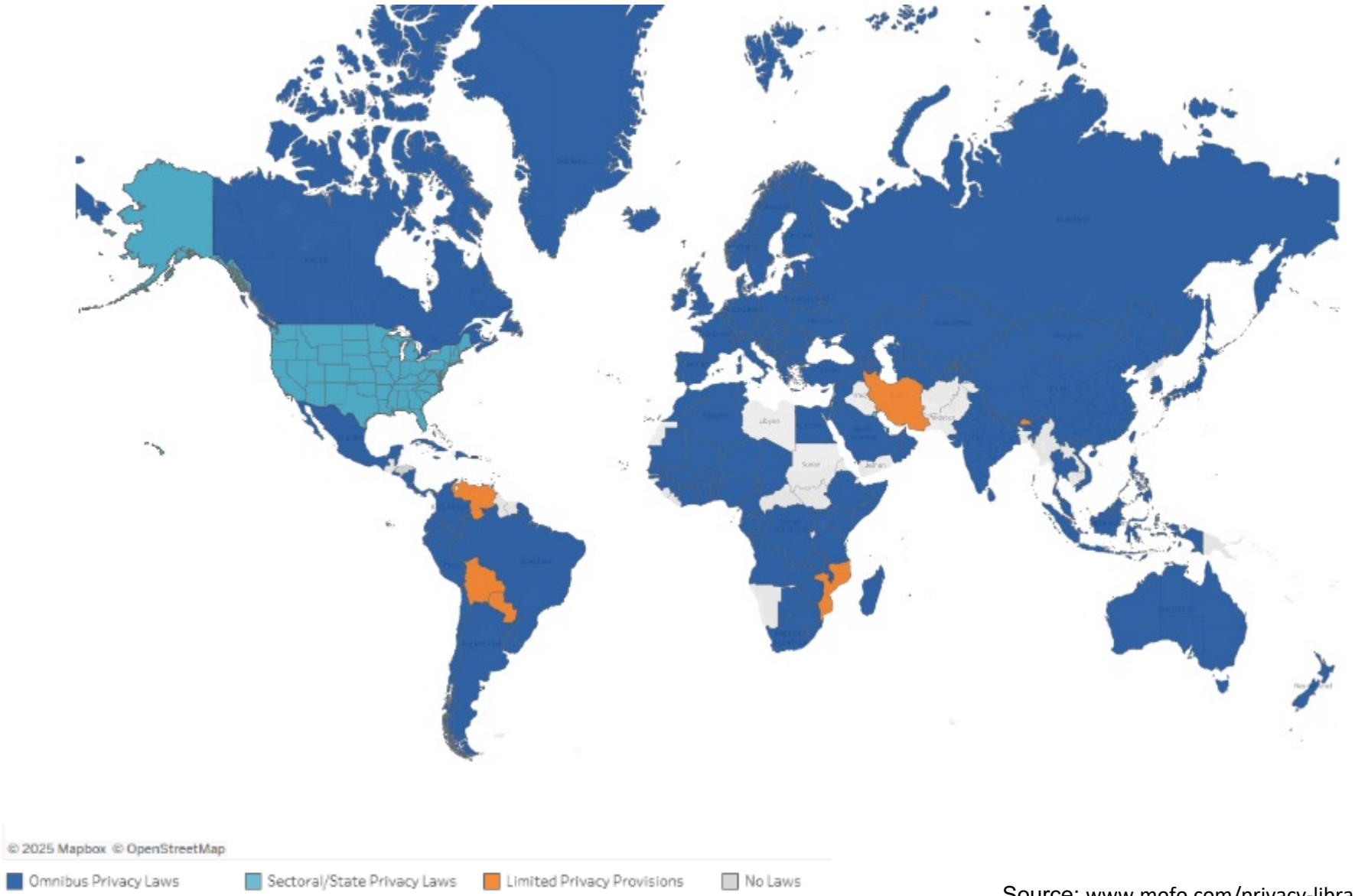
- Swiss companies must comply to the new Swiss Data Protection Act since September 1st, 2023
- This revised Data Protection law:
  - regulates the **processing of personal data**
  - grant Swiss citizens **new rights**
  - brings **new obligations** for companies based in Switzerland

Following aspects are new for Swiss companies:

- The principles of "**Privacy by Design**" and "**Privacy by Default**" are introduced
- Keeping a register of **processing activities** is mandatory
- Data Security breaches must be promptly notified to the Federal Data Protection and Information Commissioner
- Companies must carry out a **Data Protection Impact Assessment** if the data processing is likely to result in a high risk to the fundamental rights of the data subjects.

Source: www.fedlex.admin.ch/eli/cc/2022/491/en

Regulations Worldwide



Source: www.mofo.com/privacy-library

Regulations for Selected Countries





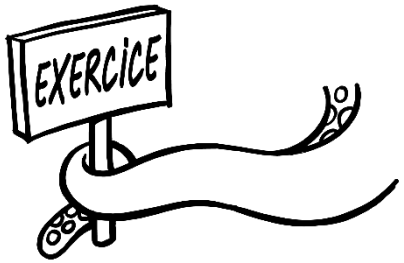


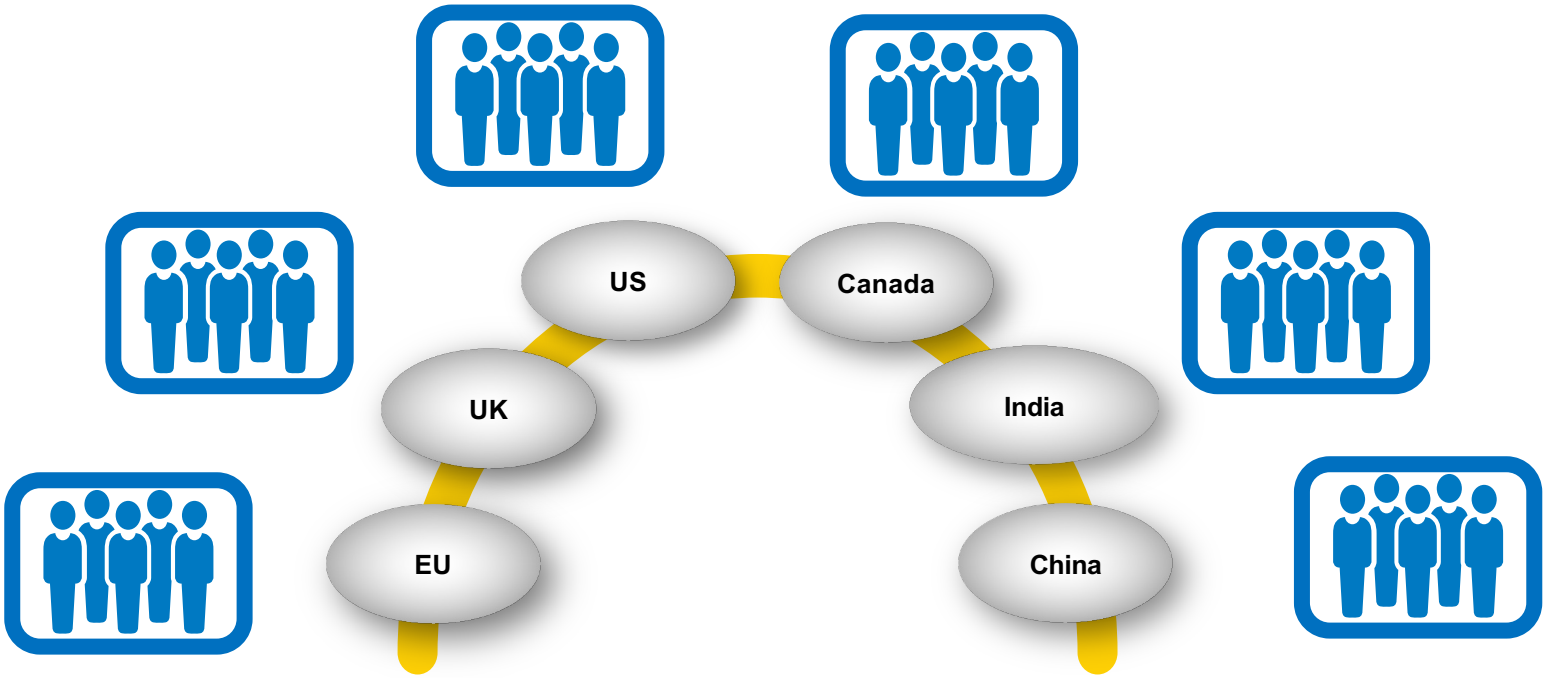
General Data Protection Regulation (GDPR)	25 May 2018	https://eur-lex.europa.eu/eli/reg/2016/679/oj
Federal Act on Data Protection (nFADP/DSG)	1 September 2023	https://www.fedlex.admin.ch/eli/cc/2022/568/en
UK GDPR + Data Protection Act 2018	25 May 2018 / 1 Jan 2021	https://www.gov.uk/data-protection
California Consumer Privacy Act (CCPA) + state laws	1 January 2020	https://oag.ca.gov/privacy/ccpa
Personal Information Protection and Electronic Documents Act (PIPEDA)	1 January 2001 (amended often)	https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
Digital Personal Data Protection Act, 2023 (DPDPA)	Enacted 11 August 2023 *(expected enforcement in 2024–2025)*	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Personal Information Protection Law (PIPL)	1 November 2021	https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Which differences between the regulations?

Compare the regulations between the following countries

- EU
- US
- India
- UK
- Canada
- China





How to enforce

GDPR Enforcement Mechanisms

European Data Protection Board (EDPB)

European Data Protection Supervisor (EDPS)

Data Protection Authorities (DPA)

https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

Complaint System

https://www.edpb.europa.eu/system/files/2024-05/edpb_20230620_templatecomplaintform_en.pdf

DPO

Data Protection Officer

- ✓ **Advise** on GDPR compliance
- ✓ **Monitor** data protection practices
- ✓ **Liaise** with DPAs and data subjects
- ✓ **Train staff** on privacy policies

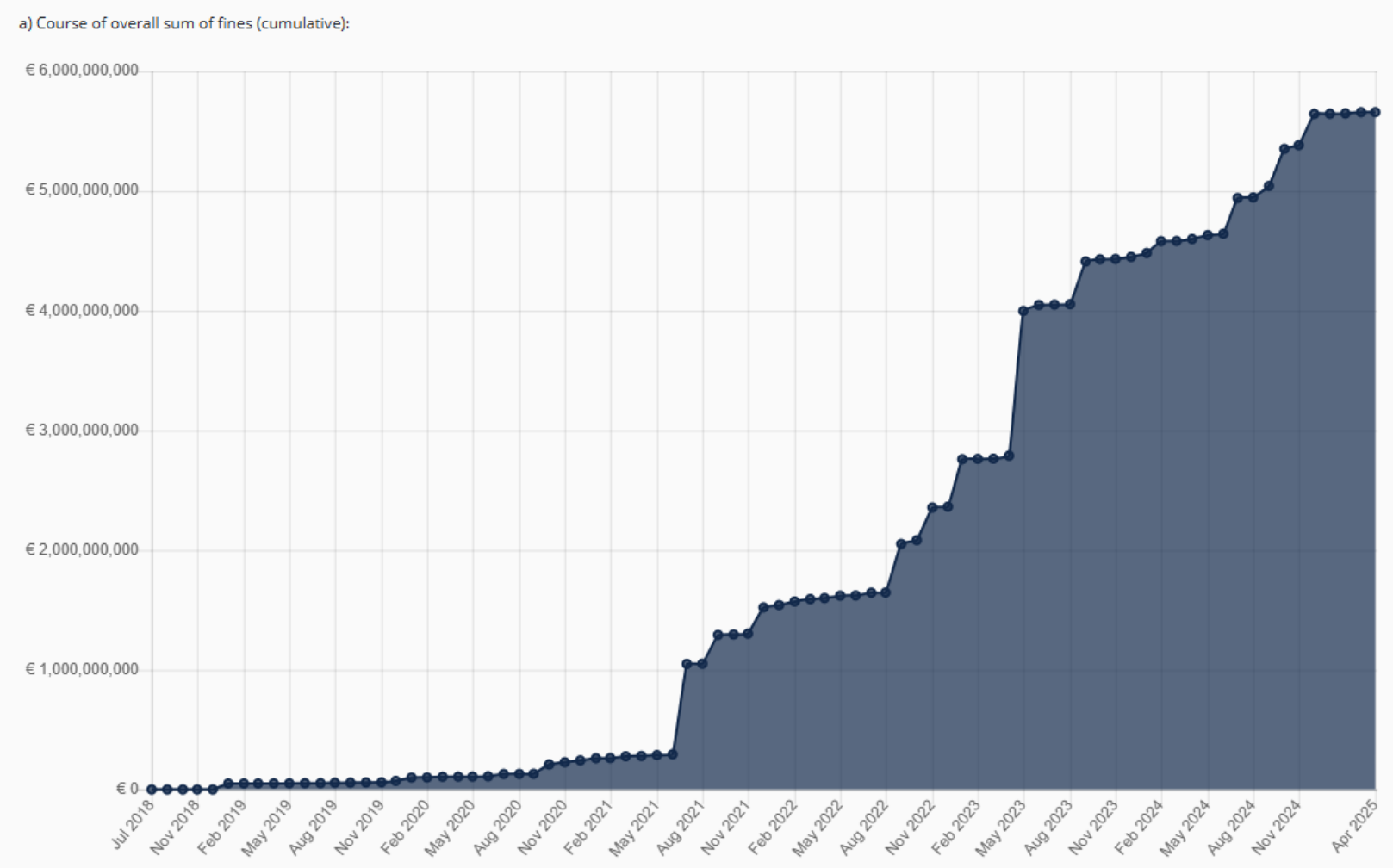
Public authorities, health, biometrics, Google, Facebook etc

DPIA

Data Protection Impact Assessment

to identify and mitigate privacy risks before processing personal data, especially for high-risk activities

Statistics about GDPR Penalties



Source: www.enforcementtracker.com/?insights

Famous Example of Penalties

WIKIPEDIA
The Free Encyclopedia

Search Wikipedia

Create account Log in

Facebook–Cambridge Analytica data scandal

16 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

Contents [hide]

- (Top)
- Overview
- Data characteristics
  - Numbers
  - Information
- Data use
  - Ted Cruz campaign
  - Donald Trump campaign
  - Potential usage
    - Russia
    - Brexit
- Responses
  - Facebook and other companies
  - Governmental actions
  - Impact on Facebook users and investors
  - #DeleteFacebook movement
  - *The Great Hack*

In the 2010s, personal data belonging to millions of Facebook users was collected without their consent by British consulting firm Cambridge Analytica, predominantly to be used for political advertising.[1]

The data was collected through an app called "This Is Your Digital Life", developed by data scientist Aleksandr Kogan and his company Global Science Research in 2013.[2] The app consisted of a series of questions to build psychological profiles on users, and collected the personal data of the users' Facebook friends via Facebook's Open Graph platform.[2] The app harvested the data of up to 87 million Facebook profiles.[2] Cambridge Analytica used the data to provide analytical assistance to the 2016 presidential campaigns of Ted Cruz and Donald Trump.[3][4] Cambridge Analytica was also widely accused of interfering with the Brexit referendum, although the official investigation recognised that the company was not involved "beyond some initial enquiries" and that "no significant breaches" took place.[5][6]

Information about the data misuse was disclosed in 2018 by Christopher Wylie, a former Cambridge Analytica employee, in interviews with *The Guardian* and *The New York Times*.[7] In response, Facebook apologized for their role in the data harvesting and their CEO Mark Zuckerberg testified in front of Congress.[7] In July 2019, it was announced that Facebook was to be fined $5 billion by the Federal Trade Commission due to its privacy violations.[8] In October 2019, Facebook agreed to pay a £500,000 fine to the UK Information Commissioner's Office for exposing the data of its users to a "serious risk of harm".[9] In May 2018, Cambridge Analytica filed for Chapter 7 bankruptcy.[10]

Other advertising agencies have been implementing various forms of psychological targeting for years and Facebook had patented a similar technology in 2012.[11] Nevertheless, Cambridge Analytica's openness about their methods and the caliber of their clients — including the Trump presidential campaign and the UK's Vote Leave campaign — brought the challenges of psychological targeting that scholars have been warning against to public awareness.[11] The scandal sparked an increased public interest in privacy and

Part of a series on
Facebook
History
IPO
Acquisitions
Criticism
Privacy
Features
Like button
Feed
Litigation
Censorship by
Censorship of
Content
CA data scandal
Oversight Board
2020 ad boycotts
2021 files leak
2021 outage
Rebranding
v · t · e

Source: en.wikipedia.org/wiki/Facebook–Cambridge_Analytica_data_scandal

Penalties “on-line”

GDPR Enforcement Tracker

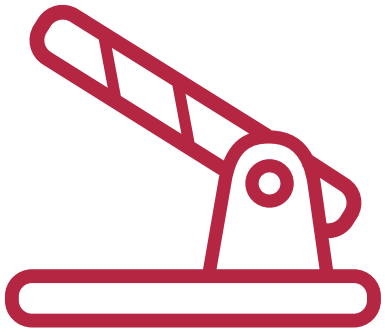
ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type
ETid-1844	IRELAND	2023-05-12	1,200,000,000	Meta Platforms Ireland Limited	Art. 46 (1) GDPR	Insufficient legal basis for data processing
ETid-778	LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à r.l.	Unknown	Non-compliance with general data processing principles
ETid-1373	IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
ETid-1543	IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Non-compliance with general data processing principles
ETid-2032	IRELAND	2025-09-01	345,000,000	TikTok Limited	Art. 5 (1) a), 5 (1) f) GDPR, Art. 12 (1) GDPR, Art. 13 (1) a) GDPR, Art. 24 (1) GDPR, Art. 25 (1), (2) GDPR	Non-compliance with general data processing principles
ETid-2069	IRELAND	2024-10-24	310,000,000	LinkedIn	Art. 5 (1) a) GDPR, Art. 6 (1) a), c), f) GDPR, Art. 13 (1) c) GDPR, Art. 14 (1) c) GDPR	Insufficient legal basis for data processing
ETid-2447	THE NETHERLANDS	2024-07-22	290,000,000	Uber Technologies Inc., Uber B.V.	Art. 44 GDPR	Non-compliance with general data processing principles
ETid-1502	IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security
ETid-2484	IRELAND	2026-12-17	251,000,000	Meta Platforms Ireland Limited	Art. 33 (1), (5) GDPR, Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security
ETid-820	IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.	Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations

Source: www.enforcementtracker.com/

Cross-Border Data Regulations

Cross-Border Data Regulations are laws and policies that govern the transfer, storage, and processing of data across national borders. These regulations aim to protect personal privacy, national security, and economic interests while facilitating international data flows in a globalized digital economy.

They are a critical part of modern data governance, especially given the rise of cloud computing, global digital services, and international data flows.



Examples of Cross-Border Data Regulations

GDPR (European Union)

- Strict rules on transferring personal data outside the EU/EEA
- Requires "adequate" protection in the destination country or use of safeguards (e.g., Standard Contractual Clauses)

China's Personal Information Protection Law (PIPL)

- Requires security assessments before exporting personal data
- Encourages data localization, especially for critical information

India's Digital Personal Data Protection Act (2023)

- Imposes restrictions on cross-border data transfers, with certain whitelisted countries allowed

U.S. CLOUD Act

- Allows U.S. authorities to access data stored by U.S. tech companies, even if the data is hosted overseas

Data Residency

Data residency refers to the physical or geographic location where an organization's data is stored and processed. It determines where data lives - often given by legal, regulatory, or policy requirements.

Sector	Country	Law	Key Requirement
Finance	U.S.	GLBA	No strict residency, but strong security required
Finance	India	RBI 2018 Rule	Payment data must be stored only in India
Finance	Russia	Federal Law 242-FZ	Financial personal data must reside in Russia
Healthcare	EU	GDPR	Health data transfers restricted outside EU
Healthcare	Australia	My Health Records Act	Health data must stay in Australia
Healthcare	China	PIPL	Critical health data must be stored in China

Relevance of Data Residency

Legal and Regulatory Compliance

Violating residency laws can lead to fines and legal penalties, Suspension of operations or Reputational damage

Privacy and Data Protection

- Residency ensures that data is subject to the privacy laws of a specific country
- Users prefer knowing their data is stored in trusted jurisdictions
- Avoids data mishandling

Data Security and Sovereignty

- Prevents **Foreign Surveillance**: Countries like Russia and China enforce residency to limit foreign government access (e.g., avoiding U.S. CLOUD Act demands).
- Reduces **Cyber Risks**: Local storage can minimize exposure to international cyber threats.
- Ensures Legal Control: Data stored locally falls under national laws, making enforcement easier
- Avoids Geopolitical & Trade Risks

Performance and User Experience

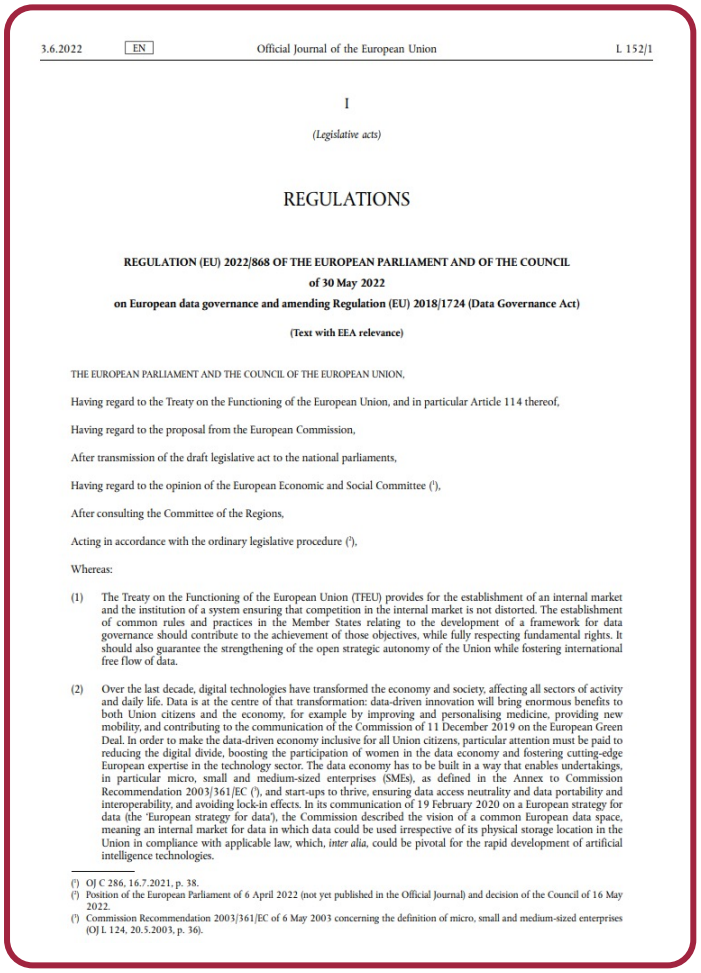
- Storing data close to end users improves Application performance (reduced latency) and Service reliability
- **Disaster Recovery**: Ensures redundancy in case of geopolitical disruptions

Business Trust and Market Access

Organizations that meet residency requirements are more likely to win contracts with government or highly regulated sectors and to expand into markets with data localization laws

The EU Regulation "Data Governance Act" (DGA)

Legal Framework for Data Sharing within the European Union



3.6.2022 EN Official Journal of the European Union L 152/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 30 May 2022
on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) The Treaty on the Functioning of the European Union (TFEU) provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted. The establishment of common rules and practices in the Member States relating to the development of a framework for data governance should contribute to the achievement of those objectives, while fully respecting fundamental rights. It should also guarantee the strengthening of the open strategic autonomy of the Union while fostering international free flow of data.

(2) Over the last decade, digital technologies have transformed the economy and society, affecting all sectors of activity and daily life. Data is at the centre of that transformation: data-driven innovation will bring enormous benefits to both Union citizens and the economy, for example by improving and personalising medicine, providing new mobility, and contributing to the communication of the Commission of 11 December 2019 on the European Green Deal. In order to make the data-driven economy inclusive for all Union citizens, particular attention must be paid to reducing the digital divide, boosting the participation of women in the data economy and fostering cutting-edge European expertise in the technology sector. The data economy has to be built in a way that enables undertakings, in particular micro, small and medium-sized enterprises (SMEs), as defined in the Annex to Commission Recommendation 2003/361/EC (3), and start-ups to thrive, ensuring data access neutrality and data portability and interoperability, and avoiding lock-in effects. In its communication of 19 February 2020 on a European strategy for data (the 'European strategy for data'), the Commission described the vision of a common European data space, meaning an internal market for data in which data could be used irrespective of its physical storage location in the Union in compliance with applicable law, which, *inter alia*, could be pivotal for the rapid development of artificial intelligence technologies.

(1) OJ C 286, 16.7.2021, p. 38.
(2) Position of the European Parliament of 6 April 2022 (not yet published in the Official Journal) and decision of the Council of 16 May 2022.
(3) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

- The goal of the «**Data Governance Act**» (applicable from **Sep. 24th, 2023**) is to create a legal framework to **facilitate data-sharing across the European Union**
- **The DGA is part of** EU Commission's "European Data Strategy"
- The scope of the DGA is **broader than GDPR** as Data in scope is **personal** as well as **non-personal data**: "'**Data** means **any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording**" (Chapter I, Article 2)

Source: https://eur-lex.europa.eu/eli/reg/2022/868/oj

DGA in a Nutshell

Re-use of Public Sector Data	Allows re-use of protected data with strict safeguards
Data Intermediation	Creates a trusted framework for neutral data-sharing services
Data Altruism	Enables voluntary data donations for public-interest uses
Cross-Border Transfers	Adds controls on international transfers of non-personal data
Compliance & Supervision	Member states enforce rules via designated authorities

The EU Regulation “Data Act” (DA)

The DA aims to regulate access to and use of non-personal data generated by connected devices, machines, and services — often called industrial or IoT data. It ensures that data generated in the EU is more accessible, shareable, and fair, while protecting trade secrets and business interests.

Official Journal of the European Union — EN — L series

2023/2854 — 22.12.2023

REGULATION (EU) 2023/2854 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 13 December 2023
on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

Having regard to the opinion of the Committee of the Regions (3),

Acting in accordance with the ordinary legislative procedure (4),

Whereas:

(1) In recent years, data-driven technologies have had transformative effects on all sectors of the economy. The proliferation of products connected to the internet in particular has increased the volume and potential value of data for consumers, businesses and society. High-quality and interoperable data from different domains increase competitiveness and innovation and ensure sustainable economic growth. The same data may be used and reused for a variety of purposes and to an unlimited degree, without any loss of quality or quantity.

(2) Barriers to data sharing prevent an optimal allocation of data for the benefit of society. Those barriers include a lack of incentives for data holders to enter voluntarily into data sharing agreements, uncertainty about rights and obligations in relation to data, the costs of contracting and implementing technical interfaces, the high level of fragmentation of information in data silos, poor metadata management, the absence of standards for semantic and technical interoperability, bottlenecks impeding data access, a lack of common data sharing practices and the abuse of contractual imbalances with regard to data access and use.

(3) In sectors characterised by the presence of microenterprises, small enterprises and medium-sized enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC (5) (SMEs), there is often a lack of digital capacities and skills to collect, analyse and use data, and access is frequently restricted where one actor holds them in the system or due to a lack of interoperability between data, between data services or across borders.

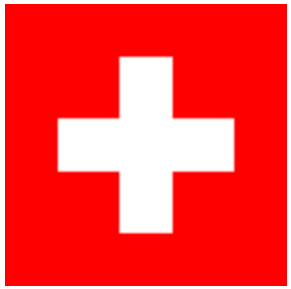
(4) In order to respond to the needs of the digital economy and to remove barriers to a well-functioning internal market for data, it is necessary to lay down a harmonised framework specifying who is entitled to use product data or related service data, under which conditions and on what basis. Accordingly, Member States should not adopt or maintain

(1) OJ C 402, 19.10.2022, p. 5.
(2) OJ C 365, 23.9.2022, p. 18.
(3) OJ C 375, 30.9.2022, p. 112.
(4) Position of the European Parliament of 9 November 2023 (not yet published in the Official Journal) and decision of the Council of 27 November 2023.
(5) Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

- The goal of the proposed regulation «Data Act» is to create a legal framework to harmonise rules on fair access to and use of data
- The Data Act is part of EU Commission's "European Data Strategy" and is complementary to the Data Governance Act. It aims to ensure a better distribution of the value derived from the use of data
- The Data Act defines “data” exactly as in the the DGA, including personal as well as non-personal data
- The Data Act will apply to device manufacturers, providers of digital services and connected products (such as IoT) as well as public authorities in the EU

Recognition of States for Data Protection

Free transfer of personal data to another country — without additional safeguards — if that country is officially recognized as offering “adequate” data protection



Germany, Andorra, Argentina, Austria, Belgium, Bulgaria, Canada, Cyprus, Croatia, Denmark, Spain, Estonia, Finland, France, Gibraltar, Greece, Guernsey, Hungary, Isle of Man, Faroe Islands, Ireland, Iceland, Israel, Italy, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Norway, New Zealand, Netherlands, Poland, Portugal, Czech Republic, Romania, United Kingdom, Slovakia, Slovenia, Sweden, Uruguay, United States

Source: www.fedlex.admin.ch/eli/cc/2022/568/en#annex_1

Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay

Source: commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

EU-US Data Privacy Framework (DPF)

The DPF, adopted in July 2023, replaces the defunct Privacy Shield and governs transatlantic data transfers while addressing EU concerns over U.S. surveillance laws

- U.S. companies self-certify under the DPF, pledging to comply with GDPR-like privacy principles
- The U.S. provides safeguards against indiscriminate surveillance (e.g., limiting NSAaccess to EU data)
- EU citizens gain legal redress via a new Data Protection Review Court (DPRC)

Key Requirements for U.S. Companies

✓ Data Minimization: Only collect necessary personal data
✓ Purpose Limitation: Use data only for specified reasons
✓ Security & Accountability: Protect data from breaches
✓ Third-Party Transfers: Ensure subcontractors also comply

➔ **Schrems I (2015) :** U.S. surveillance practices (exposed by Edward Snowden) violated EU citizens' privacy rights under EU Charter of Fundamental Rights
-> **Schrems II (2020):** insufficient safeguards against U.S. government surveillance and no effective legal remedies for EU citizens

Cross-border Transfer of Personal Data for CH

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

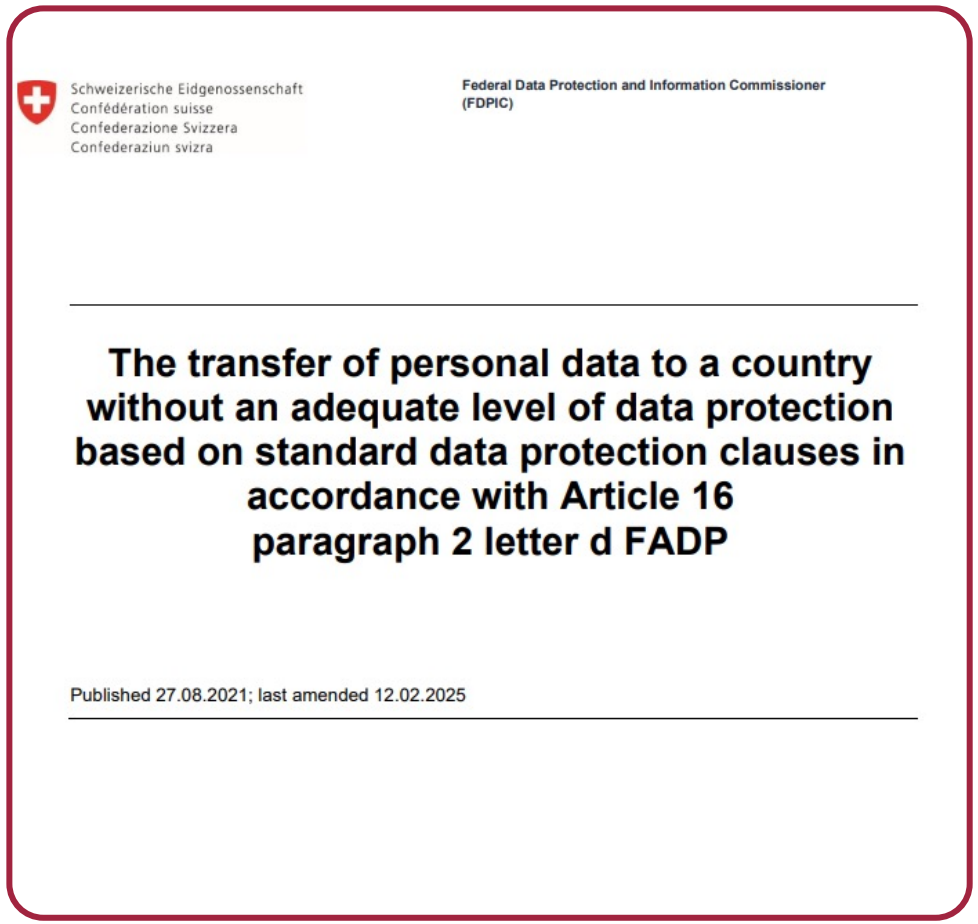
Federal Data Protection and Information Commissioner (FDPIC)

The cross-border transfer of personal data by private companies or federal bodies is only possible **under certain conditions**. It **depends on the country** to which the data is to be transferred, and certain **precautions** must be taken depending on the country.

In principle, personal data may only be transmitted abroad **if** the destination country has an **appropriate level of data protection**.
If an appropriate level of protection **is guaranteed**, personal data can be **freely** transmitted from Switzerland to a country on the list, both by private companies and by federal bodies.

Source: www.edoeb.admin.ch/en/cross-border-transfer-of-personal-data

Transfer of Personal Data to a Country without an Adequate Level of Data Protection



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner (FDPIC)

The transfer of personal data to a country without an adequate level of data protection based on standard data protection clauses in accordance with Article 16 paragraph 2 letter d FADP

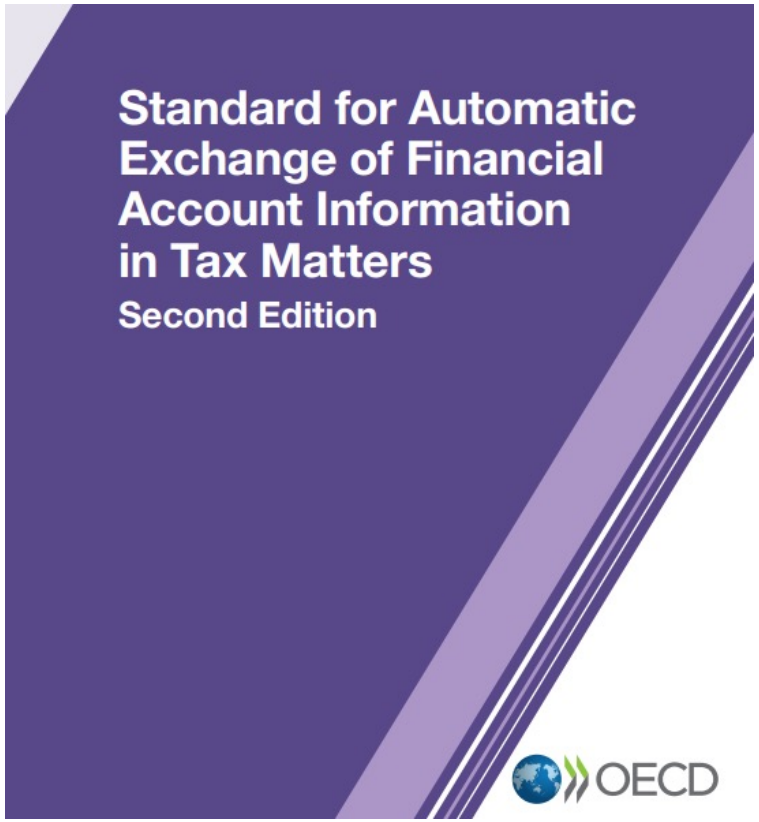
Published 27.08.2021; last amended 12.02.2025

- Use of **Standard Contractual Clauses** (SCCs) to legally bind the recipient to uphold Swiss data protection standards
- Conduct a **Transfer Impact Assessment** (TIA)
- Implement **technical safeguards** (like encryption or pseudonymization)
- Ensure the recipient cannot be **compelled by local law** (e.g., U.S. surveillance laws) to provide access to the data
- **document the legal basis and risk assessment** of the transfer
- The FDPIC may request to see how **compliance is ensured**

Source: backend.edoeb.admin.ch/fileservice/sdweb-docs-prod-edoebch-files/files/2025/02/12/fc143071-a80a-4f61-b479-0ac3249961d6.pdf

Common Reporting Standard (CRS)

The Common Reporting Standard (CRS) is an internationally agreed standard for the automatic exchange of financial account information between jurisdictions for tax purposes, to better combat tax evasion and ensure tax compliance.



Source: www.oecd.org/en/publications/standard-for-automatic-exchange-of-financial-account-information-in-tax-matters-second-dition_9789264267992-en.html

Conflict of Laws

EU GDPR vs. U.S. CLOUD Act

Conflict

- GDPR (EU) prohibits transferring personal data outside the EU unless the recipient country ensures "adequate protection"
- CLOUD Act (U.S.) allows American authorities to access data stored by U.S. companies (e.g., Microsoft, Google) even if the data is physically located in the EU

Example

A German company stores customer data in Microsoft Azure's EU data centers. The U.S. government demands access to this data for a criminal investigation under the CLOUD Act, but GDPR forbids such transfers without safeguards.

Possible Resolution

- Use EU-based cloud providers to avoid U.S. jurisdiction
- Encrypt data so only the EU entity holds decryption keys
- Rely on the EU-U.S. Data Privacy Framework (DPF), though legal challenges persist

Data Localization in China vs. Global Business Operations

Conflict

China's **Personal Information Protection Law (PIPL)** and **Cybersecurity Law** require that certain data — especially personal or "important" data — be stored **inside China** and be subject to **security assessments before export**.

Example

A Swiss multinational runs customer support for its global users out of its European HQ. It collects customer feedback from Chinese users, but Chinese law prevents exporting that data without approval.

Possible Resolution

- Store and process Chinese data within China using a local subsidiary or partner
- Separate infrastructure for China (data siloing)
- Undergo China's security assessment process for cross-border data transfer approval

Swiss Data Protection (FADP) vs. Brazilian LGPD

Conflict

Both Switzerland's **revised FADP** and Brazil's **LGPD** impose strong data protection requirements, but their **rules on data subject rights, consent**, and **data export** may differ — making compliance tricky for services operating in both jurisdictions.

Example

A Swiss tech startup launches a mobile app in Brazil. It collects location and behavioural data for analytics. Brazil's LGPD requires **clear, granular consent**, and Swiss law requires **transparency and proportionality** - but the wording and mechanisms differ.

Possible Resolution

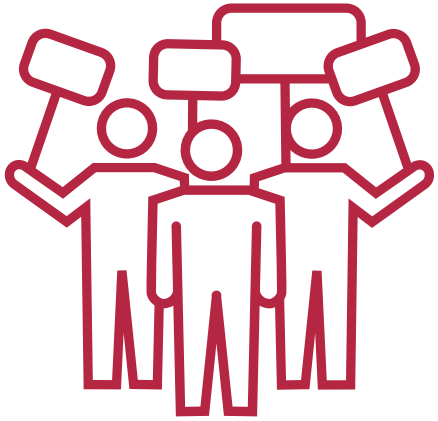
- Apply the stricter common denominator across all jurisdictions
- Use modular consent mechanisms that meet both laws
- Maintain country-specific data protection policies and appoint local representatives

Interoperability and Tech Disruption

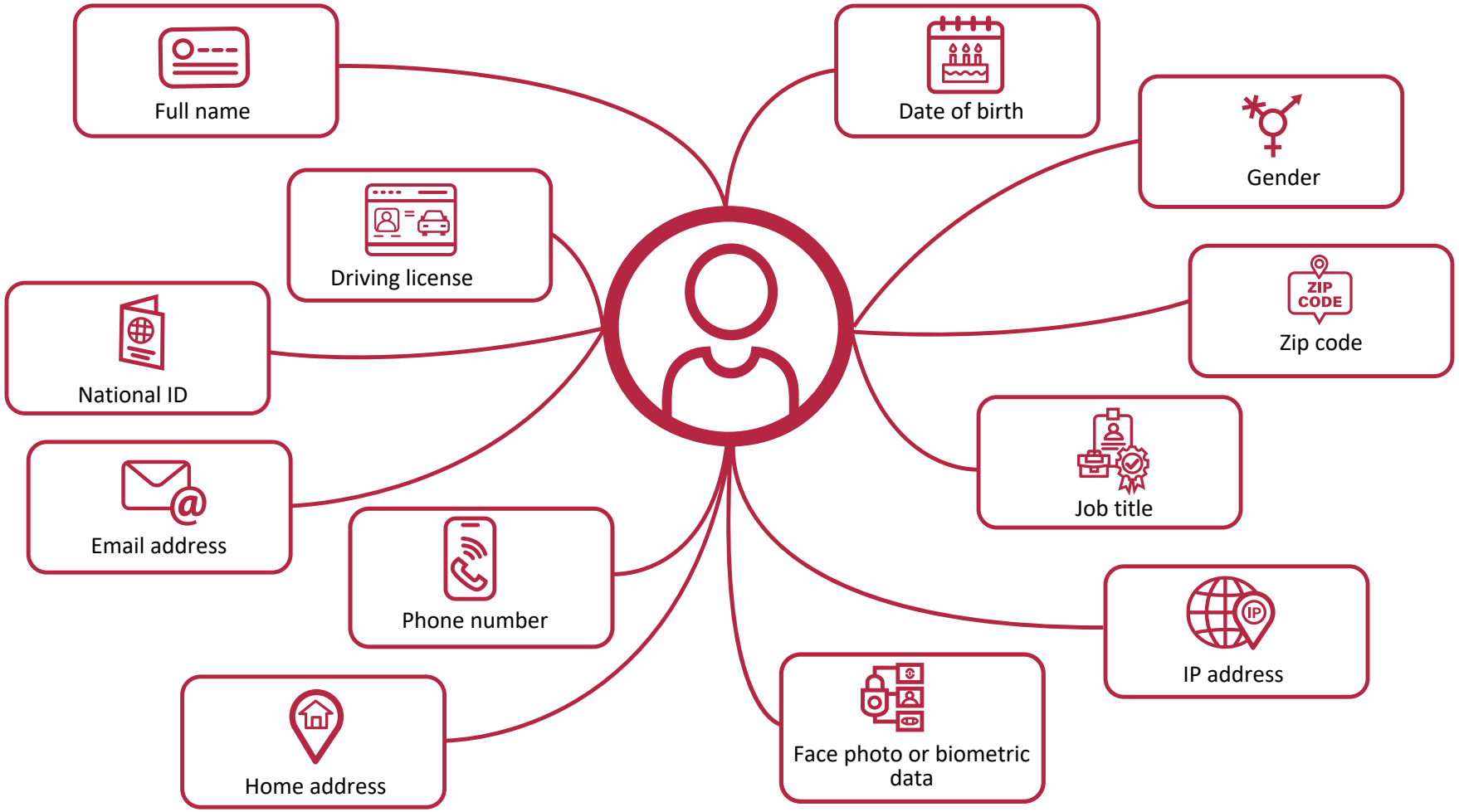
Actor	Role
EU	Sets de facto global standards via GDPR/DA
U.S.	Pushes for open flows but faces EU/China resistance
China	Prioritizes control via PIPL/Great Firewall
Multi-nationals	Lobby for harmonization (e.g., Microsoft's "Data Sovereignty" cloud solutions)
Civil Society	Advocates for rights (e.g., NOYB's Schrems II challenges)
Tech Companies	Encryption and anonymization to reduce legal risks

Trend	Likely Future Role
Data Localization	Persistent, especially in authoritarian or strategic sectors
Privacy Law Convergence	Slow but growing, driven by global pressure and trade deals
Cosmopolitan Pluralism	Most realistic "middle ground" toward interoperability
Global Standards & Forums	OECD, CBPR, and G7 shaping norms; WTO could play a role
Conflict Resolution	Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs)

Sensitive Data



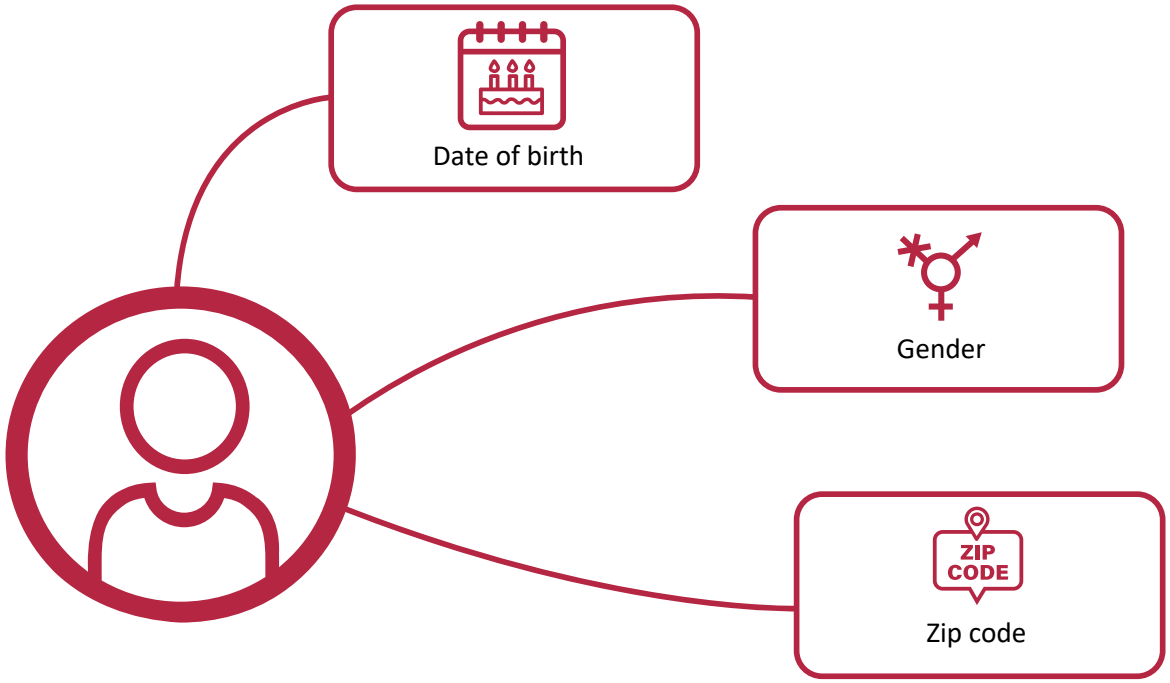
Personally Identifiable Information (PII)



Linkable Information

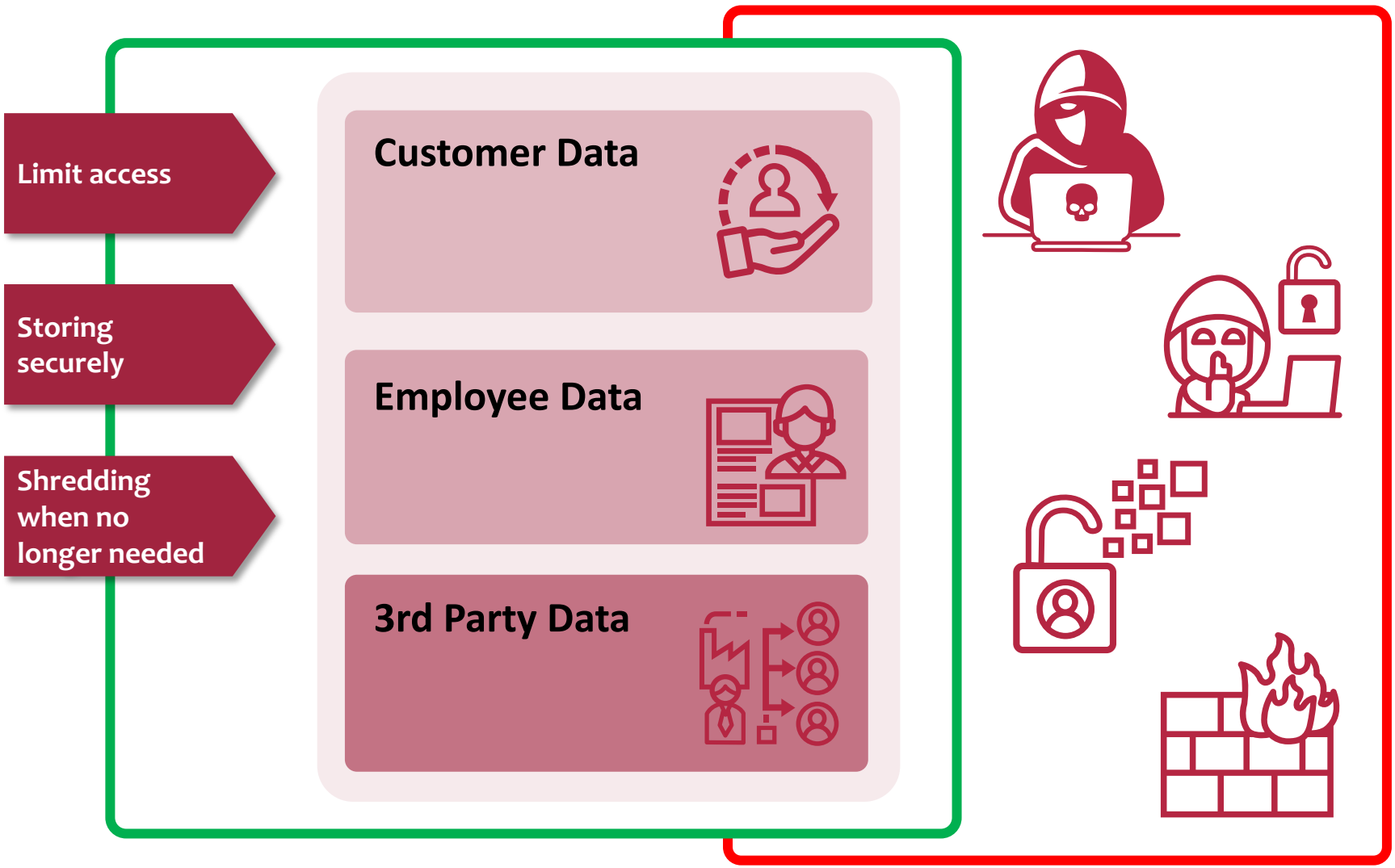
Linkable information refers to data that, while not directly identifying on its own, can be combined with other datasets to reveal a person's identity.

If information is linkable, the risk of identification is more than negligible.



Source: Latanya Sweeney, Simple Demographics Often Identify People Uniquely (2000)

PII Principles



Customer Identification Data

Any information that can be used to directly or indirectly identify a specific client

- Full name
- Social Security Number (SSN) or National ID
- Passport number
- Driver’s license number
- Bank account or credit card details
- Email address (if personally identifiable)
- Phone number

- Date of birth
- Physical address
- IP address
- Device ID (e.g., IMEI, MAC address)
- Biometric data (fingerprints, facial recognition)
- Customer ID numbers

Employee Data

Employers must protect and respect the personality rights of their employees

Recruitment process

- Questions about candidates' financial circumstances, possible debts, medical conditions are only allowed if there are special reasons for doing so in view of the position to be filled
- Information from third parties - from current or former employers, for example – they must obtain the consent of the applicant beforehand
- Documents submitted by unsuccessful candidates must be returned to them and copies

Employment relationship

- Employee file should only contain data that are essential for the performance of the employment contract
- Remove unnecessary documents
- Data processed solely by the personnel department and be accessible only to those departments entitled to use them
- disclose any personal data to third parties only with the consent of the person concerned unless required to do so by law

Employment termination

- Only essential data can be kept (e.g. accounting, social insurance or tax data)
- Data for an ongoing dispute
- Retention period between 5 and 10 years
- Data must be destroyed as soon as their retention is no longer required

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner (FDPIC)

Source: www.edoeb.admin.ch/en/different-phases-of-the-employment-relationship

3rd Party Data

Examples

- Names and contact information of customers from a partner database
- Employee records shared by a staffing agency
- Biometric data collected by a subcontractor
- Email addresses collected via co-marketing campaigns
- Identification documents for background checks from external HR vendors

Best Practices

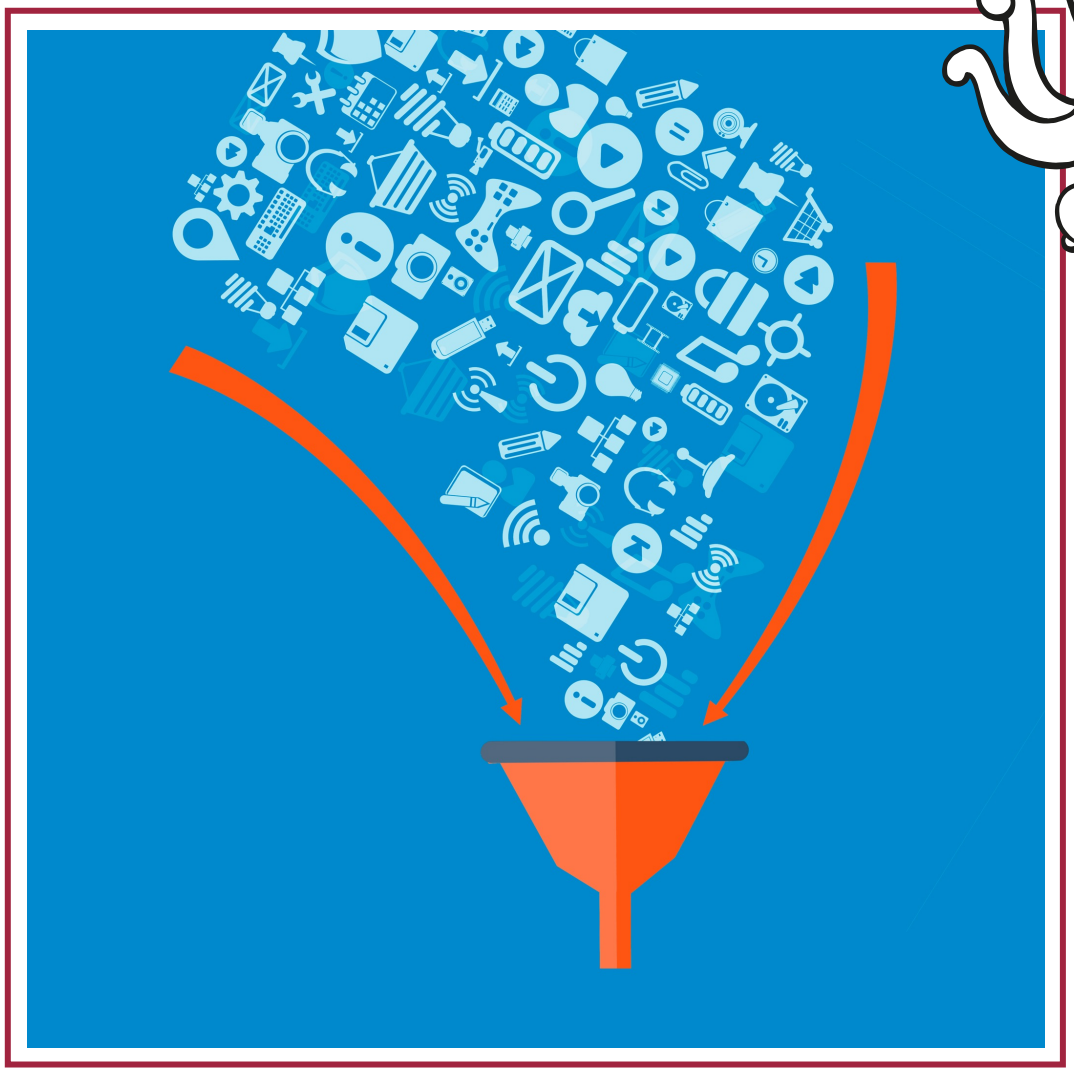
- Minimize Data Sharing: Only share necessary PII with trusted vendors.
- Use Data Processing Agreements (DPAs): Legally bind third parties to protect PII
- Anonymize/Pseudonymize – Where possible, remove direct identifiers before sharing
- Monitor Compliance – Regularly audit third-party vendors for security & privacy practices
- Provide User Control – Allow users to opt out of third-party data sharing (e.g., via cookie consent banners)

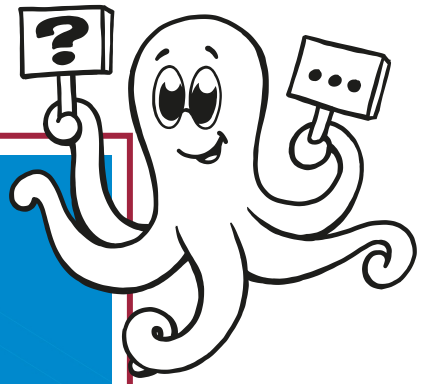
Protected Health Information (PHI)

Sensitive Data when linked to a patient:

- Medical record numbers
- Diagnosis or treatment info
- Lab test results
- Prescription history
- Health insurance policy numbers
- Appointment dates
- Notes from doctors or therapists
- Biometrics (e.g., fingerprints, retinal scans used in a healthcare context)

Which Other Data need to be protected?





Payment Card Information (PCI)

Children Data Protection

- **Parental consent** before data collection (depending on age/region)
- **Age verification mechanisms** (e.g., self-declaration or third-party verification)
- **Privacy notices** must be **age-appropriate** and easy to understand
- **Limit data collection** to what is strictly necessary
- **Avoid profiling**, behavioral advertising, or location tracking
- **Default to high privacy** settings for child users
- **Do not retain** children's data longer than needed

GDPR

Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is **at least 16 years old**. [2]Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the **holder of parental responsibility over the child**. [3]Member States may provide by law for a lower age for those purposes provided that such lower age **is not below 13 years**.

Data Protection Measures

Privacy by Design

Proactively integrate privacy into IT systems

Area	Examples
System Development	Encrypting user data by default in a messaging app
Web Forms	Collecting only required fields (e.g., name + email, not date of birth)
Data Retention	Auto-delete logs after 30 days if not needed
User Control	Users can delete their own account and data at any time
DPIAs	Conducting a Data Protection Impact Assessment before launching a new product
Default Settings	Social network profiles default to private instead of public
Incident Response	Automated alerts for suspicious logins.
User Interface (UI)	Clear cookie banners with reject-all option
Role-based access	Employees only see data needed for their role (e.g., HR accesses payroll, not customer emails)

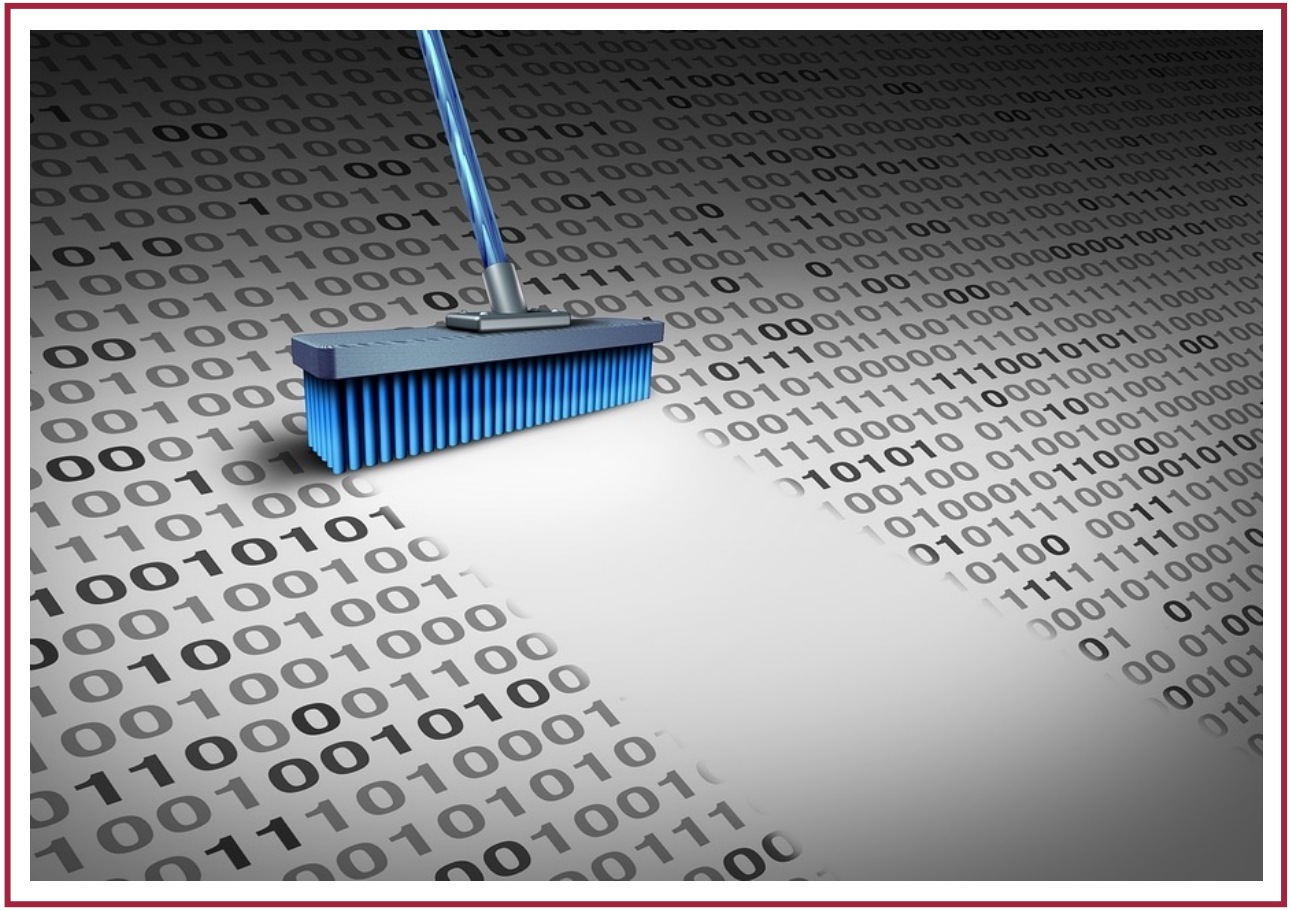
Privacy by Default

Privacy settings and practices are configured to the highest level of data protection automatically, without requiring any user action

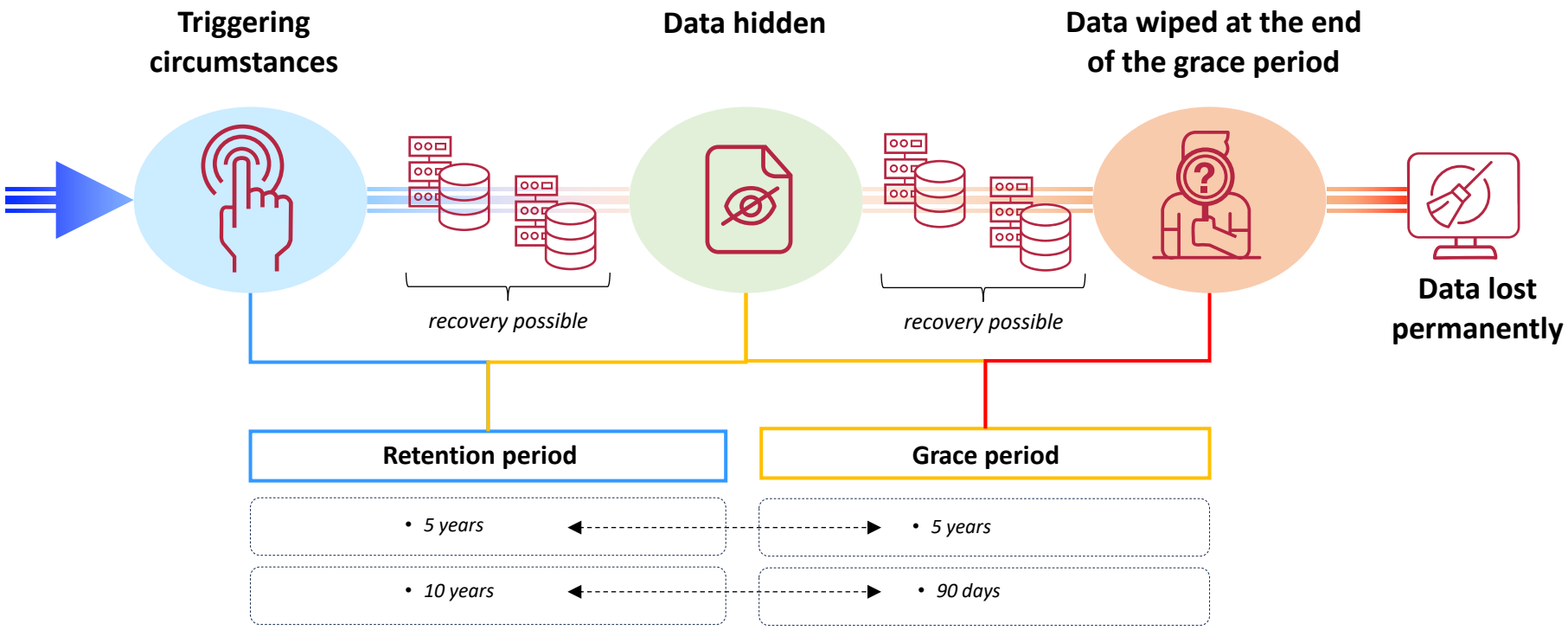
Area	Examples
User Profiles	Voice assistants (e.g., Alexa) don’t save recordings unless enabled
Third-Party Data Sharing	Ad trackers blocked by default (e.g., Brave browser)
Data Collection	Location tracking disabled by default (e.g., iOS "Ask App Not to Track")
App Development	Mobile apps request zero permissions on install (users enable later)
Access Control	New employees get minimum access by default (need-to-know basis)
Social Media Platform	New user profiles are private by default
Photo-Sharing App	Location metadata is stripped from images by default
Analytics Settings	Only anonymized data is collected unless user consents
Mobile App	Does not access contacts, camera, or location unless user enables it

Data Wiping

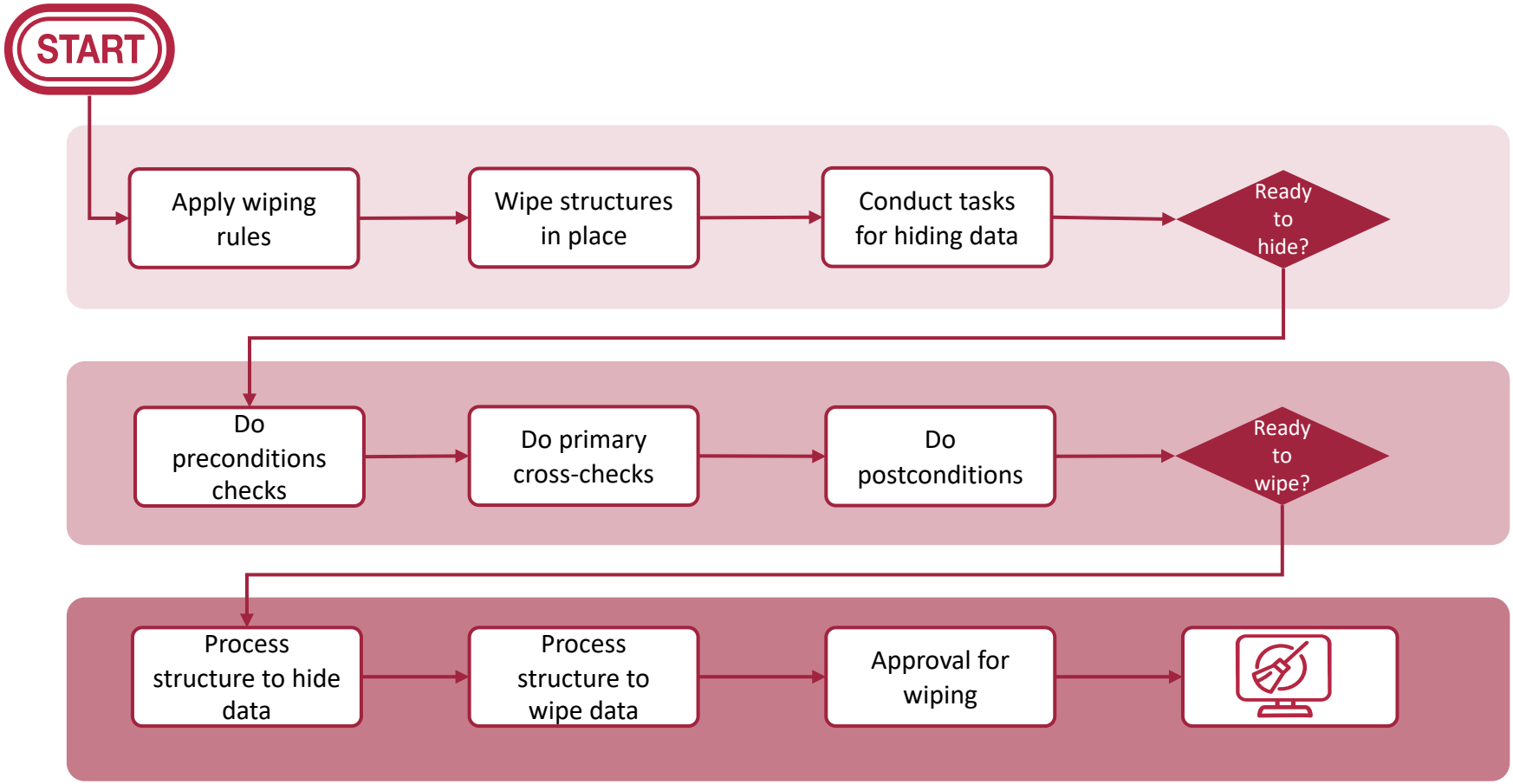
Also known as data erasure or secure data deletion, Process of permanently removing data from a storage device to ensure it cannot be recovered



Two-step Approach: Hide and Wipe



Wiping Process



Data Protection Check List

Data Inventory & Classification
- Identify the types of personal data collected or processed
- Document the data sources and data flows
- Classify data by sensitivity

Privacy by Design & Default
- Embed privacy controls into architecture and workflows early
- Default settings limit data collection, access, and retention to the minimum necessary
- Use pseudonymization or anonymization where appropriate
- Synthesize test data if technically possible and where needed (e.g. externalised testing done abroad)

Data Security & Access Controls
- Implement role-based access control (RBAC)
- Encrypt personal data at rest and in transit
- Use strong authentication (e.g., MFA) for sensitive systems
- Regularly test for vulnerabilities (e.g., penetration testing, code reviews)
- Secure backup systems and disaster recovery plans

Data Subject Rights & Transparency
- Provide clear, accessible privacy notices (DSG Art. 19)
- Enable data subjects to exercise their rights: Right to information, Right to access, Right to rectification or deletion
- procedures for responding to data access requests within legal deadlines
- Ensure data portability is possible where applicable

Retention & Deletion Policies
- Define retention periods for each data category
- Implement automatic or scheduled data deletion processes
- Include secure data wiping for decommissioned systems or drives

Third-Party & Cloud Providers
- Assess and document data processing agreements (DPAs) with all processors
- Ensure providers offer DSG-compliant safeguards
- Perform data protection impact assessments (DPIA) if high-risk processing is involved
- Monitor compliance of processors (audits or certifications)

Incident & Breach Management
- Have a data breach response plan
- Define internal reporting procedures (who, how, when)
- Notify the FDPIC (Federal Data Protection and Information Commissioner) within 72 hours if needed

Training & Awareness
- Provide mandatory data protection training to project members and staff
- Update training content with changes in legal or technical requirements
- Raise awareness about phishing, social engineering, and safe data handling

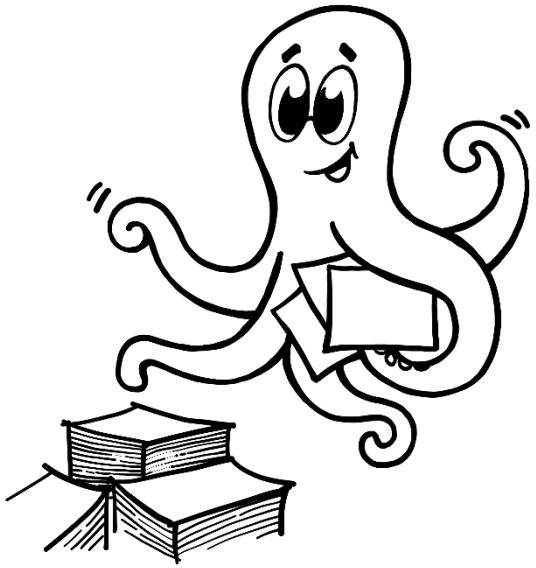
Governance & Audits
- Assign a Data Protection Officer (DPO) if required
- Regularly review and update policies and procedures
- Log access and changes to personal data (audit trails)
- Schedule data protection audits or self-assessments

Tools & Documentation
- Maintain a processing register
- Use a privacy impact checklist before deploying new features
- Keep documentation of all technical and organizational measures

What's the most effective data protection method you've encountered and why?

Take away and must know!

- To understand the importance of data protection regulations
- To identify sensitive PII data for customers, employees and 3rd parties
- To know the techniques to protect data (by design, by default, DLP and data wiping)



Literature

- www.edoeb.admin.ch/en/different-phases-of-the-employment-relationship
- www.fedlex.admin.ch/eli/cc/2022/491/en
- www.gdpr.eu/what-is-gdpr

KNOWLEDGE

www. know-ledge.ch