ACONTRARIO

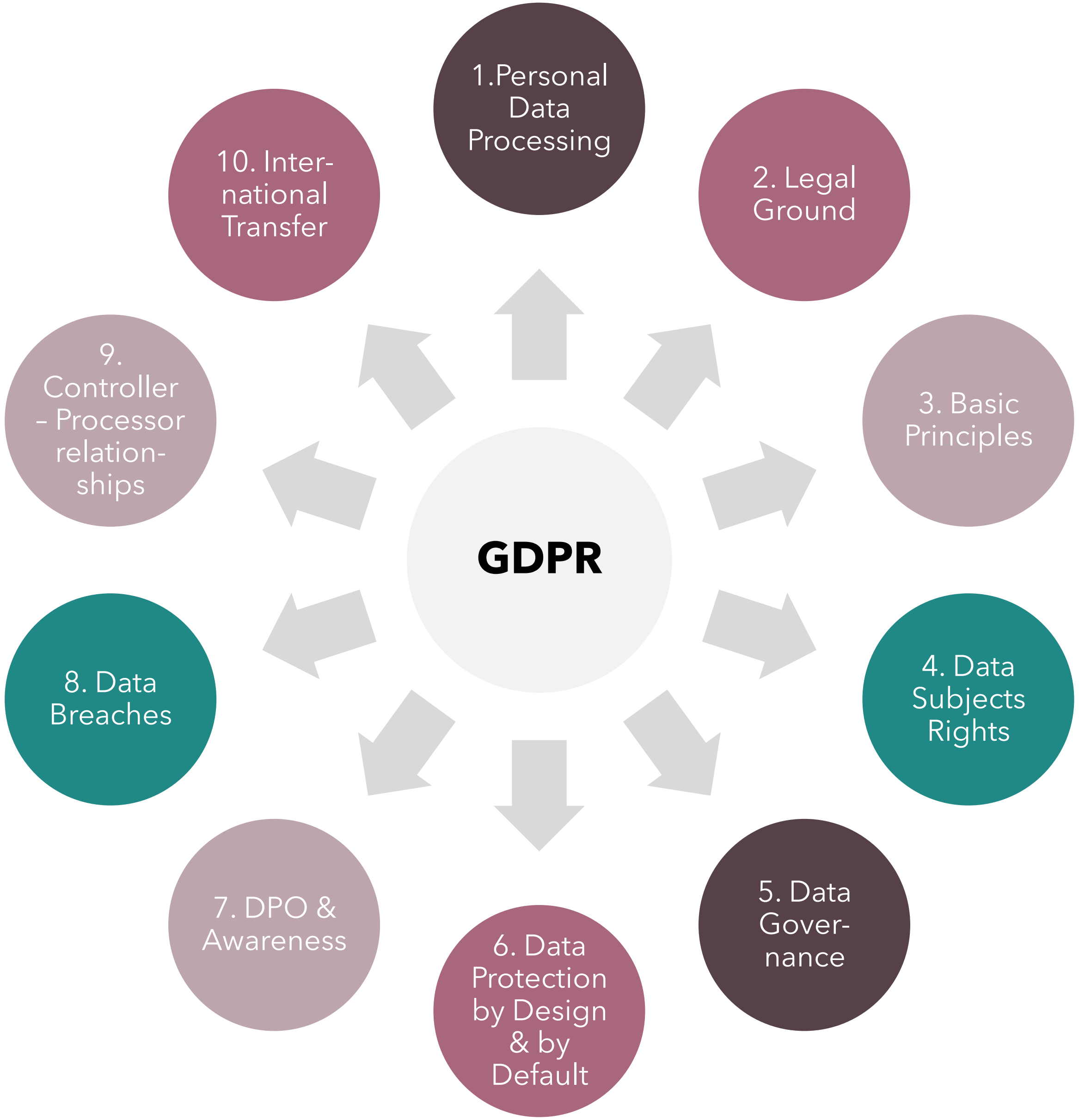
Secondary use of Healthcare Data

Anonymisation vs. Pseudonymisation

GDPR Cornerstones

AContrario's
10 cornerstones
of GDPR compliance

Interplay of **legal**, **ethical**, **organizational** and **technical** obligations and efforts


GDPR
1.Personal Data Processing
2. Legal Ground
3. Basic Principles
4. Data Subjects Rights
5. Data Gover-nance
6. Data Protection by Design & by Default
7. DPO & Awareness
8. Data Breaches
9. Controller – Processor relation-ships
10. Inter-national Transfer

Secondary Use of Health Data

General concepts

ACONTRARIO

Consent vs. Legitimate interest

GDPR Consent vs. Health law Consent

ACONTRARIO

Secondary Use of Health Data

Compatibility of Purposes (1)

- Article 5.1 (b) GDPR requires personal data to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

    - Further processing for scientific research in accordance with article 89.1 GDPR shall not be considered incompatible with the initial purpose and thus requires no new legal ground for processing
        - Article 89.1 GDPR requires appropriate safeguards to be in place in order to ensure respect for the principle of data minimization => Those measures may include GDPR compliant pseudonymization!

Secondary Use of Health Data

Compatibility of Purposes (2)

- In case the further processing is not covered by article 5.1 (b) GDPR, the purpose of further processing might still be compatible with the initial purpose on the basis of article 6.4 GDPR
  - Once again reference is made to the need for appropriate safeguards, which may include pseudonymization

- When no compatibility can be established on the basis of article 5.1 (b) or article 6.4 GDPR, a new legal basis will have to be found
  - This might entail that you will have to pass by an ethical committee

Consent vs. Legitimate Interest

As a legal ground for lawful processing

<u>In case compatibility test requires new lawful ground for secondary use of health data:</u>

- Health related personal data can only be processed (such as anonymised, shared, etcetera) on the basis of:
  - Art. 6, §1 GDPR + Art. 9, §2 GDPR

- The processing of health related patient data as part of a datavalorisation project, such as secondary use, can be justified on the basis of:
  - the legitimate interests of the data controller (= hospital) (article 6, 1, f); and
  - the necessity for scientific research (article 9, 2, j)

GDPR Consent vs. Health law Consent

- Consent under health law does not equal consent under the GDPR
  - Likewise, consent under Swiss Data Protection Act is not informed consent under Swiss Human Research Act

- Misconception about informed consent confirmed by the EDPB in its guidelines on the interplay between the GDPR and the CTR
  - Consent in CTR primarily refers to the core ethical requirement to ensure the human dignity and right to integrity => It is not conceived as an instrument for data protection!

- Consent under GDPR must be freely given, specific, informed, unambiguous (and in case of special categories of data explicit) in order to be considered as a valid legal ground for processing
  - This threshold will often not be met in the context of the CTR or HRA

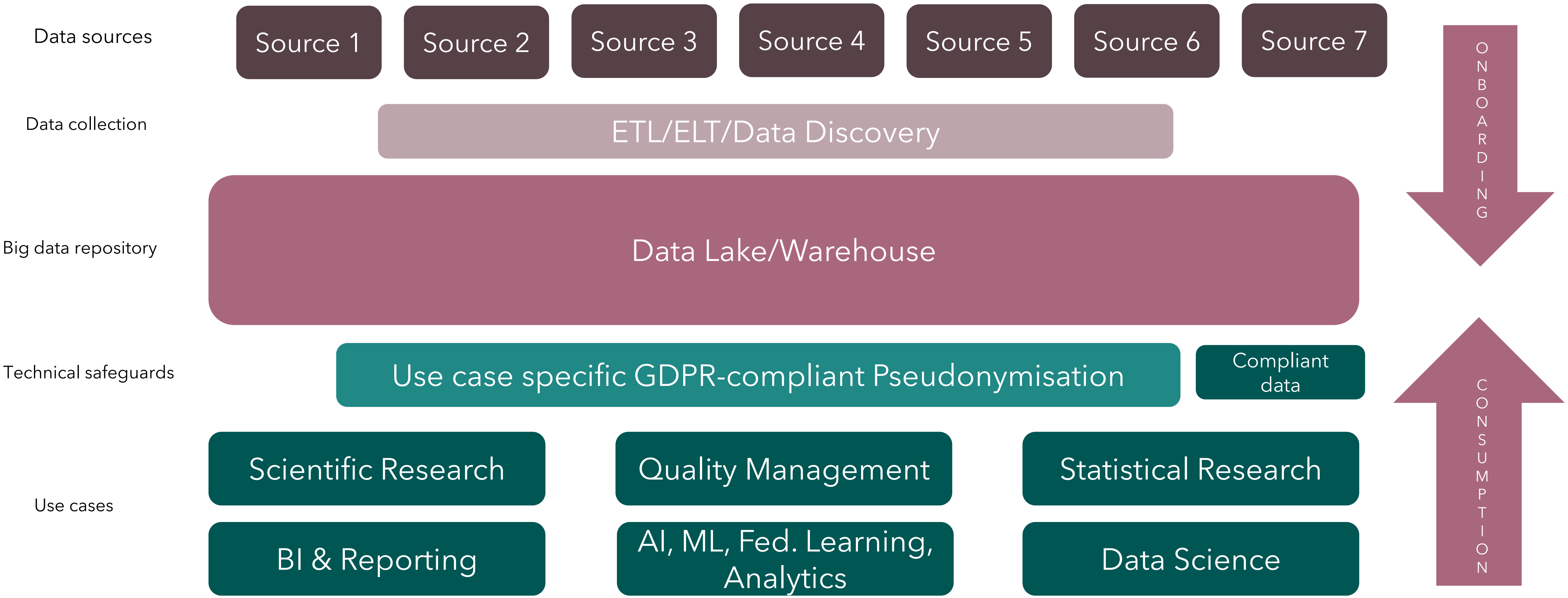
Charter for secondary use

Data governance model

ACONTRARIO

Use case governance

Role based access to data will not be sufficient to manage access correctly



Data sources

Source 1

Source 2

Source 3

Source 4

Source 5

Source 6

Source 7

Data collection

ETL/ELT/Data Discovery

Big data repository

Data Lake/Warehouse

Technical safeguards

Use case specific GDPR-compliant Pseudonymisation

Compliant data

Use cases

Scientific Research

Quality Management

Statistical Research

BI & Reporting

AI, ML, Fed. Learning, Analytics

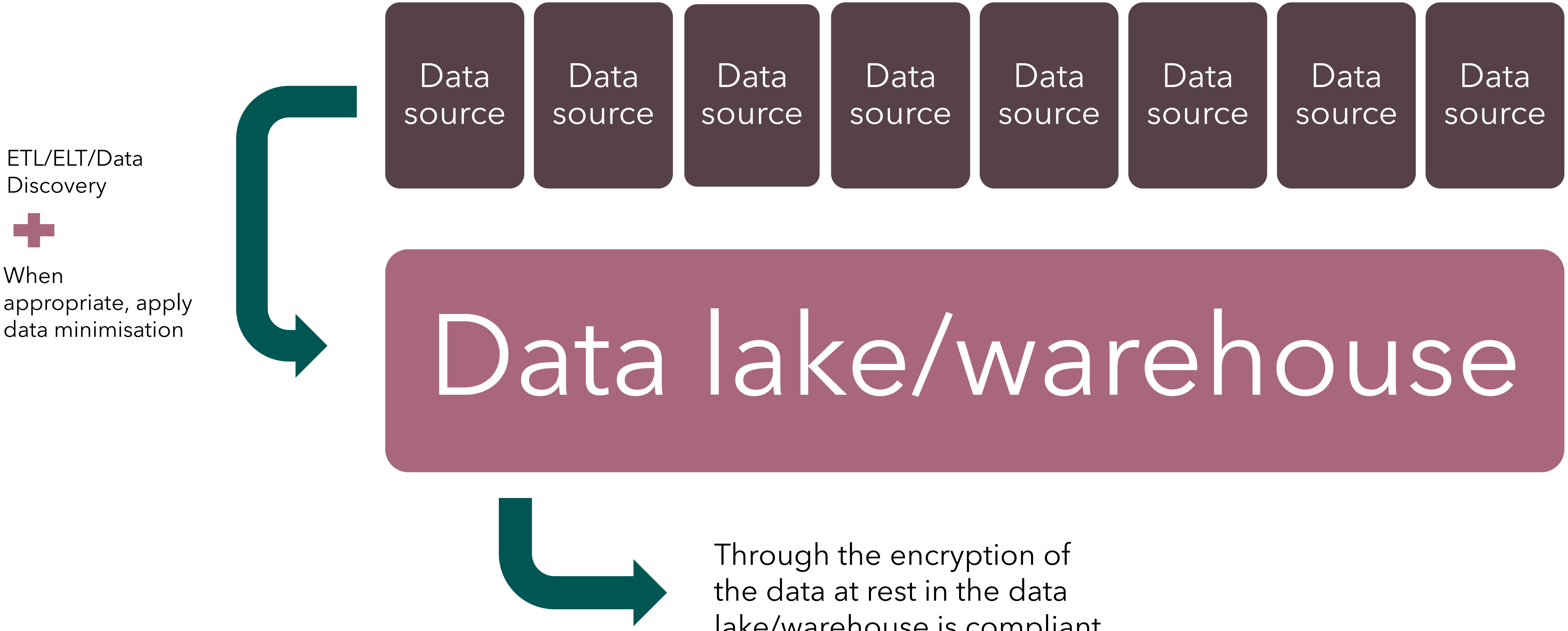
Data Science

ONBOARDING

CONSUMPTION

Use case governance

Role based access to data will not be sufficient to manage access correctly



ETL/ELT/Data Discovery

➕

When appropriate, apply data minimisation

Data source

Data source

Data source

Data source

Data source

Data source

Data source

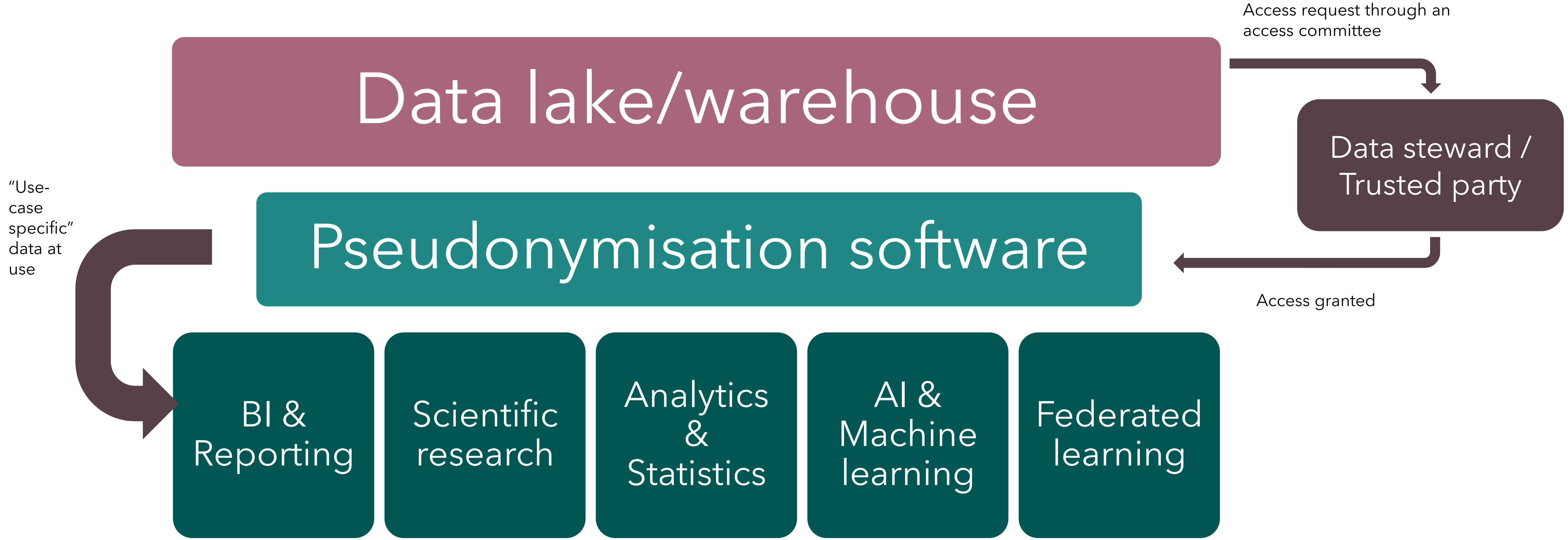
Data source

Data lake/warehouse

Through the encryption of the data at rest in the data lake/warehouse is compliant

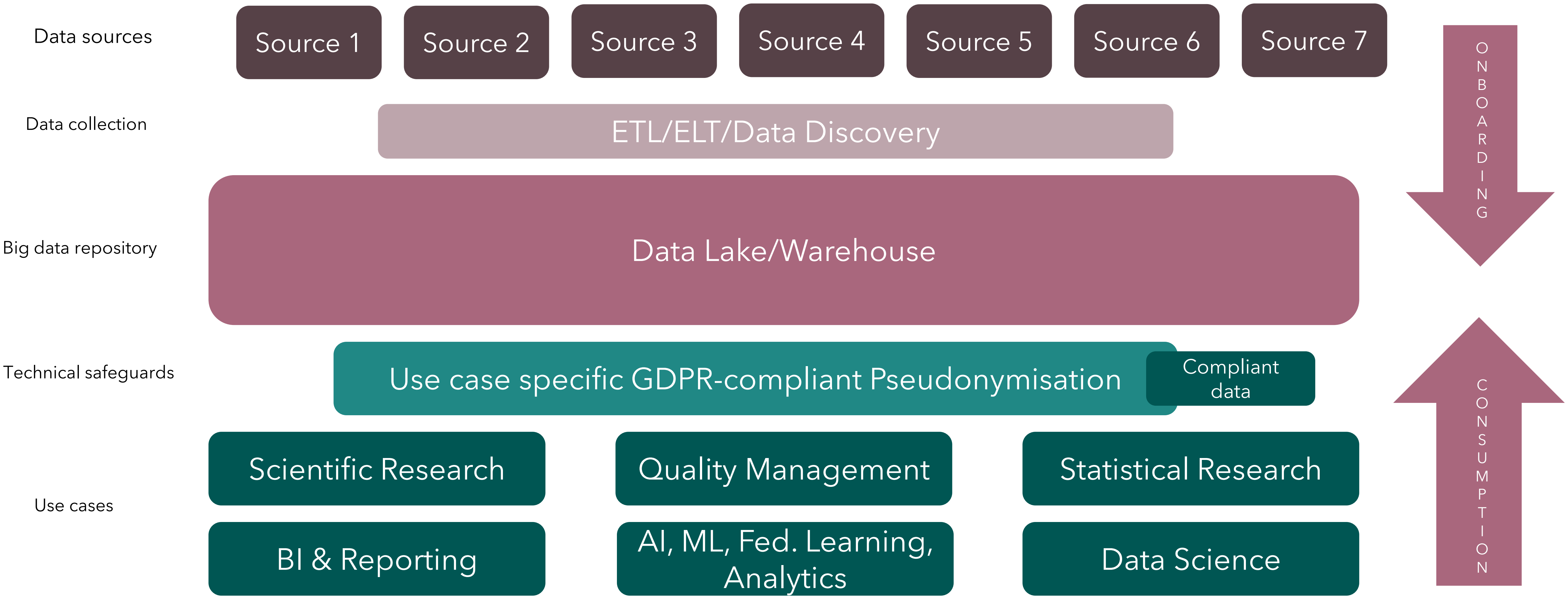
Use case governance

Role based access to data will not be sufficient to manage access correctly



Use case governance

Role based access to data will not be sufficient to manage access correctly



Data sources

Source 1

Source 2

Source 3

Source 4

Source 5

Source 6

Source 7

Data collection

ETL/ELT/Data Discovery

Big data repository

Data Lake/Warehouse

Technical safeguards

Use case specific GDPR-compliant Pseudonymisation

Compliant data

Use cases

Scientific Research

Quality Management

Statistical Research

BI & Reporting

AI, ML, Fed. Learning, Analytics

Data Science

ONBOARDING

CONSUMPTION

Anonymization vs Pseudonymization

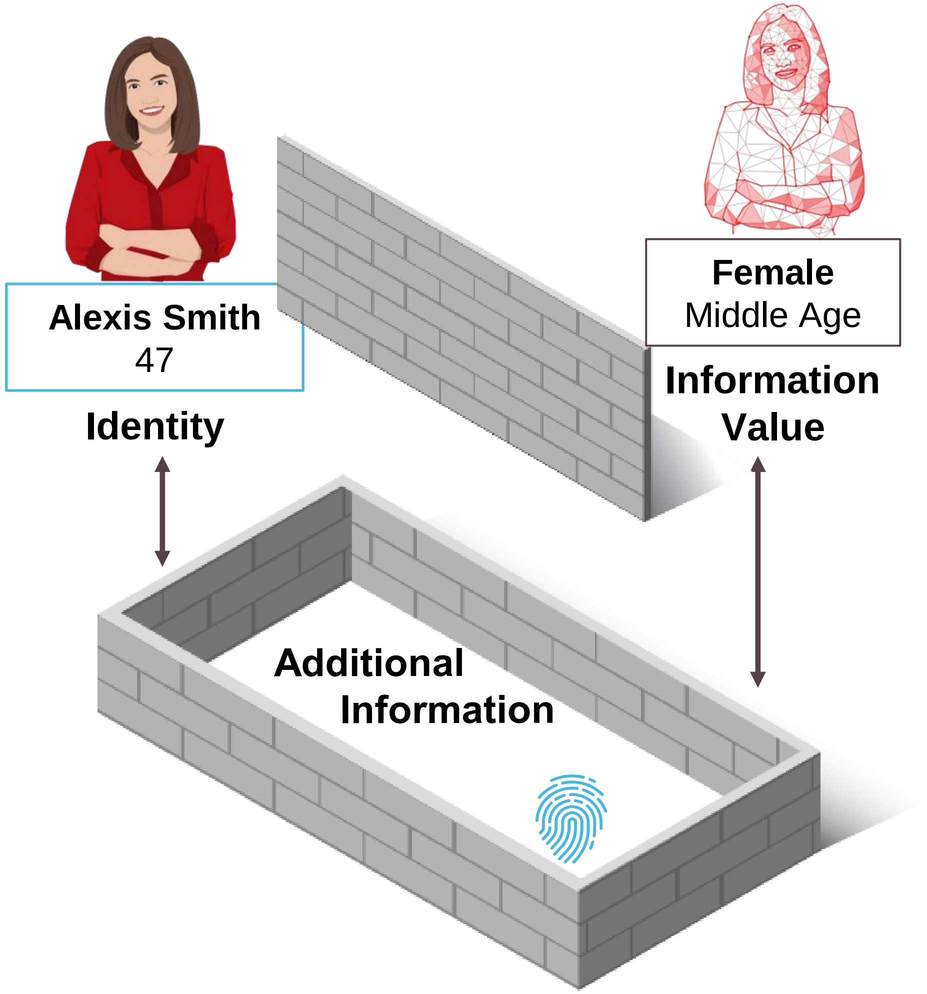
What's in a name?

ACONTRARIO

The 6 truths of Pseudonymisation

1. GDPR Pseudonymisation is not the same as Anonymisation
2. GDPR Pseudonymisation is a higher standard than pre-GDPR Pseudonymisation
3. GDPR Pseudonymisation is not failed Anonymisation
4. GDPR Pseudonymisation requires protection of more than direct identifiers
5. GDPR Pseudonymisation provides more value than Anonymisation
6. GDPR Pseudonymisation requires dynamism

The EDPB recommends GDPR pseudonymisation



Alexis Smith
47

Identity

Female
Middle Age

Information Value

Additional Information

EDPB LAWFUL SCHREMS II USE CASE 2

Transfer Of **Pseudonymised** Data

Schrems II Lawful Use Cases

USE CASE 1
Data Storage For Backup And Other Purposes That Do Not Require Access To Data in the Clear

USE CASE 2
Transfer Of **Pseudonymised** Data

USE CASE 3
Encrypted Data Merely Transiting Third Countries

USE CASE 4
Protected Recipient

USE CASE 5
Split or Multi-Party Processing

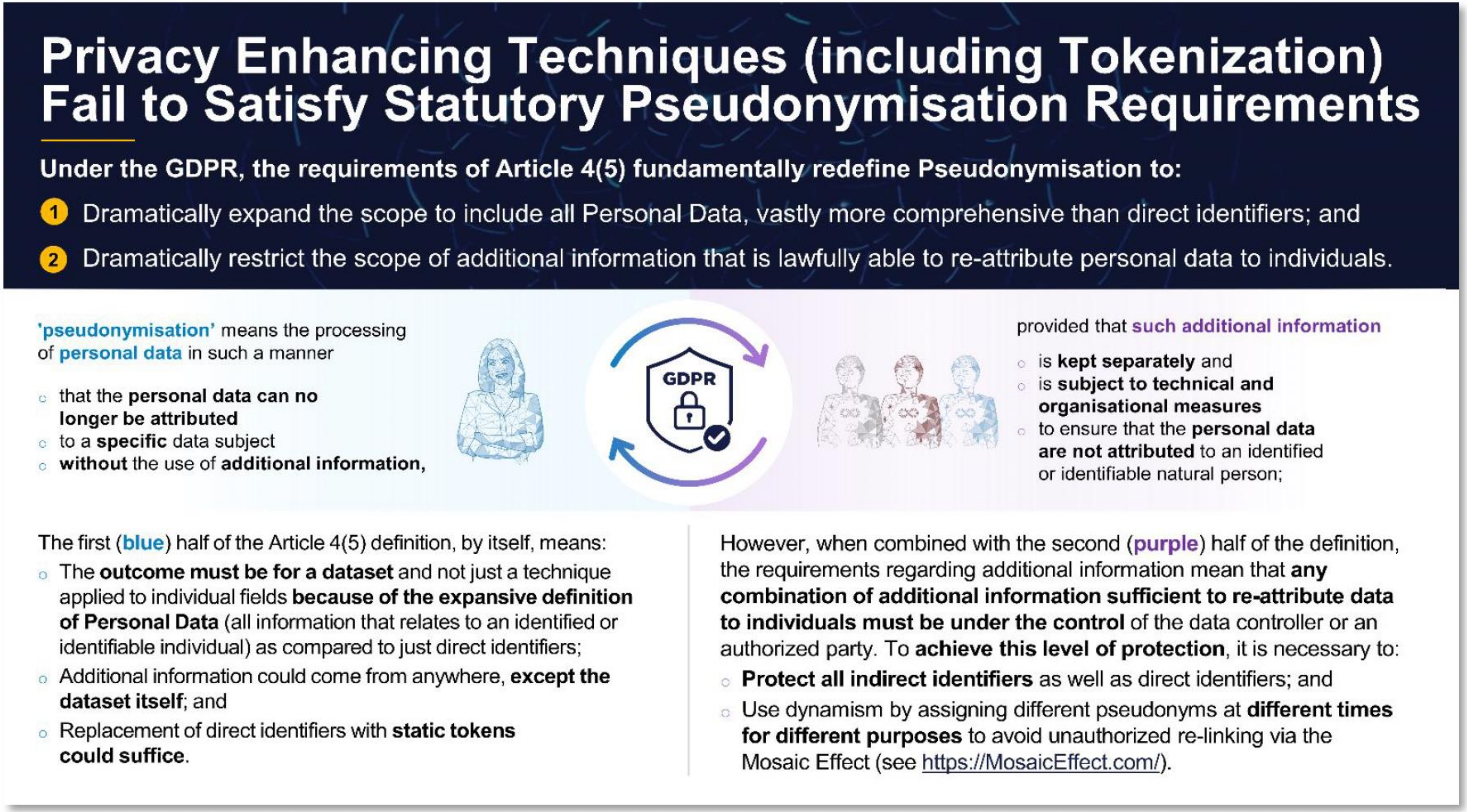
Schrems II Unlawful Use Cases

USE CASE 6*
Transfer to Cloud Services Providers or Other Processors Which Require Access to Data in the Clear

USE CASE 7*
Transfer of Personal Data for Business Purposes Including by Way of Remote Access

* and **this data is not – or cannot – be pseudonymised as described in Use Case 2** or encrypted as described in Use Case 1 because the processing **requires accessing data in the clear**

https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf



Privacy Enhancing Techniques (including Tokenization) Fail to Satisfy Statutory Pseudonymisation Requirements

Under the GDPR, the requirements of Article 4(5) fundamentally redefine Pseudonymisation to:

1. Dramatically expand the scope to include all Personal Data, vastly more comprehensive than direct identifiers; and
2. Dramatically restrict the scope of additional information that is lawfully able to re-attribute personal data to individuals.

'pseudonymisation' means the processing of **personal data** in such a manner

- that the **personal data can no longer be attributed**
- to a **specific** data subject
- **without** the use of **additional information,**

provided that **such additional information**

- is **kept separately** and
- is **subject to technical and organisational measures**
- to ensure that the **personal data are not attributed** to an identified or identifiable natural person;

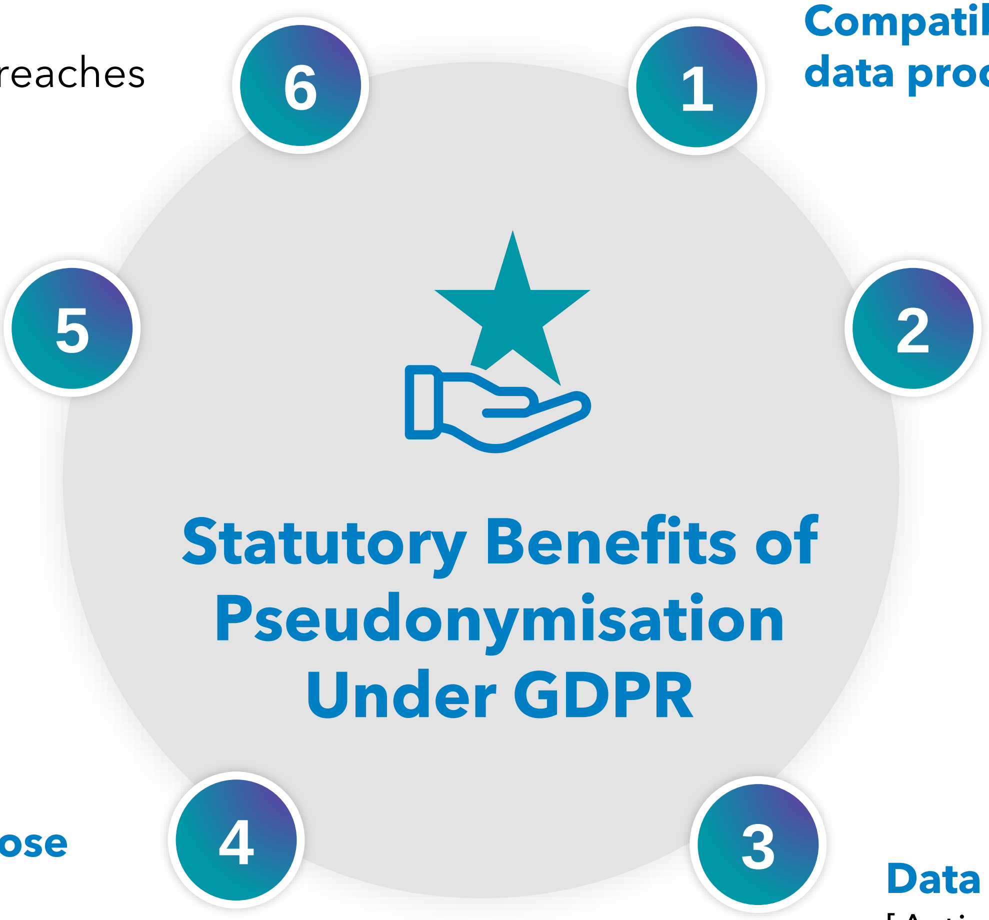
The first (**blue**) half of the Article 4(5) definition, by itself, means:

- The **outcome must be for a dataset** and not just a technique applied to individual fields **because of the expansive definition of Personal Data** (all information that relates to an identified or identifiable individual) as compared to just direct identifiers;
- Additional information could come from anywhere, **except the dataset itself**; and
- Replacement of direct identifiers with **static tokens could suffice**.

However, when combined with the second (**purple**) half of the definition, the requirements regarding additional information mean that **any combination of additional information sufficient to re-attribute data to individuals must be under the control** of the data controller or an authorized party. To **achieve this level of protection**, it is necessary to:

- **Protect all indirect identifiers** as well as direct identifiers; and
- Use dynamism by assigning different pseudonyms at **different times for different purposes** to avoid unauthorized re-linking via the Mosaic Effect (see https://MosaicEffect.com/).

Statutory Benefits of Statutory Pseudonymisation



Statutory Benefits of Pseudonymisation Under GDPR

1 **Compatibility of new (secondary) data processes** [GDPR Article 6(4)]

2 **Support for Legitimate Interest processing** for: [Article 6(1)(f)]

- Greater flexibility in complying with **Right to be Forgotten / Right to Erasure** requests [Article 17(1)(c)]
- Greater flexibility in complying with **Right to Restrict Processing** requests [Article 18(1)(d)]
- Exclusion from the **Right to Data Portability** [Article 20(1)]
- Greater flexibility in overcoming **Right to Object to Processing** requests [Article 21(1)]

3 **Data sharing & combining**: [Articles 11(2) & 12(2)]

4 **Data minimisation, purpose limitation, & data protection by design and by default** [Articles 5(1)(b) & (c), 25(1)]

5 **Support for scientific/historical research and statistical processing** to enable: [Article 89(1)]

- **Secondary processing, sharing and combining of data by** expanding purpose limitation [Article 5(1)(b)]
- **Extended permissible storage** of data [Article 5(1)(e)]
- **Processing of "sensitive" special categories** of personal data [Article 9(2)(j)]

6 **Reduced disclosure obligations/liability** for data breaches [Articles 32, 33 and 34]

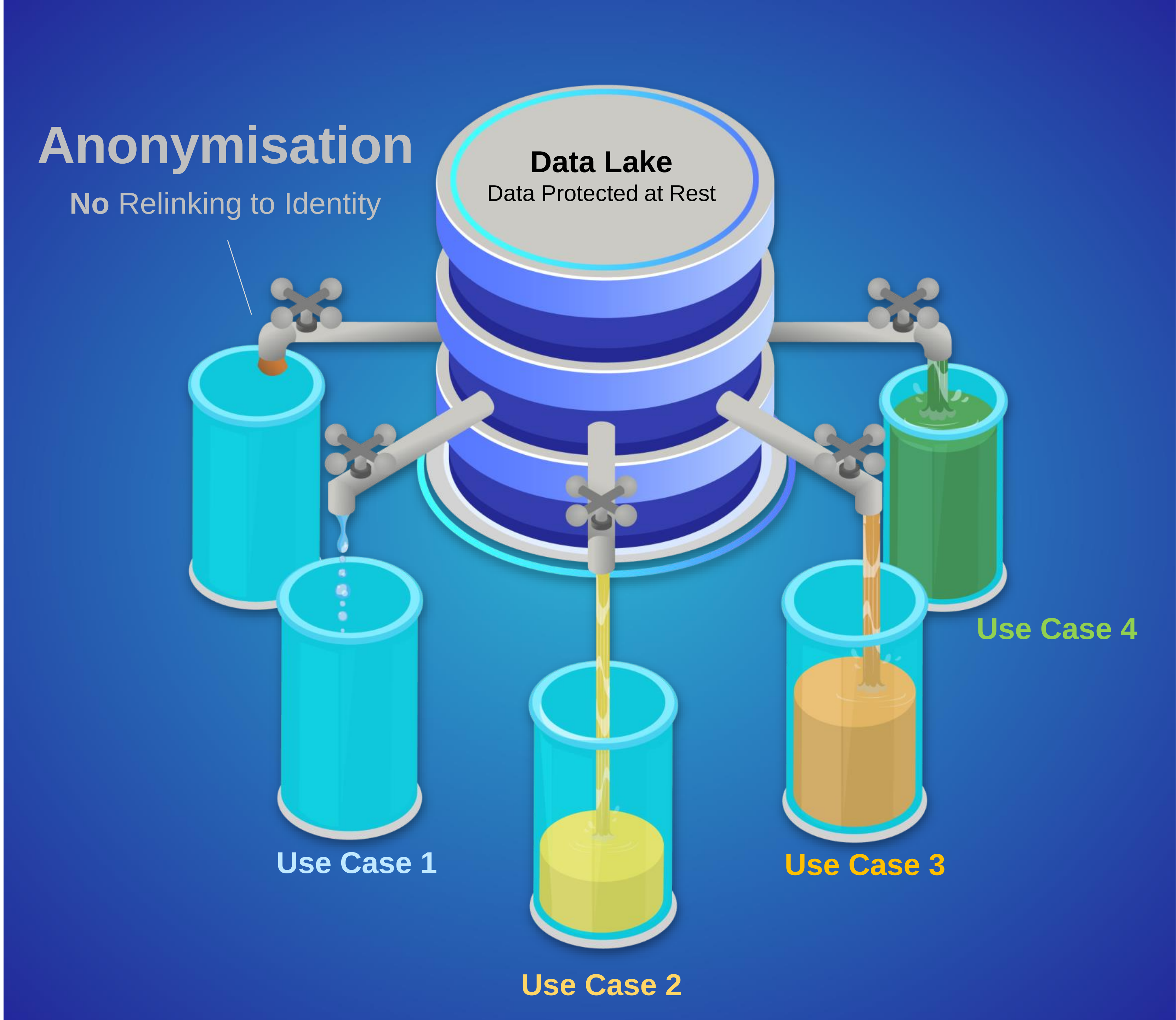
Use case governance

Data Type	Data As Is	Variant 1: lightly minimsed	Variant 2: further minimised	Variant 3: pseudonymised
Photo		/	/	/
Name	Vanessa Nsomme	Vanessa Nsomme	ID_RE3Kjj33	ID_345aZJ98
Date of birth	2 June 1992	/	/	ID 125687
Sex	Female	Female	Female	ID ABC13
Address (street)	Stationstraat 4	/	/	/
Address (city)	Zonnedorp	Zonnedorp	Zonnedorp	Province of Antwerp
Reference department	Endocrinology	Endocrinology	Unit ID dfjm7	Unit ID dfjm7
Diabetes Type	1	1	1	Type ID KJMKJ12
Retinopathy	Yes	Yes	Yes	Retino ID sfjL9I
Last glucose reading	124	110-130	/	110-130

GDPR Pseudonymisation Context Specific At Use Protection:

- Purpose Limitation
- Data Minimisation
- Value Maximisation

Only GDPR Pseudonymisation-enabled "At Risk" controls limit the AMOUNT of identifying data (Data Minimisation) and the TYPE of data (Purpose Limitation) to enable ALL use cases.



Anonymisation

No Relinking to Identity

Data Lake

Data Protected at Rest

Use Case 1

Use Case 2

Use Case 3

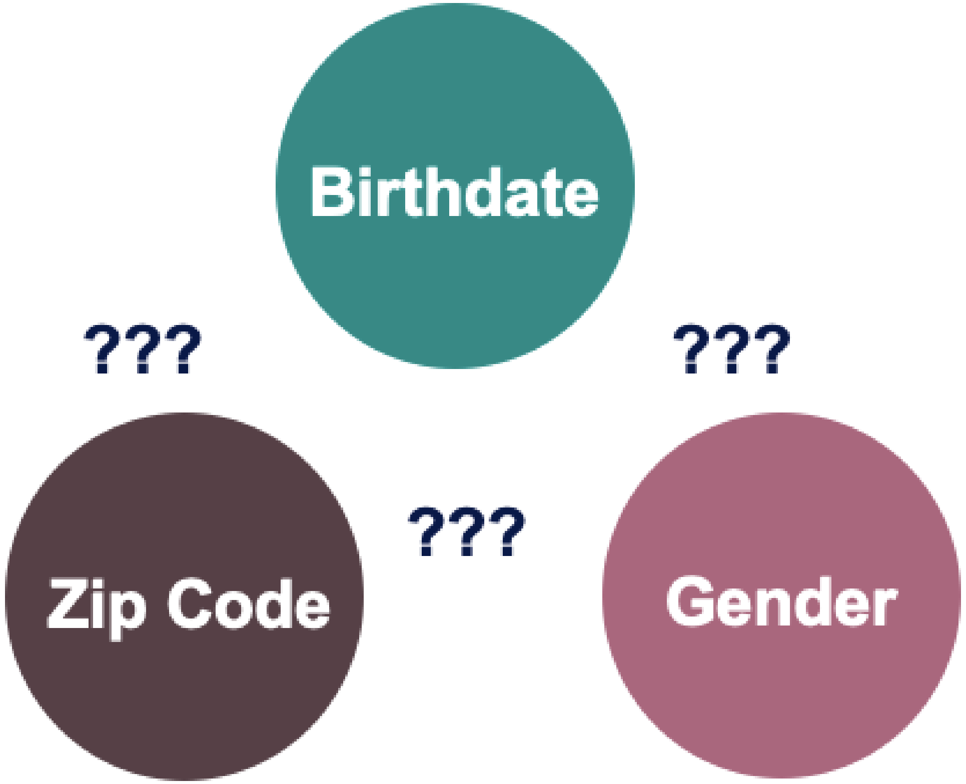
Use Case 4

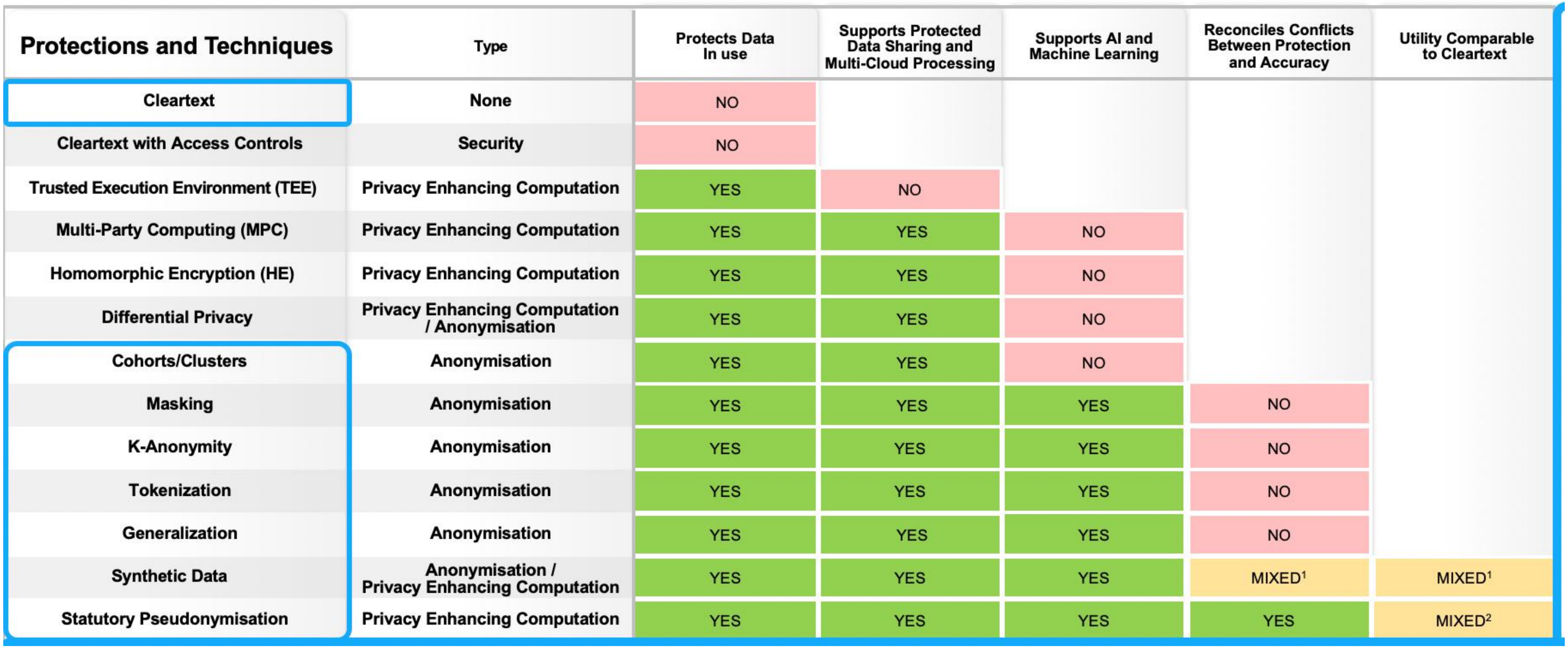
Using dynamism to defeat re-identification risk via the mosaic effect

???
ABCD
???
Q991
???
19Q4

Additional Information Kept Separately

ABCD	Q991	19Q4
Alex Smith	Alex Smith	Alex Smith





Protections and Techniques	Type	Protects Data In use	Supports Protected Data Sharing and Multi-Cloud Processing	Supports AI and Machine Learning	Reconciles Conflicts Between Protection and Accuracy	Utility Comparable to Cleartext
Cleartext	None	NO				
Cleartext with Access Controls	Security	NO				
Trusted Execution Environment (TEE)	Privacy Enhancing Computation	YES	NO			
Multi-Party Computing (MPC)	Privacy Enhancing Computation	YES	YES	NO		
Homomorphic Encryption (HE)	Privacy Enhancing Computation	YES	YES	NO		
Differential Privacy	Privacy Enhancing Computation / Anonymisation	YES	YES	NO		
Cohorts/Clusters	Anonymisation	YES	YES	NO		
Masking	Anonymisation	YES	YES	YES	NO	
K-Anonymity	Anonymisation	YES	YES	YES	NO	
Tokenization	Anonymisation	YES	YES	YES	NO	
Generalization	Anonymisation	YES	YES	YES	NO	
Synthetic Data	Anonymisation / Privacy Enhancing Computation	YES	YES	YES	MIXED[1]	MIXED[1]
Statutory Pseudonymisation	Privacy Enhancing Computation	YES	YES	YES	YES	MIXED[2]

[1] Vendors claim and Buyers believe YES; informed commentary concludes NO.

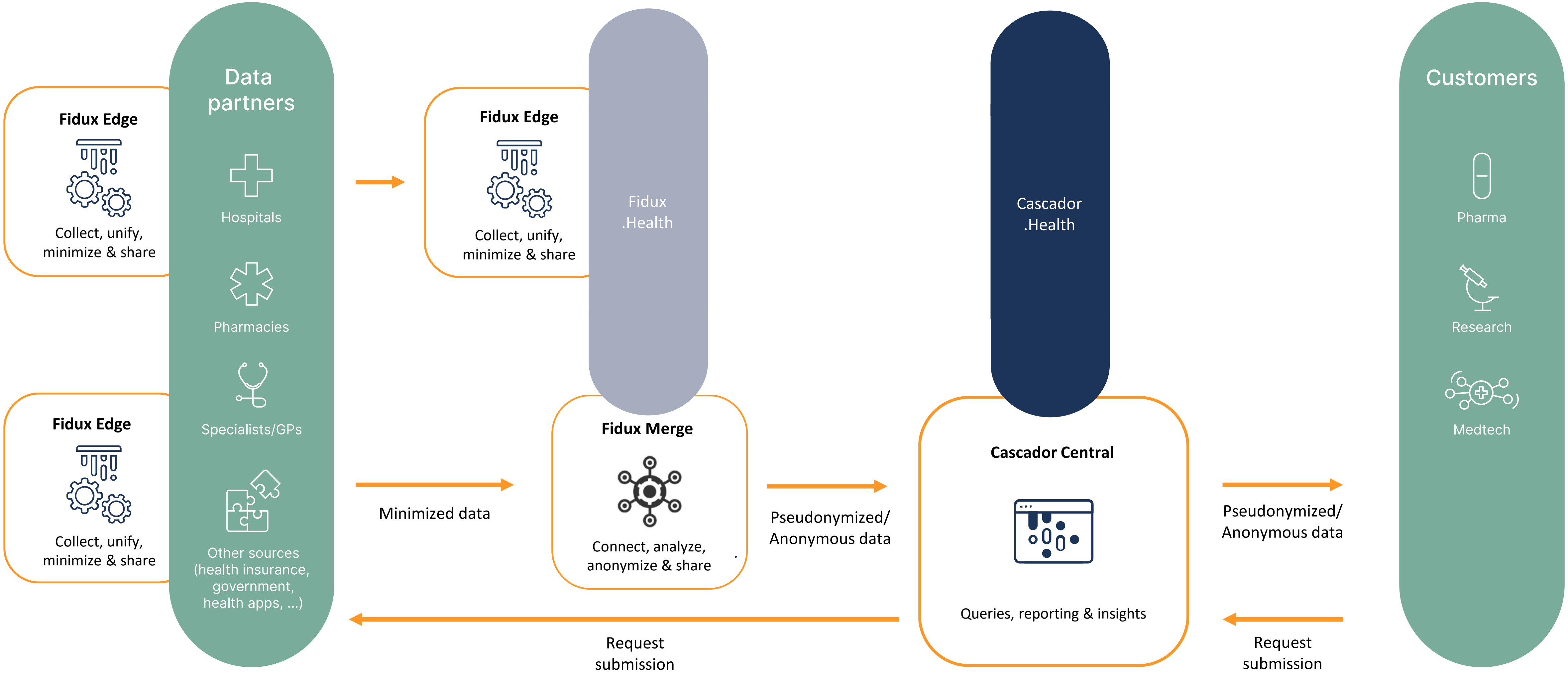
[2] Buyers assume NO; informed commentary concludes YES.

Charter for secondary use

Data governance model

ACONTRARIO

Ecosystem for RWD use & valorisation

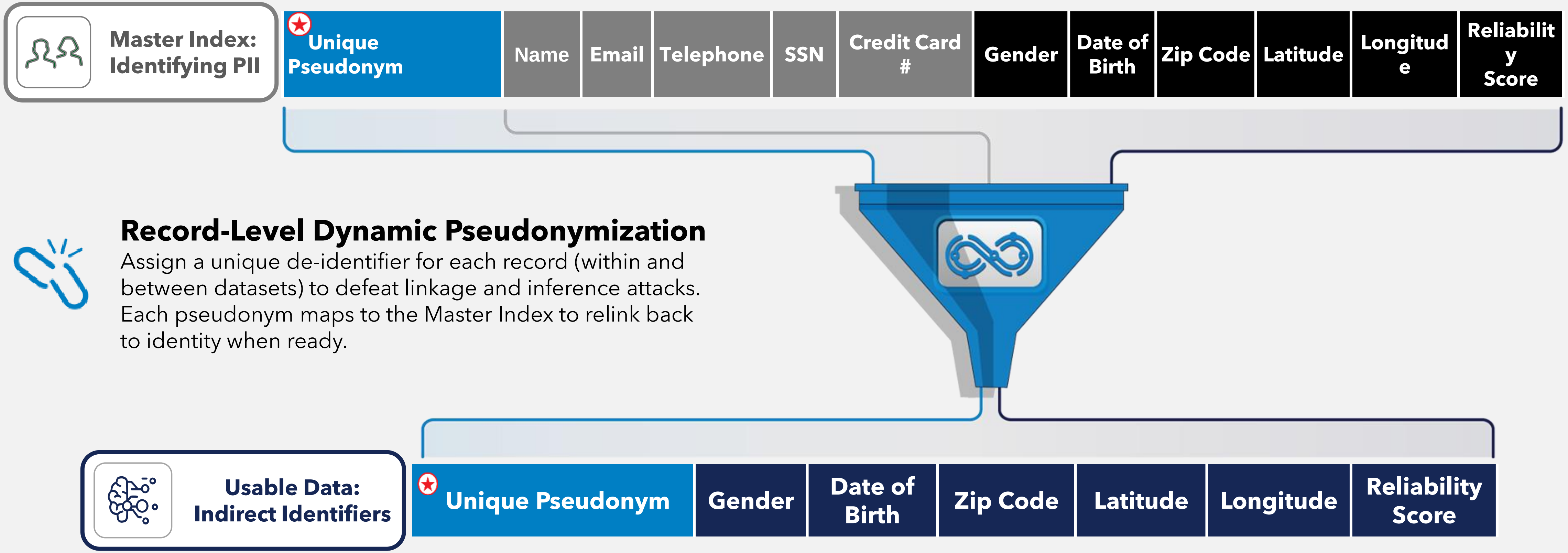

Fidux Edge
Collect, unify, minimize & share
Fidux Edge
Collect, unify, minimize & share
Data partners
Hospitals
Pharmacies
Specialists/GPs
Other sources (health insurance, government, health apps, ...)
Fidux Edge
Collect, unify, minimize & share
Fidux .Health
Minimized data
Fidux Merge
Connect, analyze, anonymize & share
Pseudonymized/ Anonymous data
Cascador .Health
Cascador Central
Queries, reporting & insights
Pseudonymized/ Anonymous data
Request submission
Request submission
Customers
Pharma
Research
Medtech

Example of pseudonymised complex dataset

ACONTRARIO

De-Linking & Data Use Minimization:

Separating Information Value From Identity



Master Index: Identifying PII	★ Unique Pseudonym	Name	Email	Telephone	SSN	Credit Card #	Gender	Date of Birth	Zip Code	Latitude	Longitude	Reliability Score

Record-Level Dynamic Pseudonymization
Assign a unique de-identifier for each record (within and between datasets) to defeat linkage and inference attacks. Each pseudonym maps to the Master Index to relink back to identity when ready.

Usable Data: Indirect Identifiers	★ Unique Pseudonym	Gender	Date of Birth	Zip Code	Latitude	Longitude	Reliability Score

★ Enables Dynamic De-Risking and Controlled Relinkability

Dynamic De-Risking:

Creation of Privacy Transformers

Embedding protection into the data:

1. Anonymization Techniques
2. Field-Level Pseudonymization
3. Re-Identification Risk Management

Protecting against:

✓ Inference attacks
✓ Linkage attacks
✓ Singling out

RD-97cef37aef9ad9120efc	Gender	Date of Birth	Zip Code	Latitude	Longitude	Reliability Score
RD-97cef37aef9ad9120efc	Male	40-49	100XX	51.593	-0.037	Very Good
	Gender-wr6m	age10-Vf2Q	zip3-d9Bh	lat3-ev8F	long3-dv9S	rel-Udv3

Privacy Action + Re-ID Mitigation = Privacy Transformer

Policy Automation:

Privacy Transformer Scales Variant Twin Creation

Privacy Transformer Enforces Policy

★RD-97cef37aef9ad9120efc	gender-wr6m	age10-Vf2Q	zip3-d9Bh	lat3-ev8F	long3-dv9S	rel-Udv3

Variant Twin Embodies Policy

Unique Pseudonym	Gender	Age_10	Zip_3	Lat_3	Long_3	Reliability Score
★ RD-97cef37aef9ad9120efc	gender-wr6m	age10-Vf2Q	zip3-d9Bh	lat3-ev8F	long3-dv9S	rel-Udv3
RD-c75dd862e63ed8d259b0	gender-wr6m	age10-0z4S	zip3-1cgh	lat3-dv0J	long3-dv2X	rel-Udv3
RD-9c015cba189493b9cac8	gender-wr6m	age10-qPTL	zip3-d9Bh	lat3-ev8F	long3-dv9S	rel-sc6K
RD-80d74c7536e5bc706f8a	gender-OrWg	age10-1fcQ	zip3-uy4c	lat3-iob4	long3-iev5	rel-Udv3
RD-b6ff1a08bf59ecc70f15	gender-OrWg	age10-aMpl	zip3-d9Bh	lat3-5jAn	long3-7eeG	rel-j9dV

Variant Twins enable scalable sharing, combining and enriching of data for Big Data, AI and ML

Controlled Relinkability:

Universal Protection & Unrivaled Utility

Variant Twin

Unique Pseudonym	Gender	Age_10	Zip_3	Lat_3	Long_3	Reliability Score	Retention Offer
RD-97cef37aef9ad9120efc	gender-wr6m	age10-Vf2Q	zip3-d9Bh	lat3-ev8F	long3-dv9S	rel-Udv3	Yes
RD-c75dd862e63ed8d259b0	gender-wr6m	age10-0z4S	zip3-1cgh	lat3-dv0J	long3-dv2X	rel-Udv3	No
RD-9c015cba189493b9cac8	gender-wr6m	age10-qPTL	zip3-d9Bh	lat3-ev8F	long3-dv9S	rel-sc6K	No
RD-80d74c7536e5bc706f8a	gender-OrWg	age10-1fcQ	zip3-uy4c	lat3-iob4	long3-iev5	rel-Udv3	Yes
RD-b6ff1a08bf59ecc70f15	gender-OrWg	age10-aMpl	zip3-d9Bh	lat3-5jAn	long3-7eeG	rel-j9dV	Yes

Master Index Match

Unique Pseudonym	Name	Email	Telephone	SSN	Credit Card #	Gender	Date of Birth	Zip Code	Latitude	Longitude	Reliability Score
RD-97cef37aef9ad9120efc	Steve	Steve@gmail.com	818-222-9067								
RD-80d74c7536e5bc706f8a	Sarah	Sarah@me.com	310-334-7854								
RD-b6ff1a08bf59ecc70f15	Jessie	Jessie@you.com	747-408-3402								

Next best action = Contact Steve, Sarah and Jessie with offer

About AContrario

<a contrario> lat., adj. or adv. "on the contrary"; contrary, contrarily, in the opposite sense

Focused on commercial, IP, IT and data protection law, AContrario is a premier business law firm offering innovative, specialized and personalized legal advice.

But AContrario is much more than that. It's the law firm reinvented. It's the escape from the ivory tower.

Sure, we can provide top-notch legal advice. We'll represent you in court or work out a settlement agreement for you too. But there is so much more we can do for you.

Find out more on www.acontrario.law.

Your contacts.

Magali Feys
Founder
IP, IT & Data Protection Lawyer

Tim Wulgaert
Data Security Lead
CISSP, CRISC, CISA & ISO27701 LI Certified

AContrario.Law

Stapelplein 70 – B. 9000 Gent
Ter Poelen 2 – B. 9080 Lochristi
+32 474 29 61 25