PRIVACY

IN PRACTICE

BAROUM MRAD
DPO, LLM, MBA

BAROUM MRAD

A LITTLE BIT OF HISTORY

Before moving to Switzerland, Baroum was the Director of Business Intelligence at CCA in Washington DC. He led a task force of Intelligence analyst teams with the objective to track Human Trafficking in Africa.

Baroum Started as a market research analyst in the IT industry, earning his experience and certifications in data science and intelligence analytics, before moving to the government field, where he was also exposed to privacy and Human Rights.

Baroum earned his Bachelor degree in Communication Sciences and Data Science at Rutgers University, in New Jersey, and his Executive Master of Business Administration (EMBA). He also completed the CAS DPO at St. Gallen University (HSG) and recently his Master of Law (LLM) in Compliance at Fribourg University.

CYBER TERRORISM

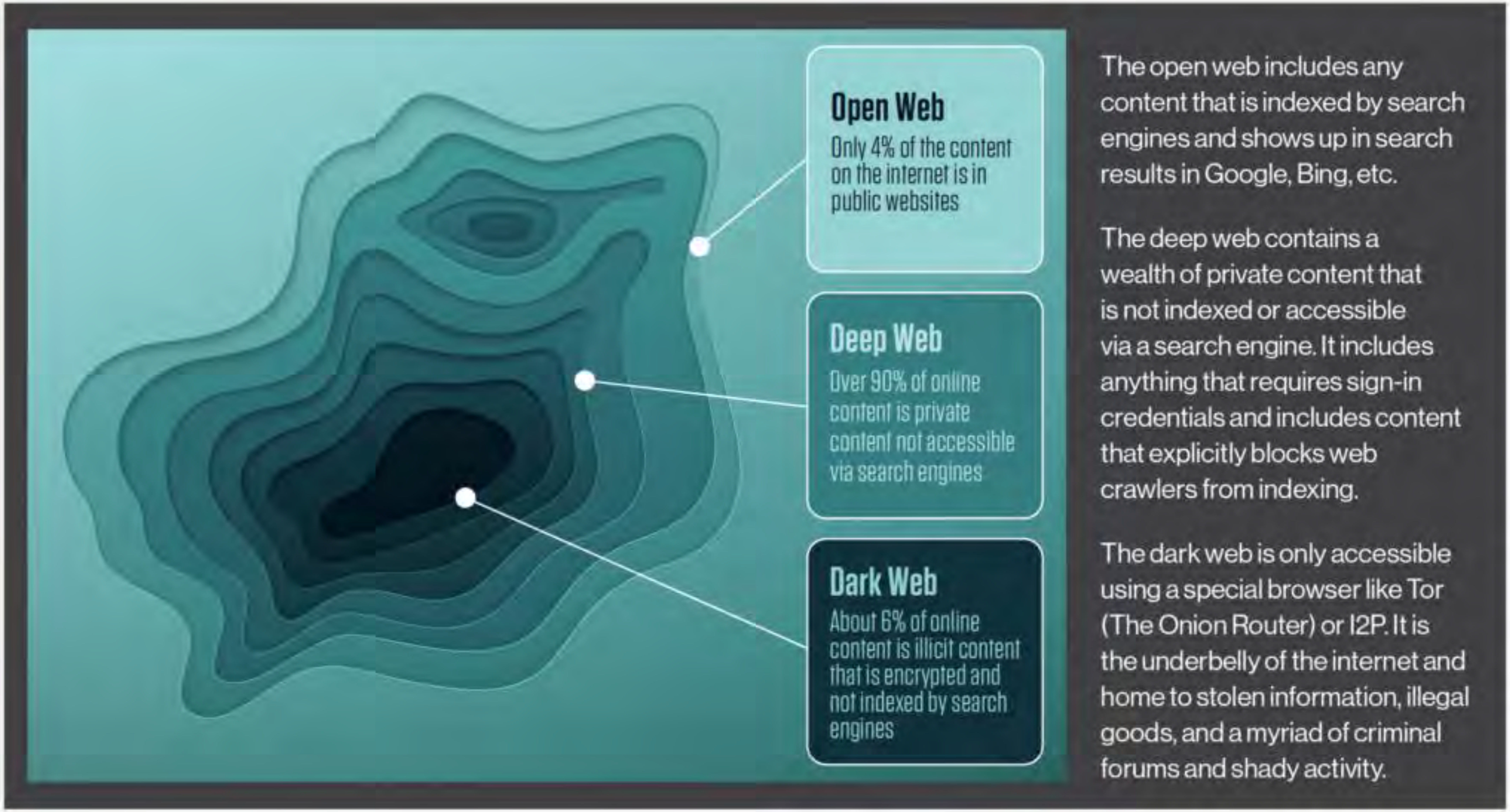
THE OTHER WEB

One is the most well known part of the Web, the Surface Web. The other parts are the submerged ones: Deep and Dark web, terms often confused, used interchangeably, and sometimes demonized. But in reality they indicate two different digital territories, of which in most cases there is no need to be afraid. However, it is important to understand what they are, particularly the Dark web.

4% Surface Web

96% Deep and Dark Web

Surface Web
Deep Web
Dark Web



Open Web

Only 4% of the content on the internet is in public websites

Deep Web

Over 90% of online content is private content not accessible via search engines

Dark Web

About 6% of online content is illicit content that is encrypted and not indexed by search engines

The open web includes any content that is indexed by search engines and shows up in search results in Google, Bing, etc.

The deep web contains a wealth of private content that is not indexed or accessible via a search engine. It includes anything that requires sign-in credentials and includes content that explicitly blocks web crawlers from indexing.

The dark web is only accessible using a special browser like Tor (The Onion Router) or I2P. It is the underbelly of the internet and home to stolen information, illegal goods, and a myriad of criminal forums and shady activity.

DARKNET

You can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you break into other people's computers.

Buy login credentials to a $50,000 Bank of America account for $500. Get $3,000 in counterfeit $20 bills for $600.

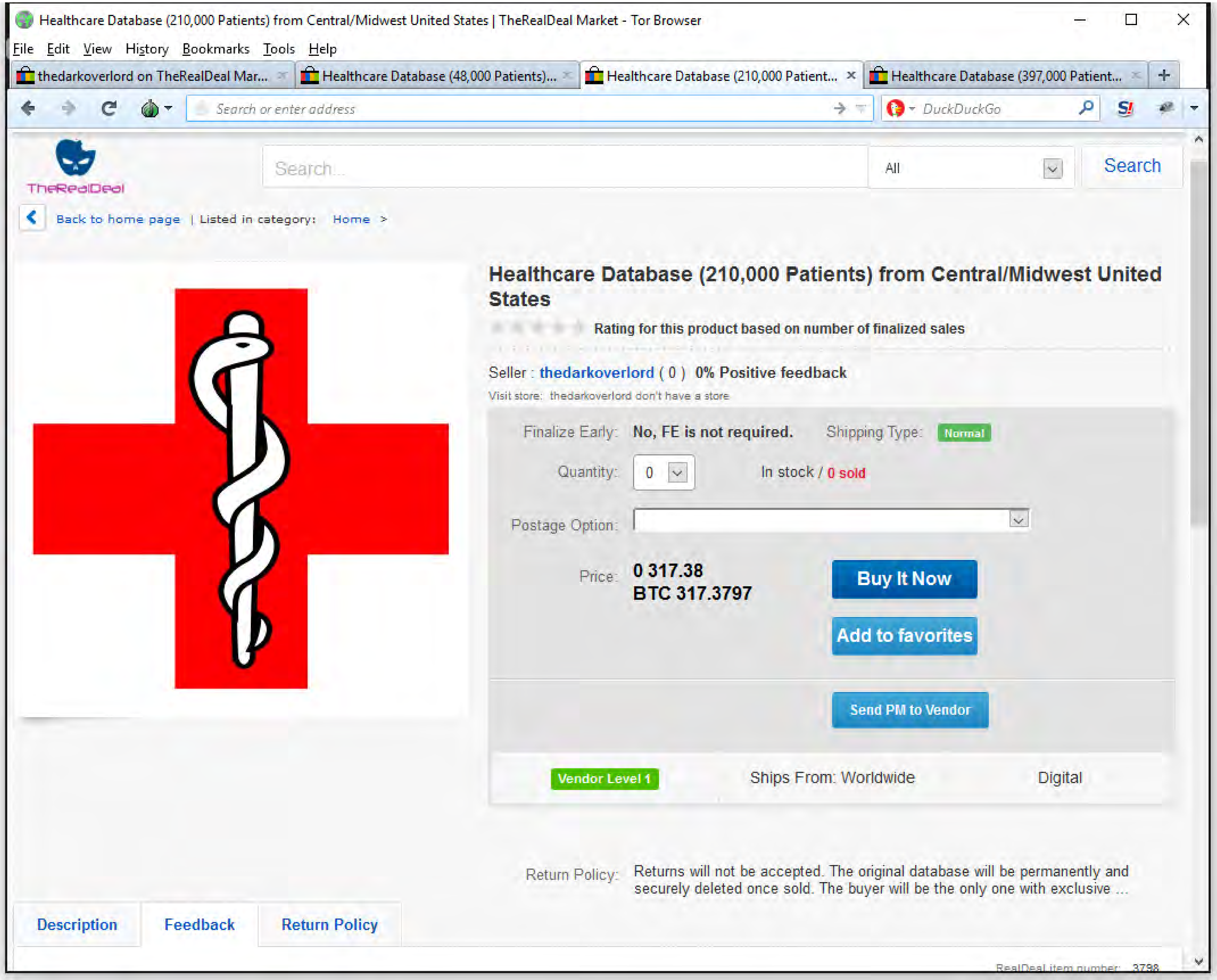
Buy seven prepaid debit cards, each with a $2,500 balance, for $500 (express shipping included).

A “lifetime” Netflix premium account goes for $6.

You can hire hackers to attack computers for you.

You can buy usernames and passwords.

But it is also used for secure communications and freedom of expression in countries where the risk of such communications is the death penalty or legal consequences.


Healthcare Database (210,000 Patients) from Central/Midwest United States | TheRealDeal Market - Tor Browser
File
Edit
View
History
Bookmarks
Tools
Help
thedarkoverlord on TheRealDeal Mar...
Healthcare Database (48,000 Patients)...
Healthcare Database (210,000 Patient...
Healthcare Database (397,000 Patient...
Search or enter address
DuckDuckGo
TheRealDeal
Search...
All
Search
Back to home page
Buy It Now
Add to favorites
Send PM to Vendor
Description
Feedback
Return Policy

Back to home page | Listed in category: Home >

Healthcare Database (210,000 Patients) from Central/Midwest United States

Rating for this product based on number of finalized sales

Seller : thedarkoverlord (0) 0% Positive feedback

Visit store: thedarkoverlord don't have a store

Finalize Early: No, FE is not required. Shipping Type: Normal

Quantity: 0 In stock / 0 sold

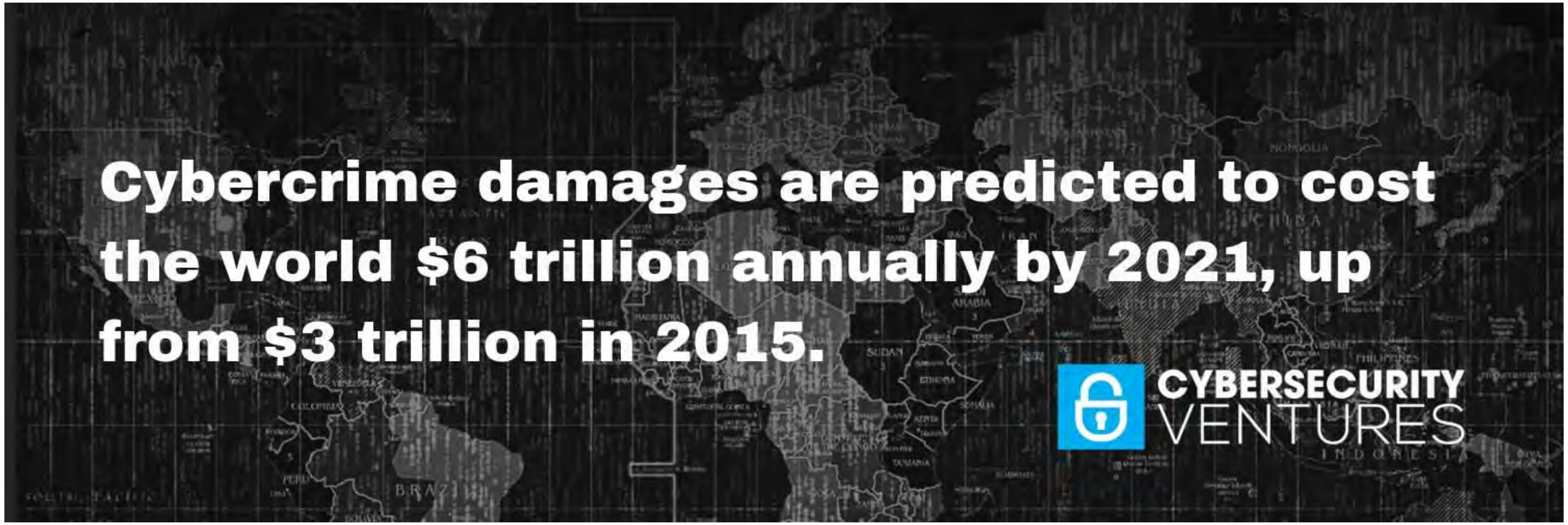
Postage Option:

Price: 0 317.38
BTC 317.3797

Vendor Level 1 Ships From: Worldwide Digital

Return Policy: Returns will not be accepted. The original database will be permanently and securely deleted once sold. The buyer will be the only one with exclusive ...

RealDeal item number: 3798



Cybercrime damages are predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

CYBERSECURITY
VENTURES

PRIVACY

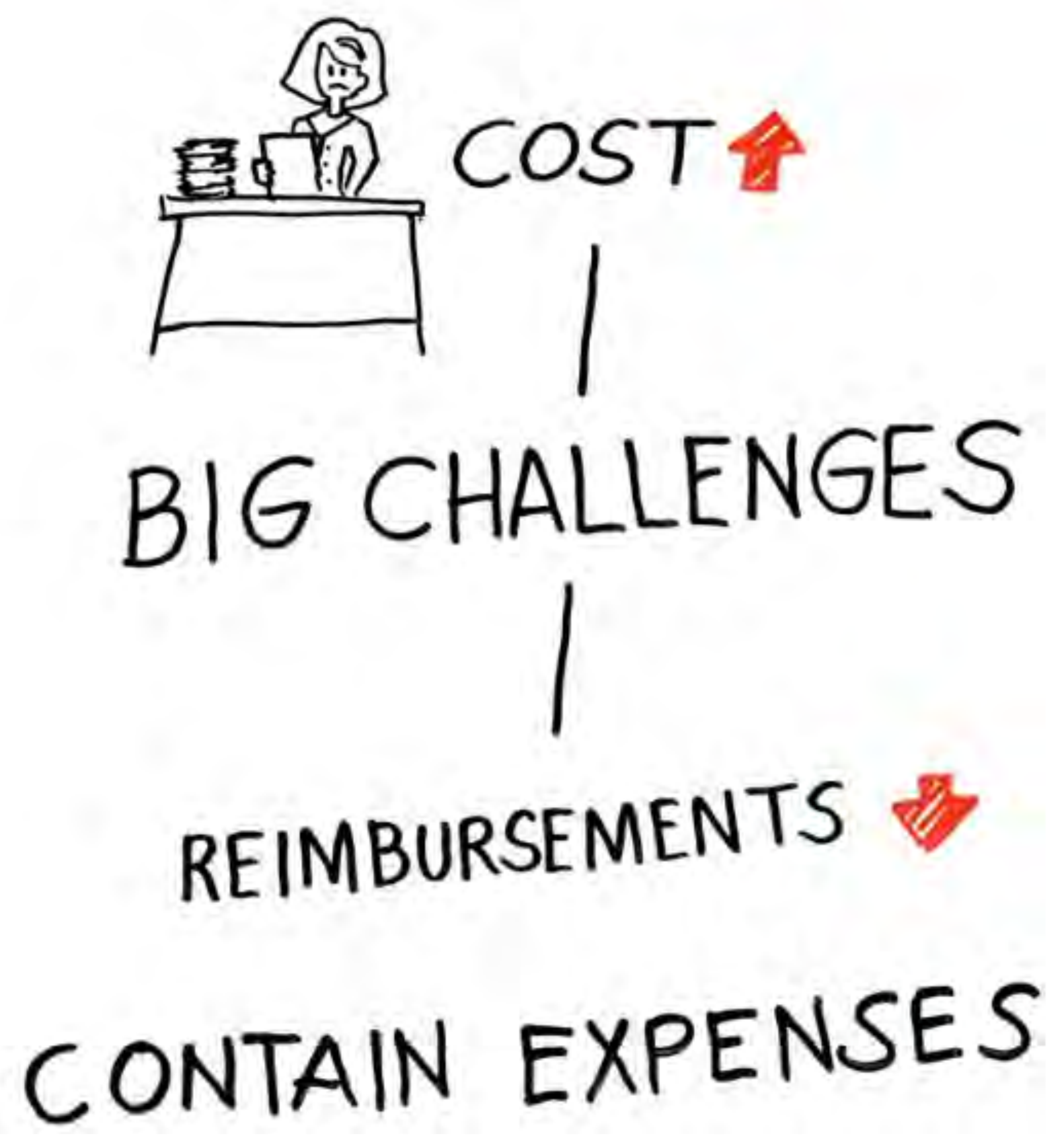
IN PRACTICE

LET US ANALYSE A PRACTICAL CASE:

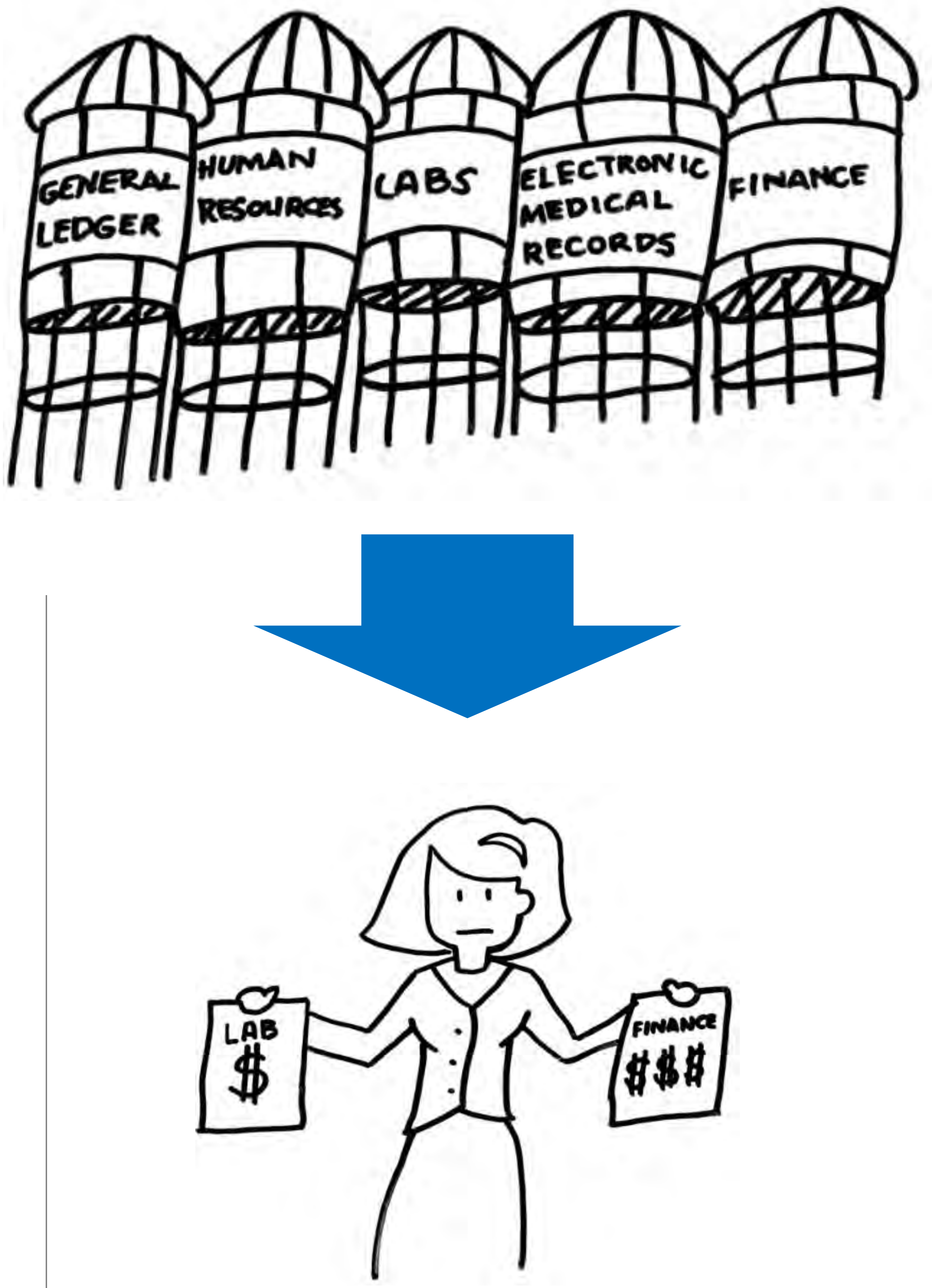
- HEALTH DATA
- DATA PROTECTION STRATEGY
- PANDEMIC
- THE FUTURE OF PRIVACY

PRIVACY IN PRACTICE

HEALTH DATA



?
DATA DATA
DATA DATA DATA
DATA DATA DATA
DATA DATA
DATA DATA

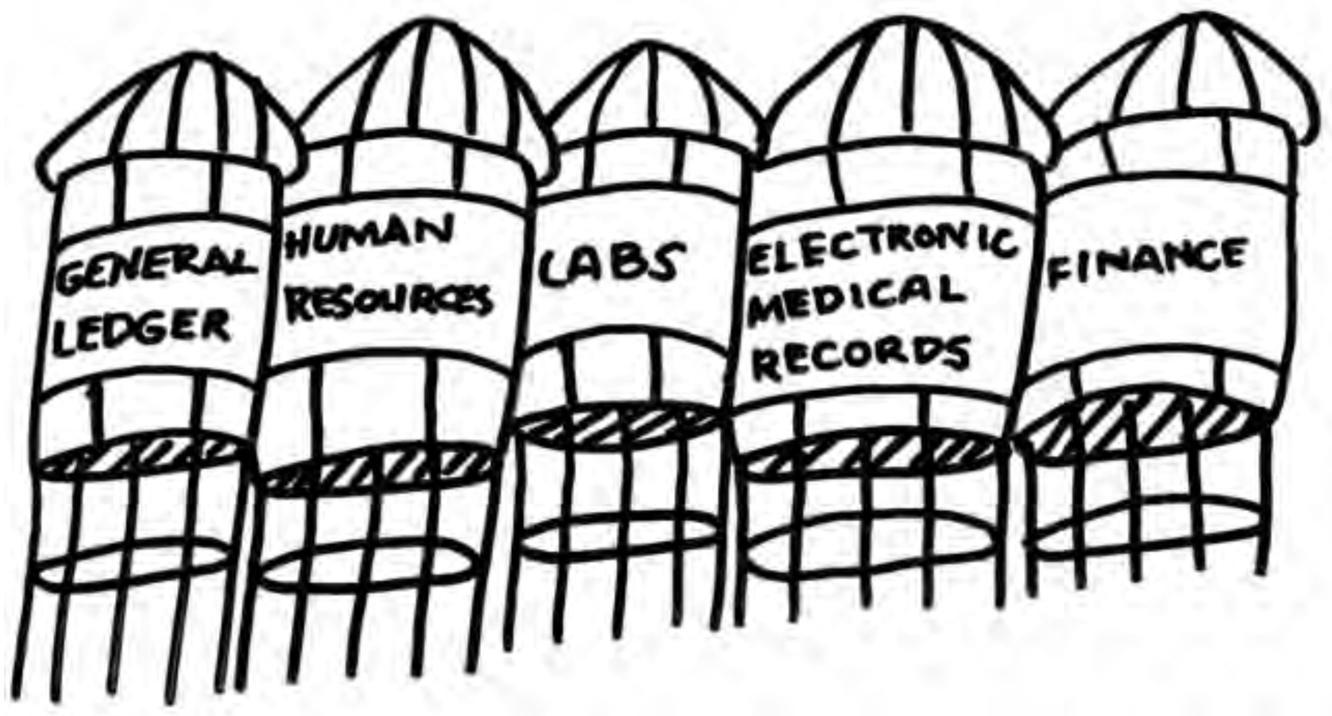


PRIVACY IN PRACTICE

HEALTH DATA

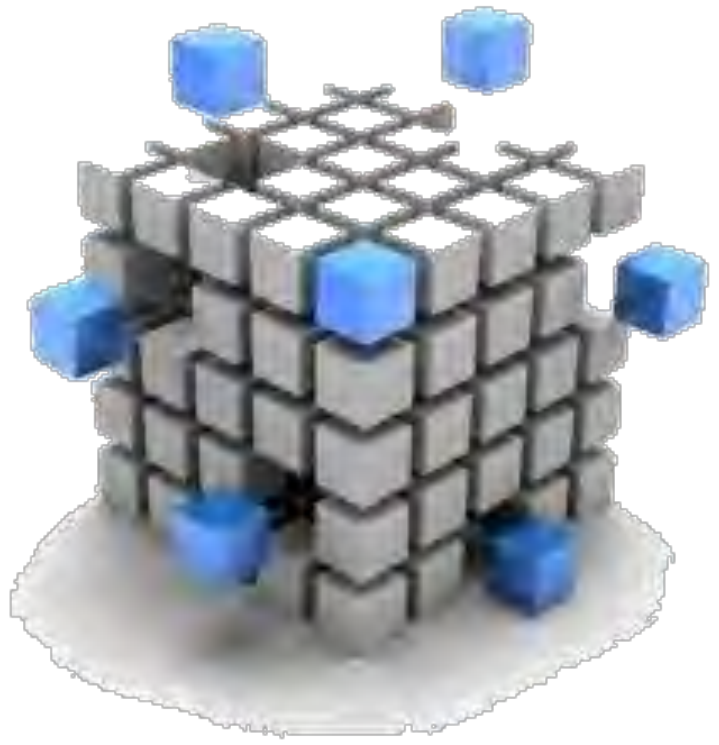
OLTP

- Operational data
- Short and simple data/queries
- Frequent updates



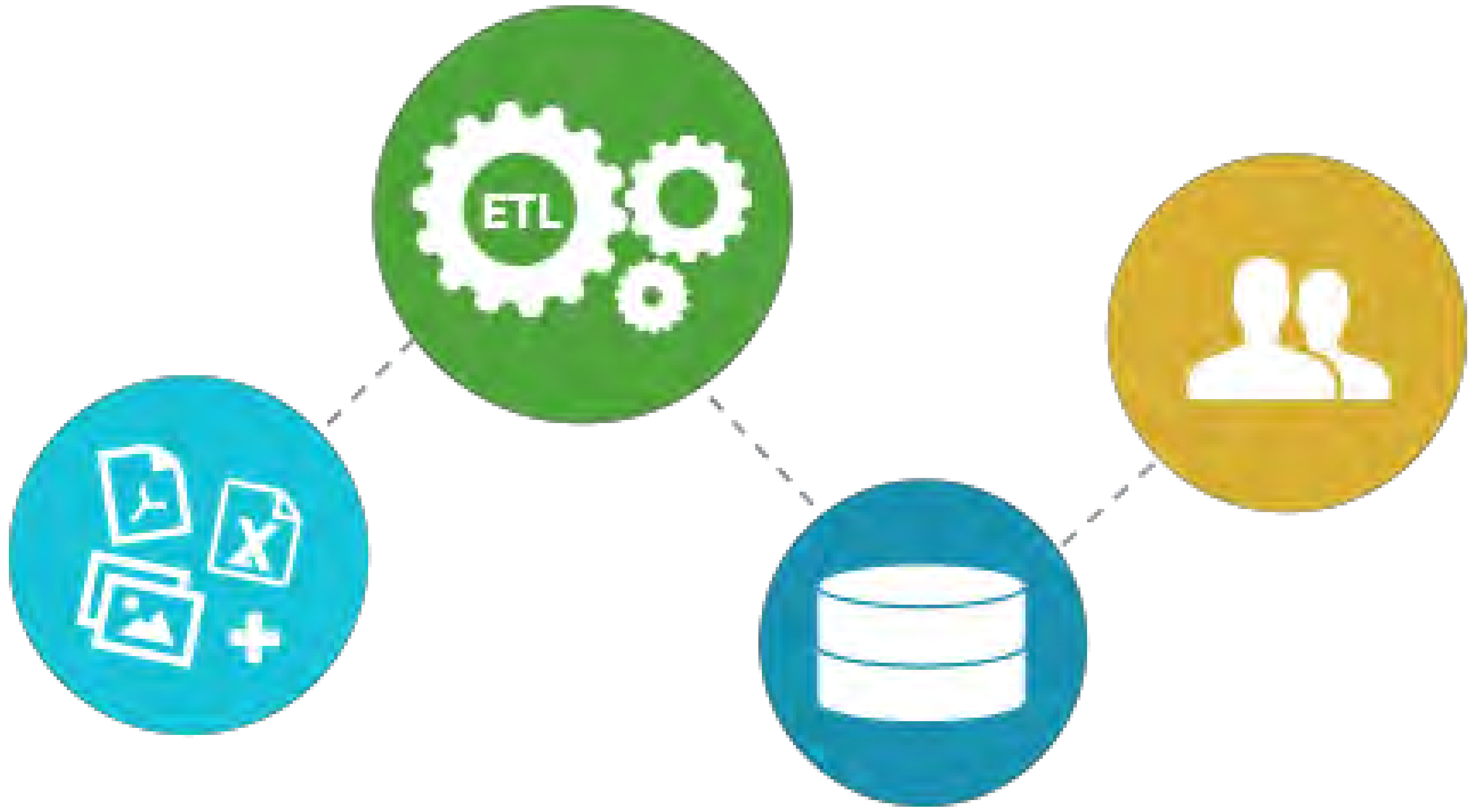
OLAP

- Consolidated data
- Complex data
- Infrequent updates



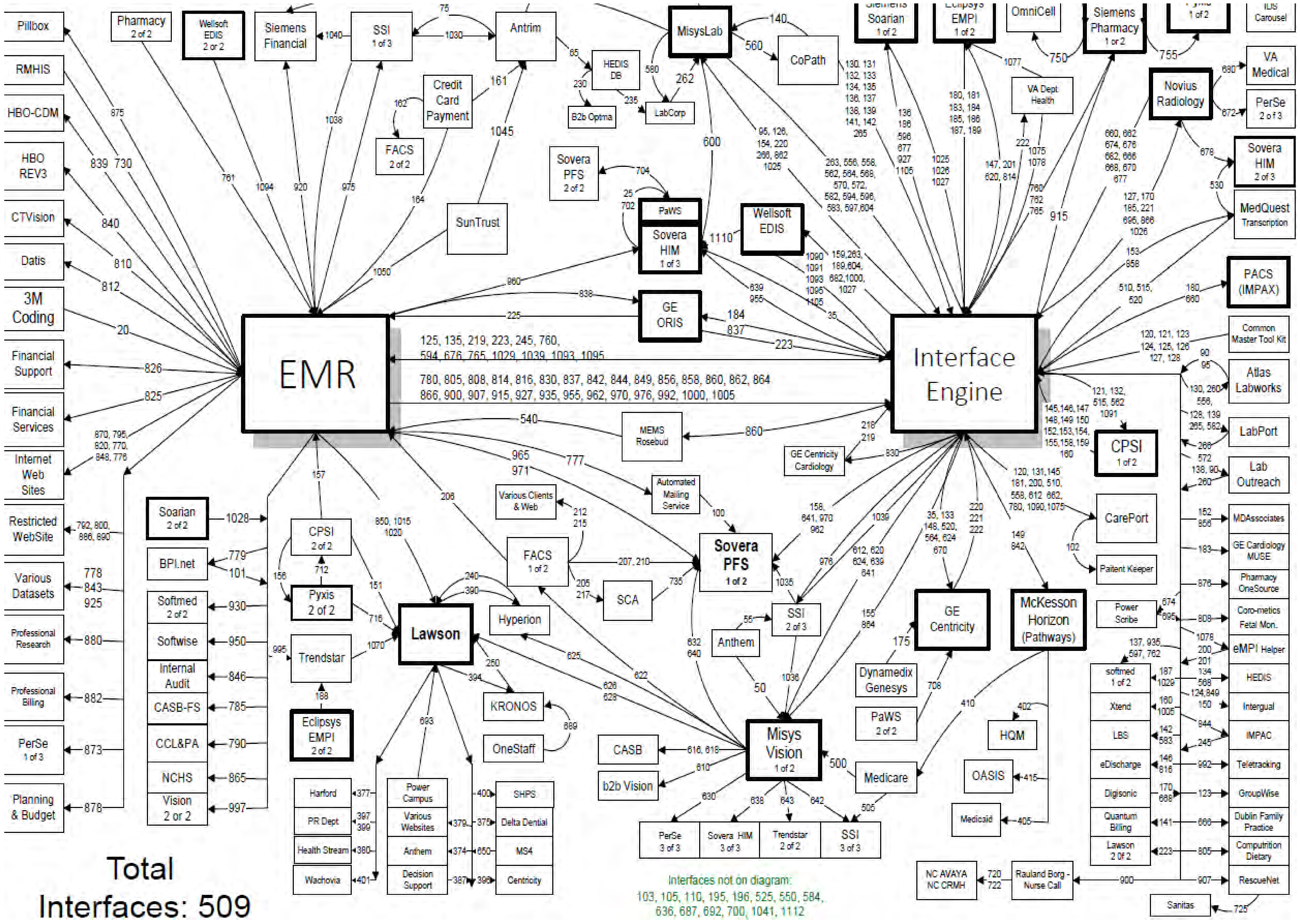
Decision Support System (DSS)

- Go from OLTP sources to single big data warehouse OLAP



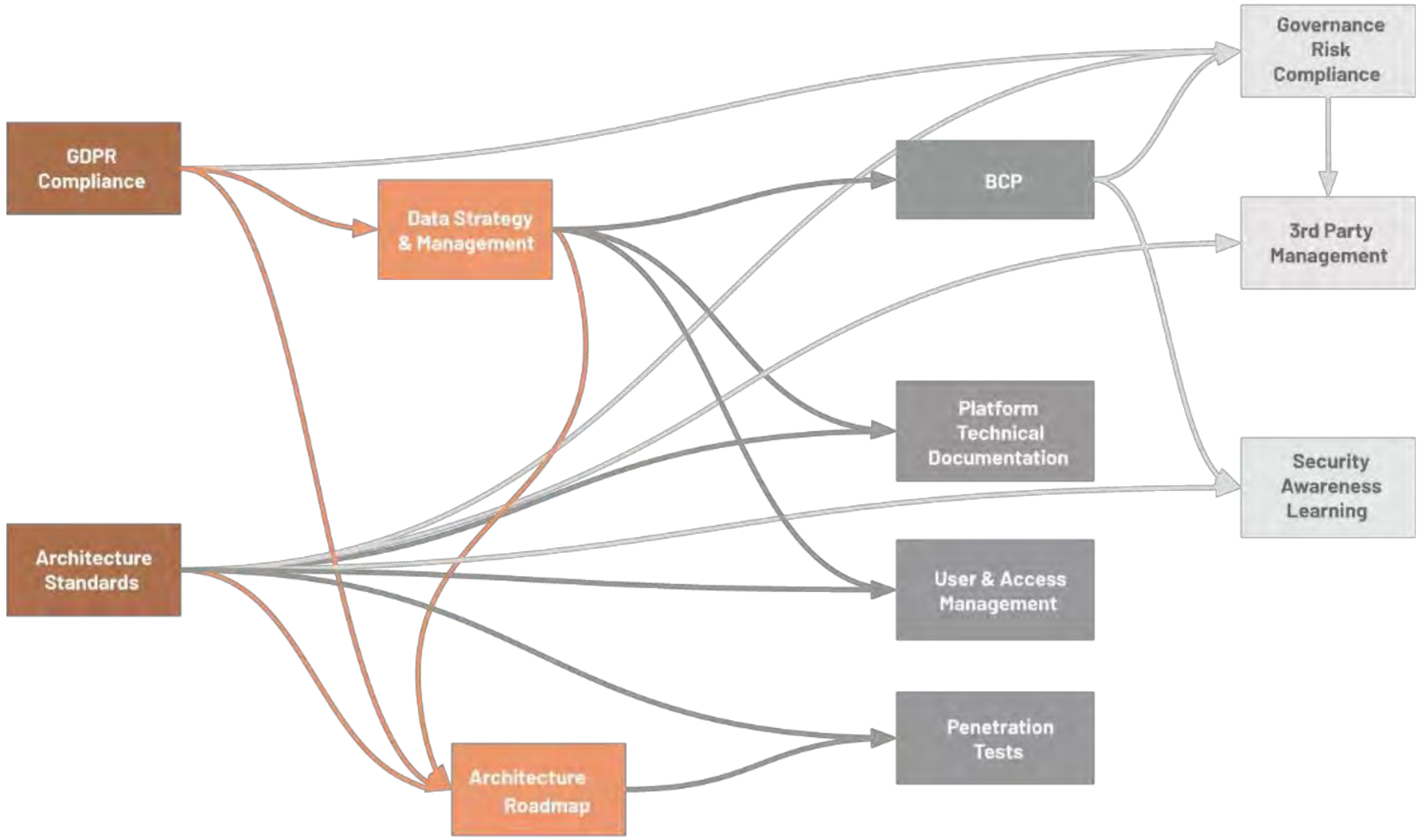
PRIVACY IN PRACTICE

HEALTH DATA



PRIVACY IN PRACTICE

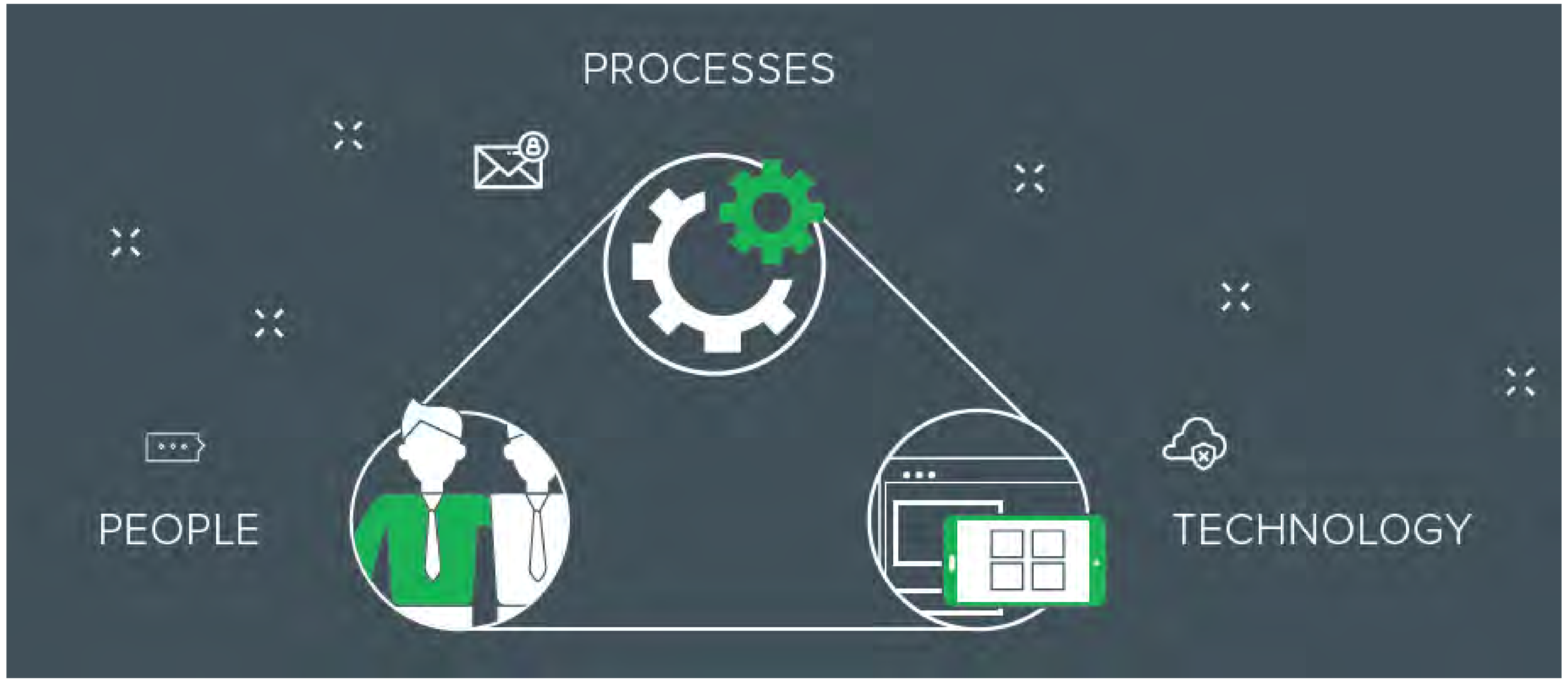
DATA PROTECTION STRATEGY



PRIVACY IN PRACTICE

DATA PROTECTION STRATEGY

PRIVACY BY DESIGN



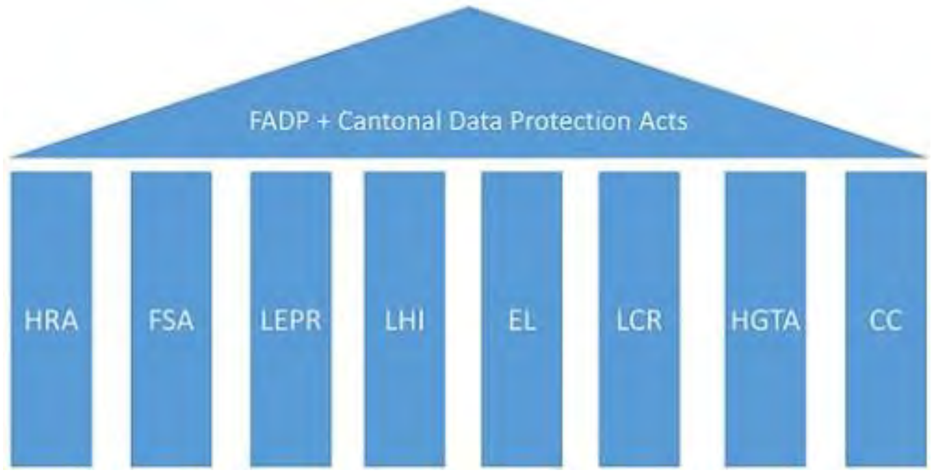
- **Dimension 1 –** Legal Framework
- **Dimension 2 –** Internal Compliance
- **Dimension 3 –** External Compliance

- **Think:**
  - Industry
  - HR
  - IT
  - Surveilance
  - Administration

PRIVACY IN PRACTICE

DATA PROTECTION STRATEGY

LEGAL FRAMEWORK



In Switzerland, for example, **the FADP contains general rules on the processing of personal data by federal bodies (e.g. federal universities) and private persons (e.g. pharmaceutical companies)**, while cantonal data protection regulations set the norms for the processing of data relating to or deriving from cantonal bodies (e.g. cantonal hospitals and cantonal universities).

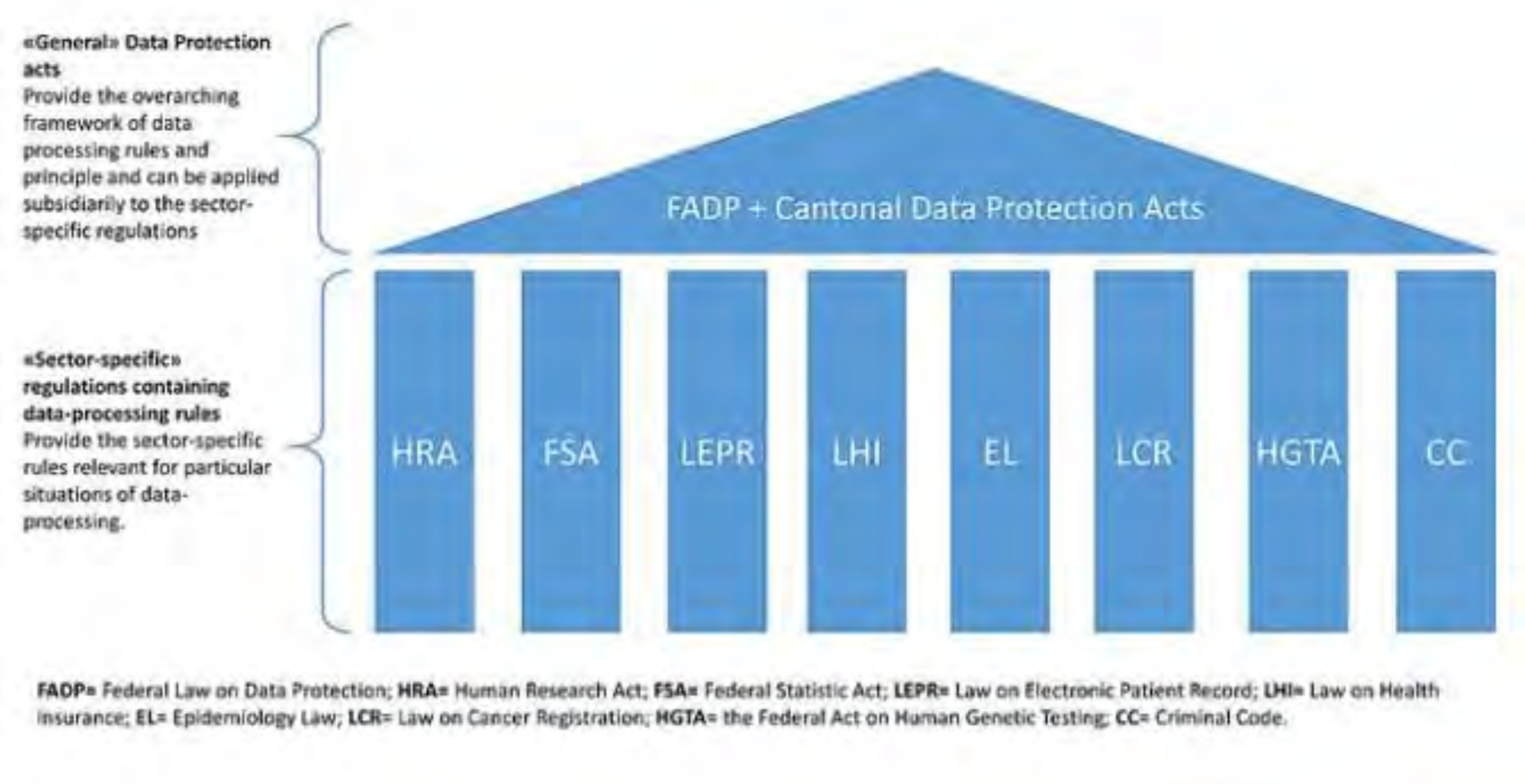
On top of these general regulations, a number of additional data protection rules are scattered across several sectorial legislative acts (fig. 2). The principal ones in the field of interest for this article are the HRA [11], **the law on electronic patient record (LEPR [30]),** the **Law on Health insurance (LHI [31]), the Epidemic Law (EL [32]), the Law on Cancer Registration (LCR [33]), the Federal Statistic Act (FSA [34]) and the Federal Act on Human Genetic Testing (HGTA [35]).**

- The HRA covers the collection and analysis of data in the field of human research.
- The LEPR concerns the “processing of data in the electronic patient record” (art. 1 [30]), which hospitals and nursing homes have the duty to offer [36].
- The LHI contains some data protection rules concerning duties of healthcare providers and healthcare payees to transfer data to federal offices with monitoring (art. 23 and art 59a [31]) or quality control purposes (art 58b and 58c [31]).
- The EL has some sectorial rules applicable to “process personal data, including data concerning health, for the purpose of identifying people who are ill, potentially ill, infected, potentially infected or that expel pathogen elements with respect to public health provisions, in particular to single out and surveil contagious illness and fight against them” (art. 58 [32]).
- The LCR regulates the “collection, recording and analysis of data concerning cancer illnesses” (Art. 1 [33]) for monitoring, prevention, quality development and research purposes (art. 2 [33]).
- The FSA delineates some data protection rules for the processing of data by the Federal Office of Statistics. The HGTA focuses on the regulation of genetic testing for the medical, employment, insurance and liability contexts and it contains some rules on the protection of genetic data.
- Lastly, the processing of data by healthcare professionals and researchers is also covered by the rules on confidentiality in the Criminal Code (art. 321 and art. 321bis Criminal Code [37]).

Martani, A., Egli, P., Widmer, M., &amp; Elger, B. (2020, September 1). Data Protection and biomedical research in Switzerland: Setting the record straight. Swiss Medical Weekly. Retrieved October 21, 2022, from https://smw.ch/article/doi/smw.2020.20332

PRIVACY IN PRACTICE

DATA PROTECTION STRATEGY



«General» Data Protection acts
Provide the overarching framework of data processing rules and principle and can be applied subsidiarily to the sector-specific regulations

«Sector-specific» regulations containing data-processing rules
Provide the sector-specific rules relevant for particular situations of data-processing.

FADP= Federal Law on Data Protection; **HRA=** Human Research Act; **FSA=** Federal Statistic Act; **LEPR=** Law on Electronic Patient Record; **LHI=** Law on Health insurance; **EL=** Epidemiology Law; **LCR=** Law on Cancer Registration; **HGTA=** the Federal Act on Human Genetic Testing; **CC=** Criminal Code.

An overview of parts of the legislative framework concerning data processing in Switzerland. The image does not aim to be exhaustive, but merely indicative of the relationship between different legislative acts concerning data protection and data processing in the healthcare sector.

Martani, A., Egli, P., Widmer, M., &amp; Elger, B. (2020, September 1). Data Protection and biomedical research in Switzerland: Setting the record straight. Swiss Medical Weekly. Retrieved October 21, 2022, from https://smw.ch/article/doi/smw.2020.20332

PRIVACY IN PRACTICE

DATA PROTECTION STRATEGY

Why is Data Protection important in the pharmaceutical industry?

- All pharmaceutical companies hold personal data about individuals.
- The processing of personal data is heavily regulated.

What should you do?

- Establish a lawful basis to undertake such processing.
    - There are general lawful basis, such as:
        - processing activities relate to staff. In this case the processing is necessary for performing the employment contract with that staff member.
    - On the other hand, processing of special categories of data, through research and clinical trials etc., require a separate lawful basis to process this type of data.
- Apply all organizational and technical measures for protecting data and privacy.

PRIVACY IN PRACTICE

DATA PROTECTION STRATEGY

PRIVACY BY DESIGN – RISK BASED APPROACH

DATA PROTECTION OFFICER

RECORDS OF PROCESSING ACTIVITIES

DATA PROTECTION IMPACT ASSESSMENT

RISK-BASED APPROPRIATE SECURITY MEASURES

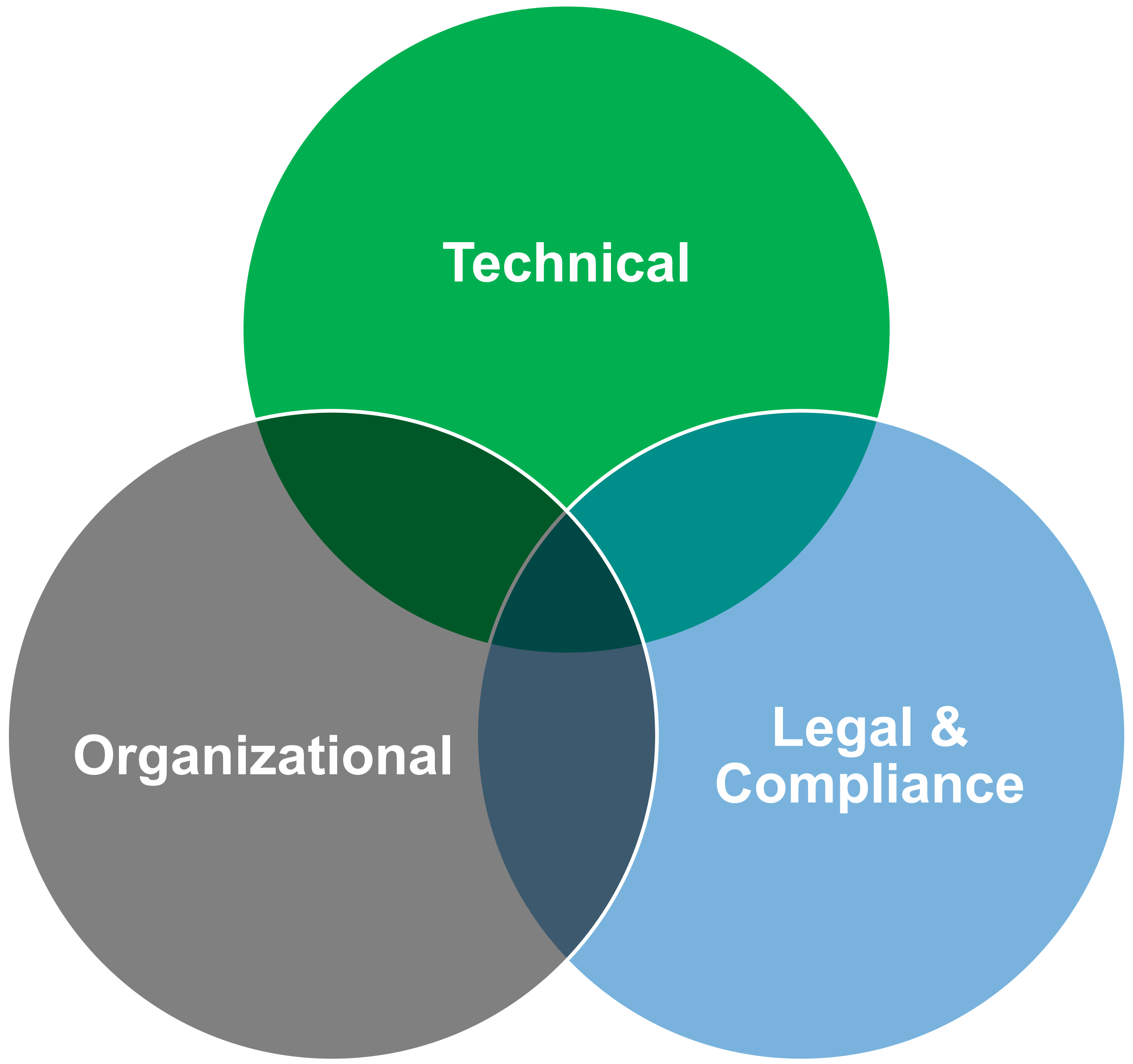
DATA PROTECTION BY DEFAULT AND BY DESIGN

EXPLICIT CONSENT AND LAWFULNESS OF PROCESSING

EXPANDED TERRITORIAL REACH

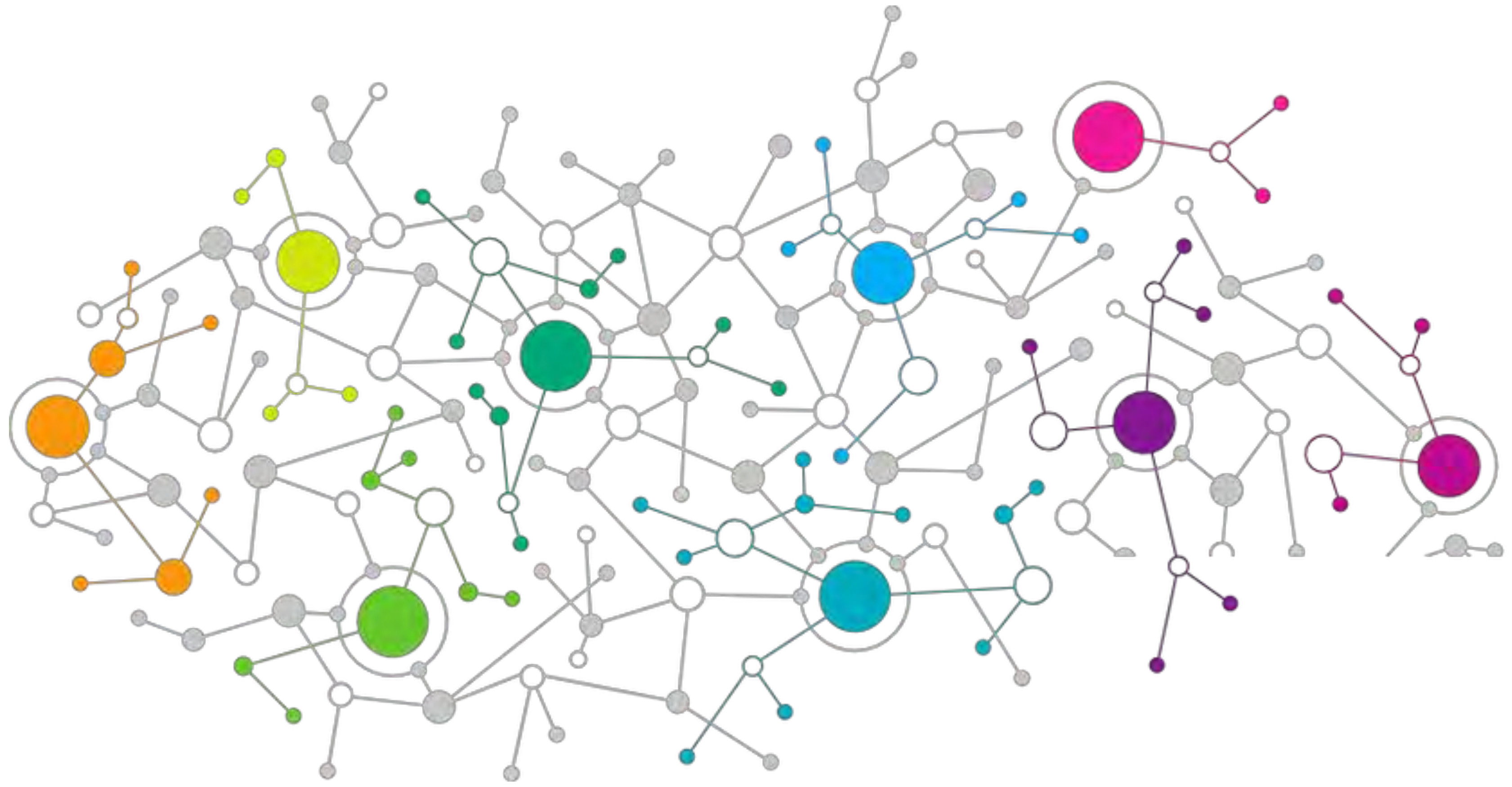
DATA PORTABILITY & RIGHT TO BE FORGOTTEN

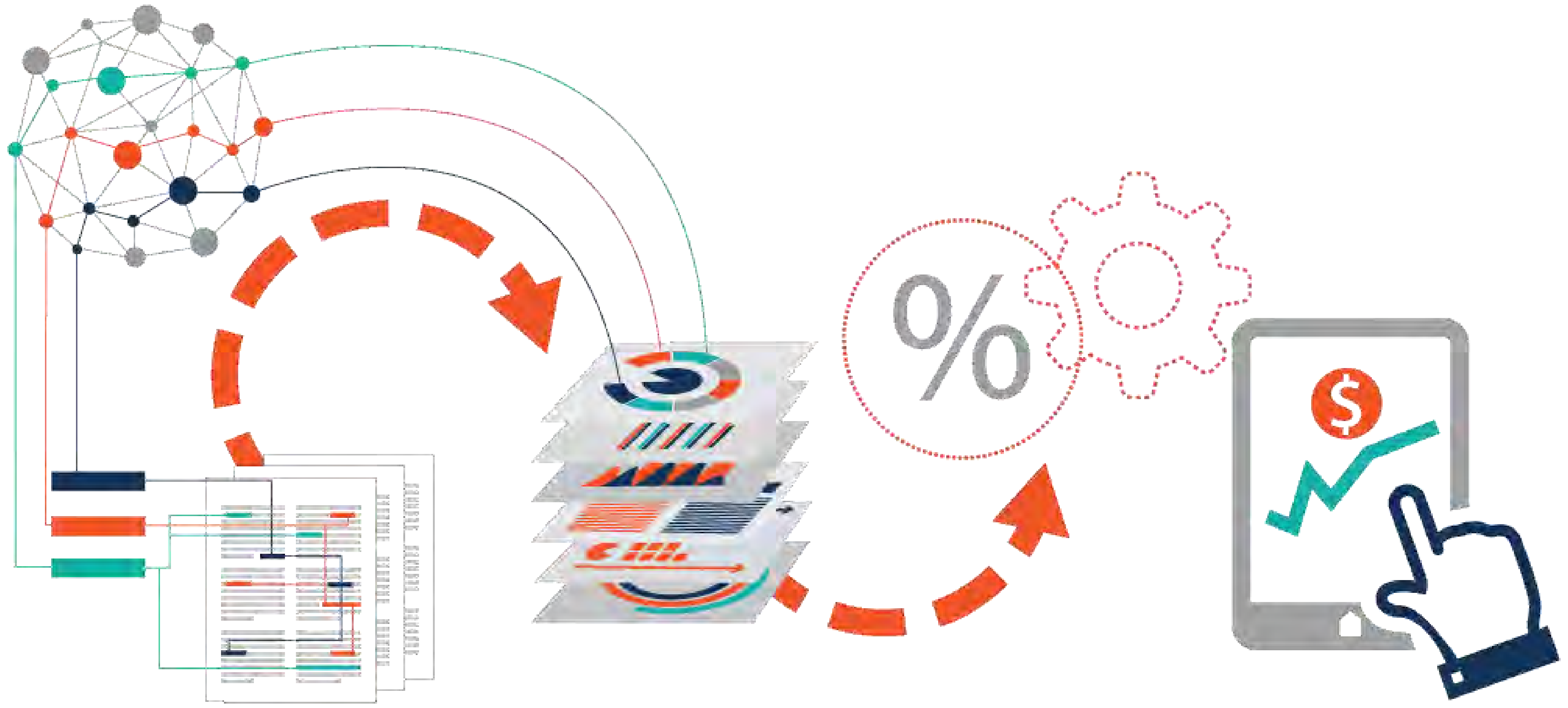
DATA BREACH



PRIVACY IN PRACTICE

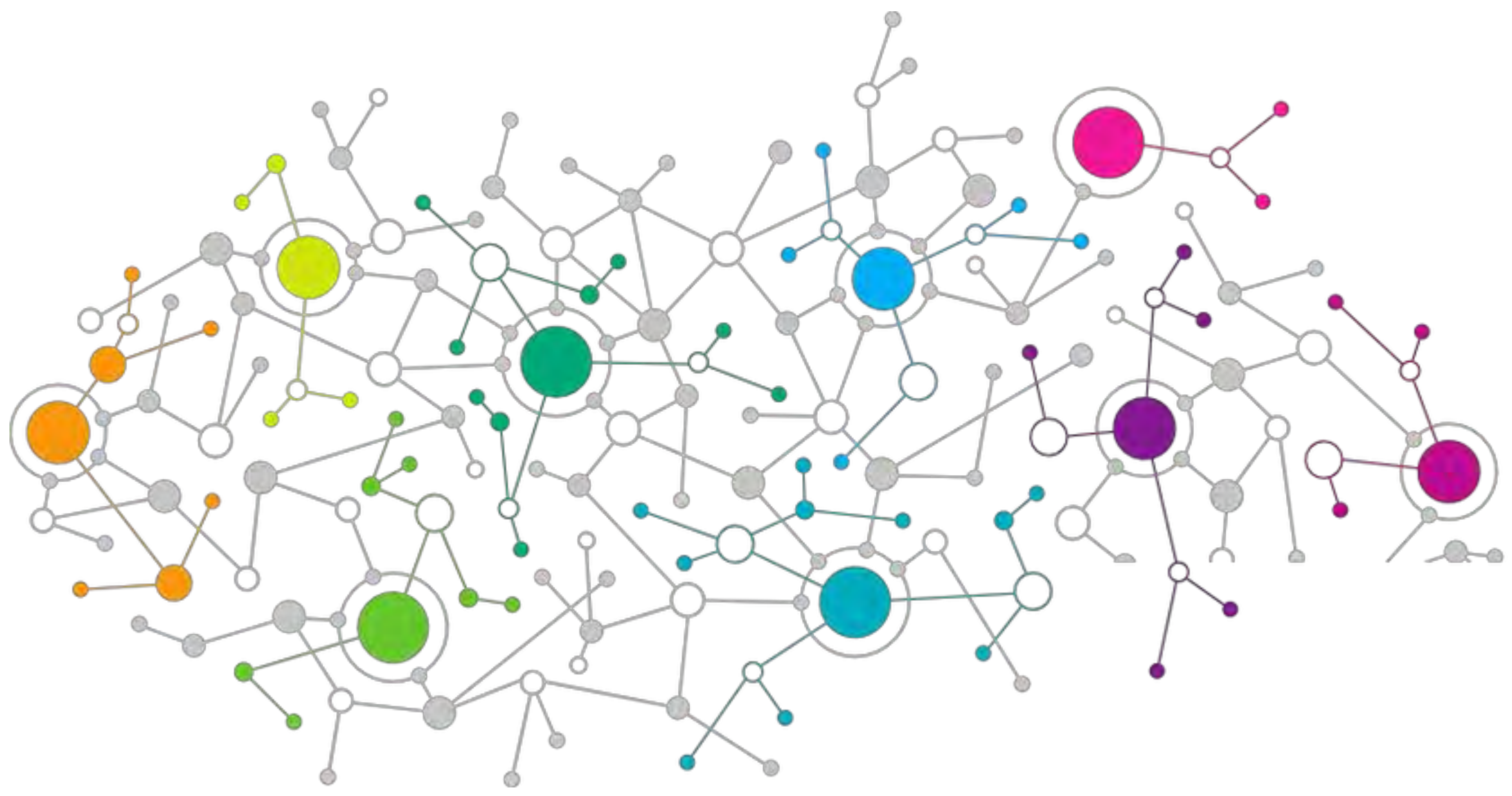
DATA PROTECTION STRATEGY

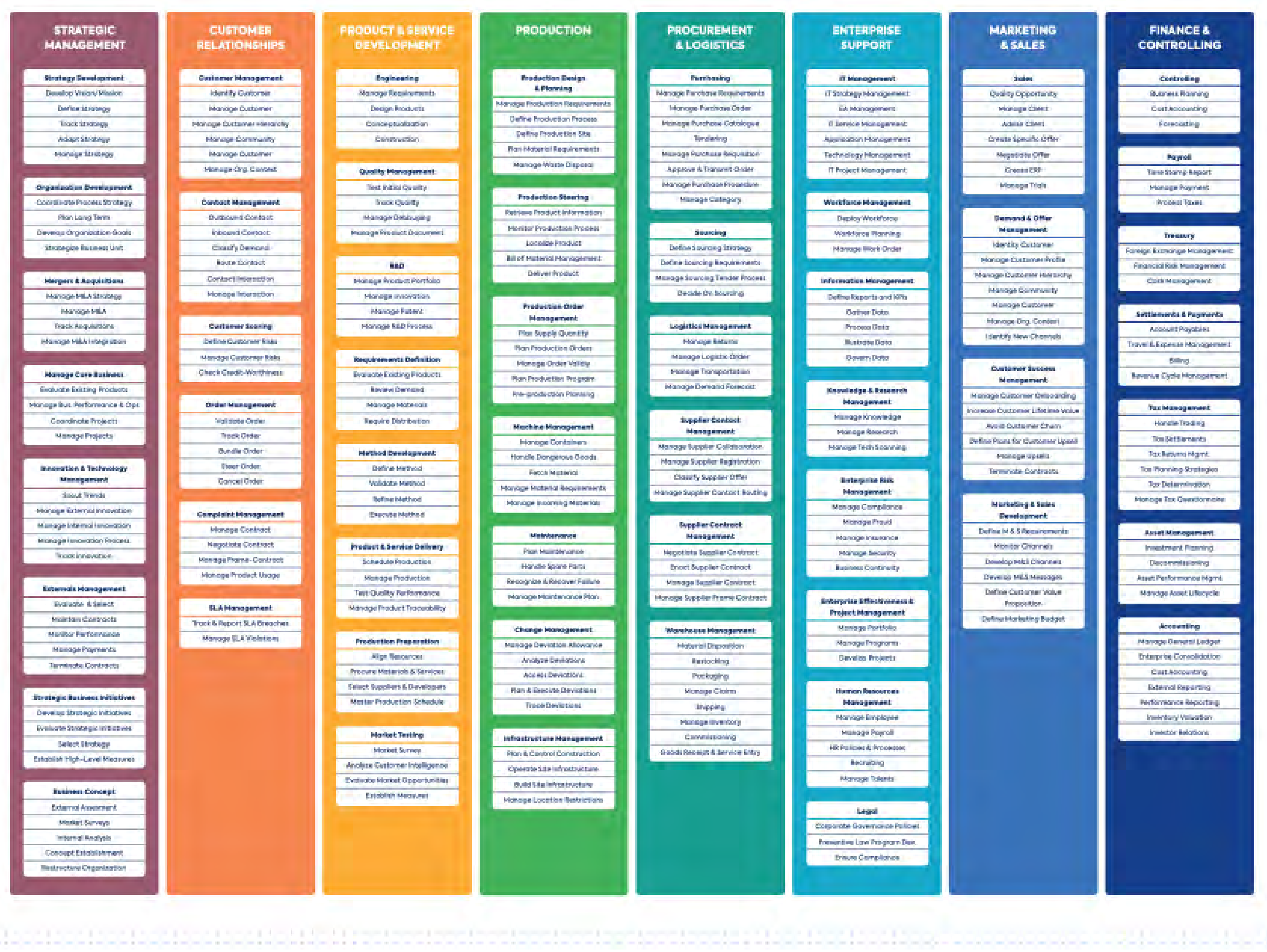


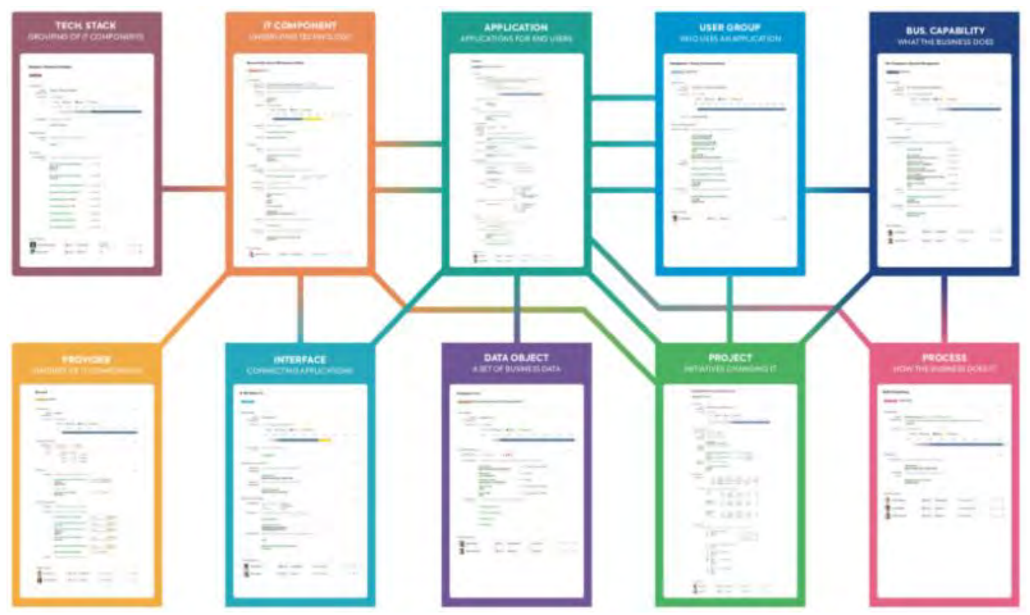


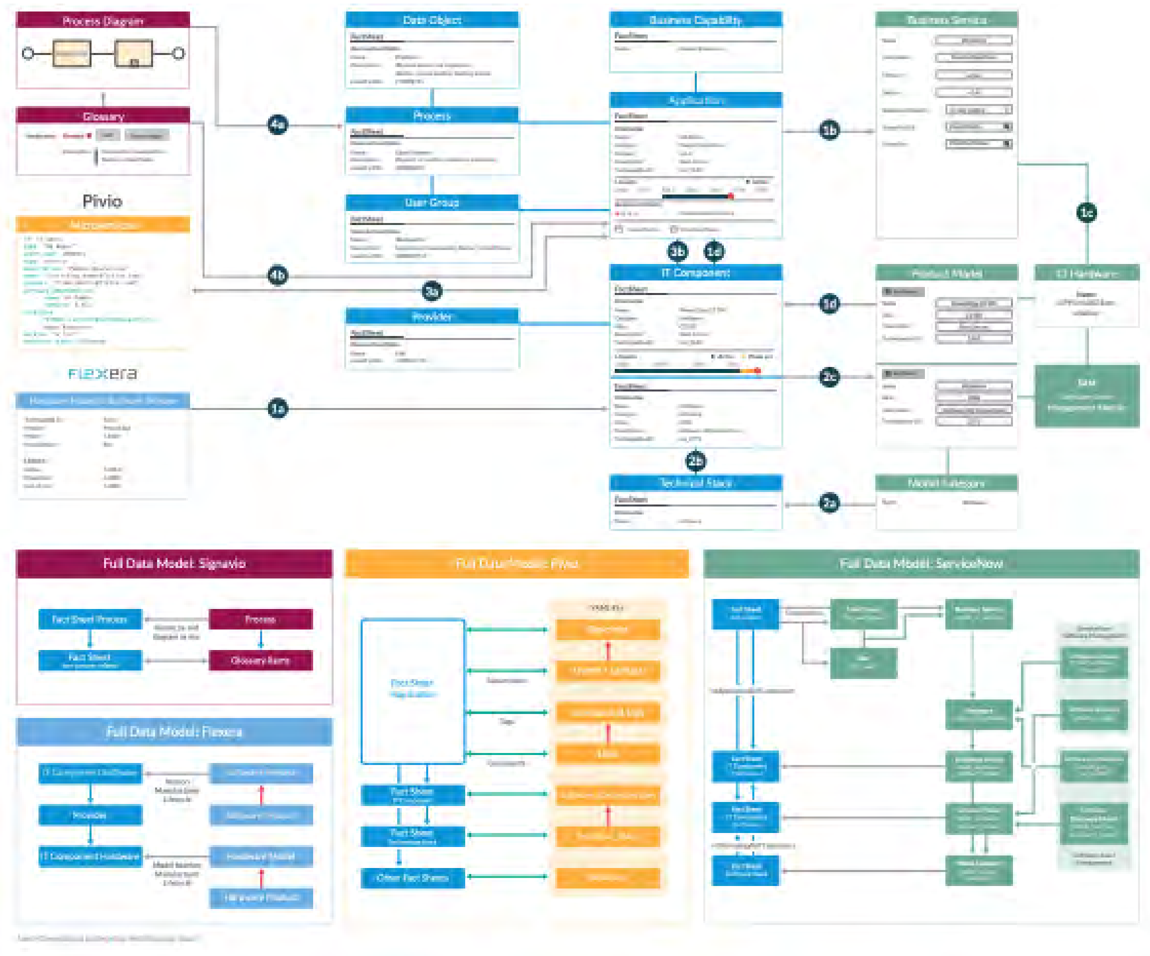
PRIVACY IN PRACTICE

DATA PROTECTION STRATEGY



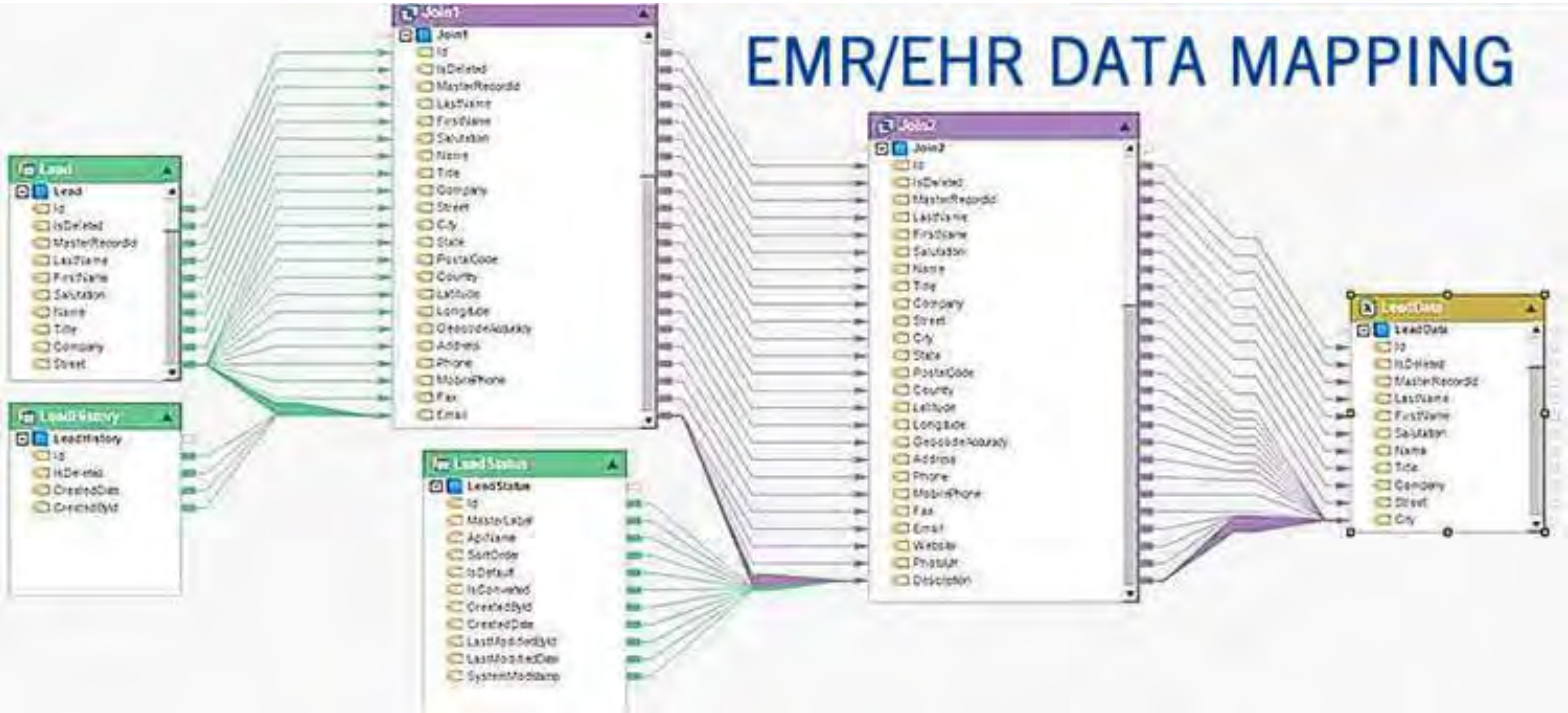






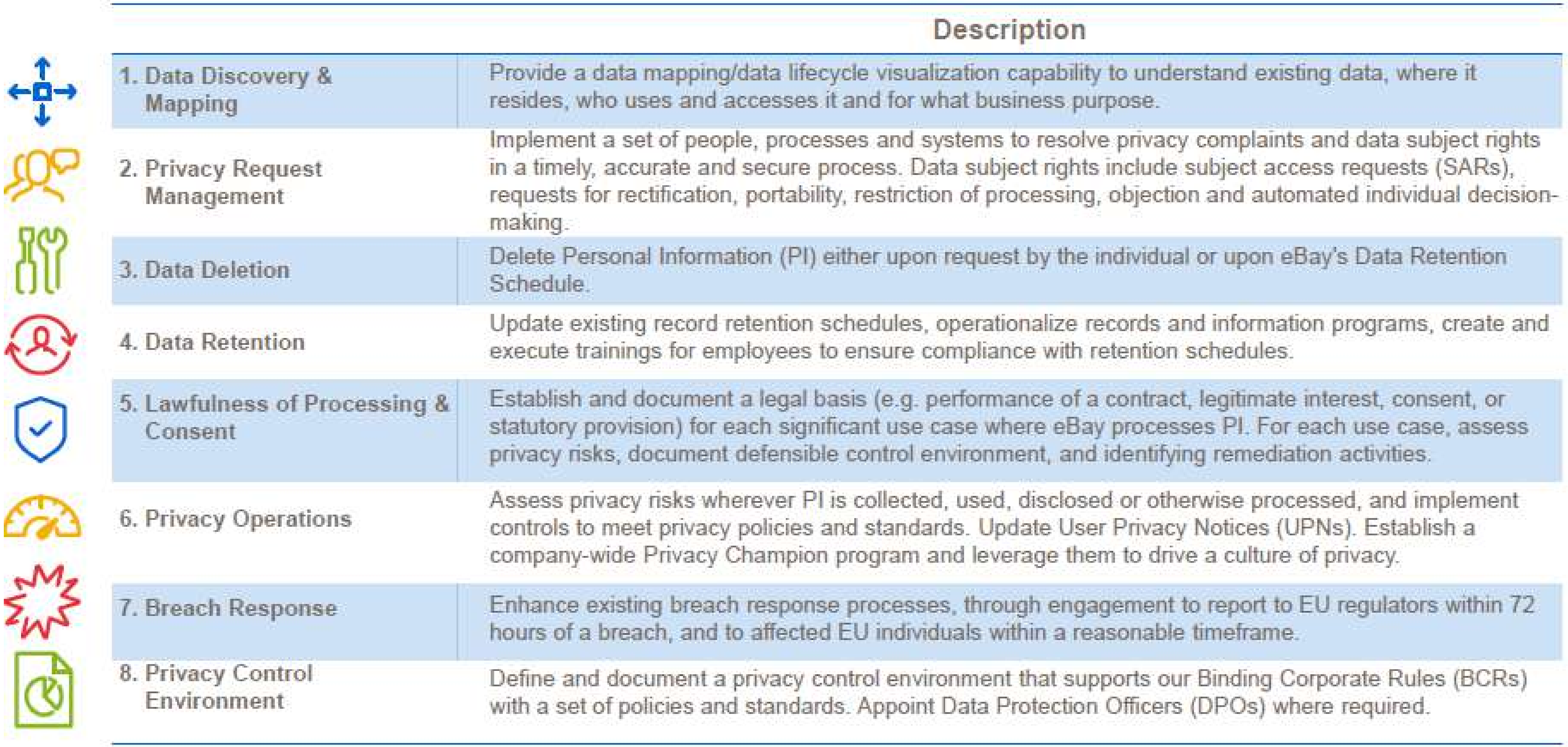
PRIVACY IN PRACTICE

DATA PROTECTION STRATEGY



PRIVACY IN PRACTICE

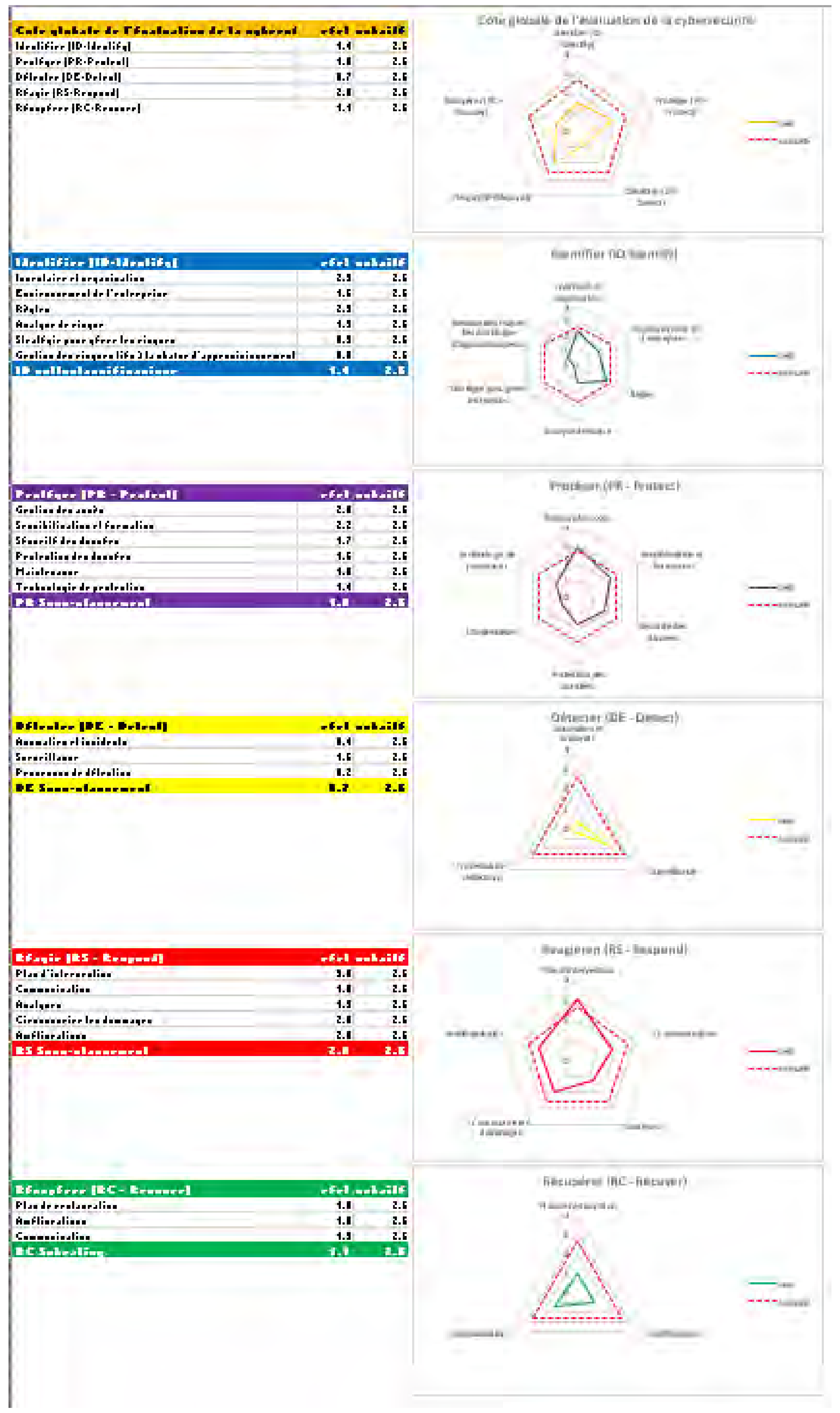
DATA PROTECTION STRATEGY



	Description
1. Data Discovery & Mapping	Provide a data mapping/data lifecycle visualization capability to understand existing data, where it resides, who uses and accesses it and for what business purpose.
2. Privacy Request Management	Implement a set of people, processes and systems to resolve privacy complaints and data subject rights in a timely, accurate and secure process. Data subject rights include subject access requests (SARs), requests for rectification, portability, restriction of processing, objection and automated individual decision-making.
3. Data Deletion	Delete Personal Information (PI) either upon request by the individual or upon eBay's Data Retention Schedule.
4. Data Retention	Update existing record retention schedules, operationalize records and information programs, create and execute trainings for employees to ensure compliance with retention schedules.
5. Lawfulness of Processing & Consent	Establish and document a legal basis (e.g. performance of a contract, legitimate interest, consent, or statutory provision) for each significant use case where eBay processes PI. For each use case, assess privacy risks, document defensible control environment, and identifying remediation activities.
6. Privacy Operations	Assess privacy risks wherever PI is collected, used, disclosed or otherwise processed, and implement controls to meet privacy policies and standards. Update User Privacy Notices (UPNs). Establish a company-wide Privacy Champion program and leverage them to drive a culture of privacy.
7. Breach Response	Enhance existing breach response processes, through engagement to report to EU regulators within 72 hours of a breach, and to affected EU individuals within a reasonable timeframe.
8. Privacy Control Environment	Define and document a privacy control environment that supports our Binding Corporate Rules (BCRs) with a set of policies and standards. Appoint Data Protection Officers (DPOs) where required.

PRIVACY IN PRACTICE

DATA PROTECTION STRATEGY



Cote globale de l'évaluation de la cybersécurité	état	souhaité
Identifier (ID-Identify)	1.4	2.5
Protéger (PR-Protect)	1.8	2.5
Détecter (DE-Detect)	0.7	2.5
Réagir (RS-Respond)	2.0	2.5
Récupérer (RC-Recover)	1.1	2.5

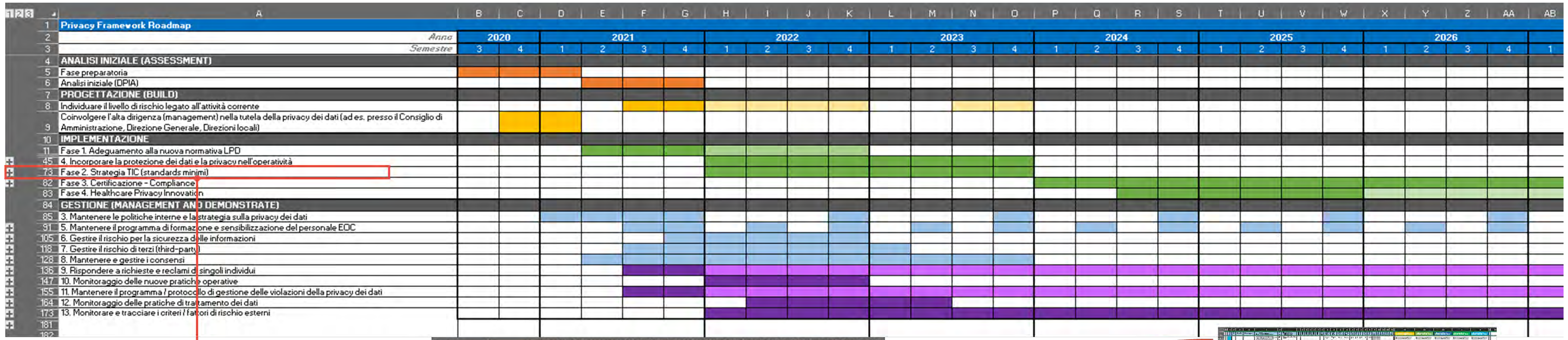
Identifier (ID-Identify)	état	souhaité
Inventaire et organisation	2.3	2.5
Environnement de l'entreprise	1.5	2.5
Règles	2.3	2.5
Analyse de risque	1.3	2.5
Stratégie pour gérer les risques	0.3	2.5
Gestion des risques liés à la chaîne d'approvisionnement	0.0	2.5
ID Sous-classement	1.4	2.5

Protéger (PR - Protect)	état	souhaité
Gestion des accès	2.0	2.5
Sensibilisation et formation	2.2	2.5
Sécurité des données	1.7	2.5
Protection des données	1.6	2.5
Maintenance	1.0	2.5
Technologie de protection	1.4	2.5
PR Sous-classement	1.8	2.5

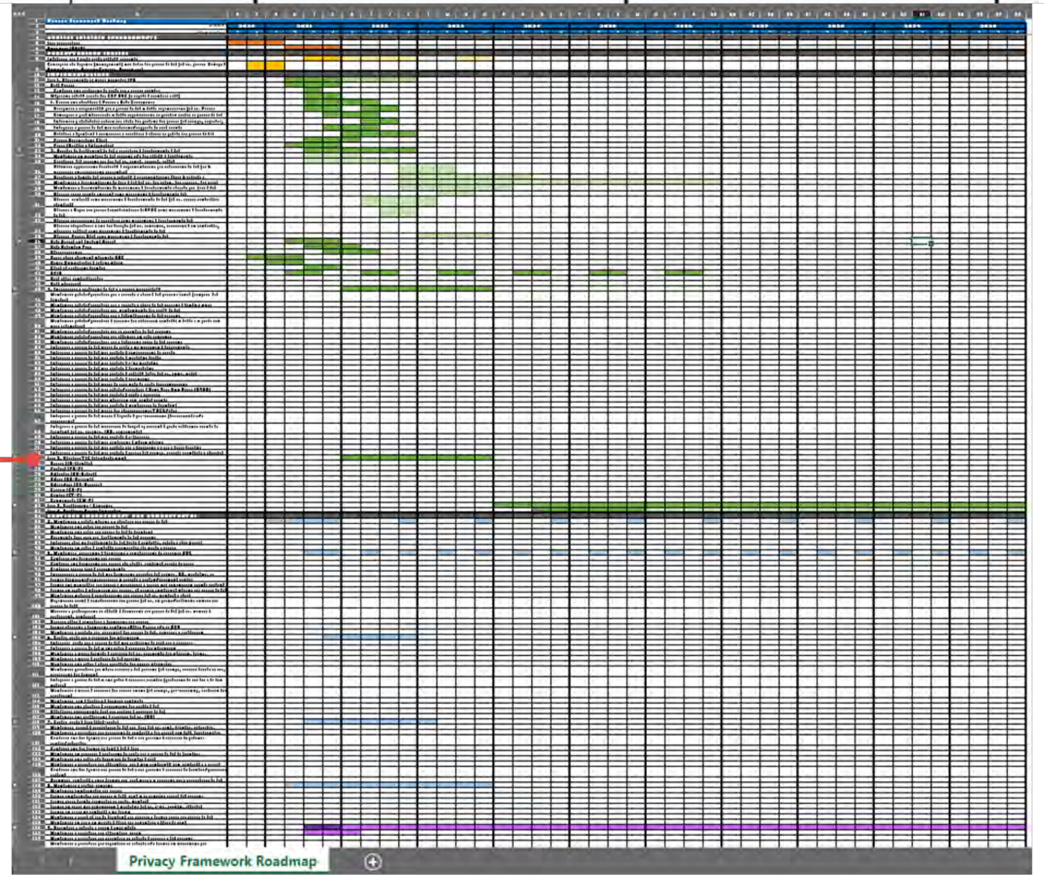
Détecter (DE - Detect)	état	souhaité
Anomalies et incidents	0.4	2.5
Surveillance	1.6	2.5
Processus de détection	0.2	2.5
DE Sous-classement	0.7	2.5

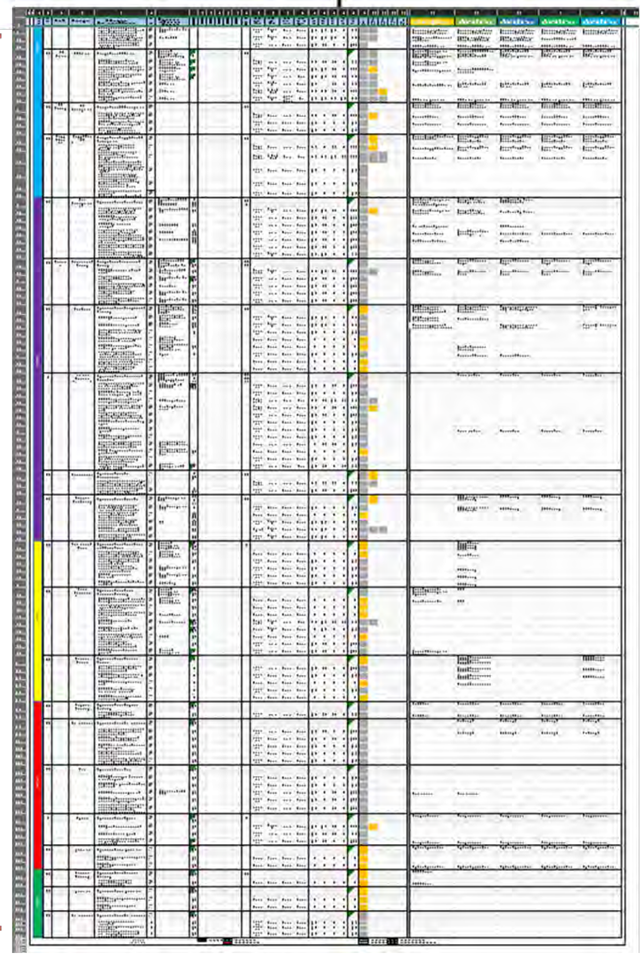
Réagir (RS - Respond)	état	souhaité
Plan d'intervention	3.0	2.5
Communication	1.0	2.5
Analyses	1.5	2.5
Circonscrire les dommages	2.0	2.5
Améliorations	2.0	2.5
RS Sous-classement	2.0	2.5

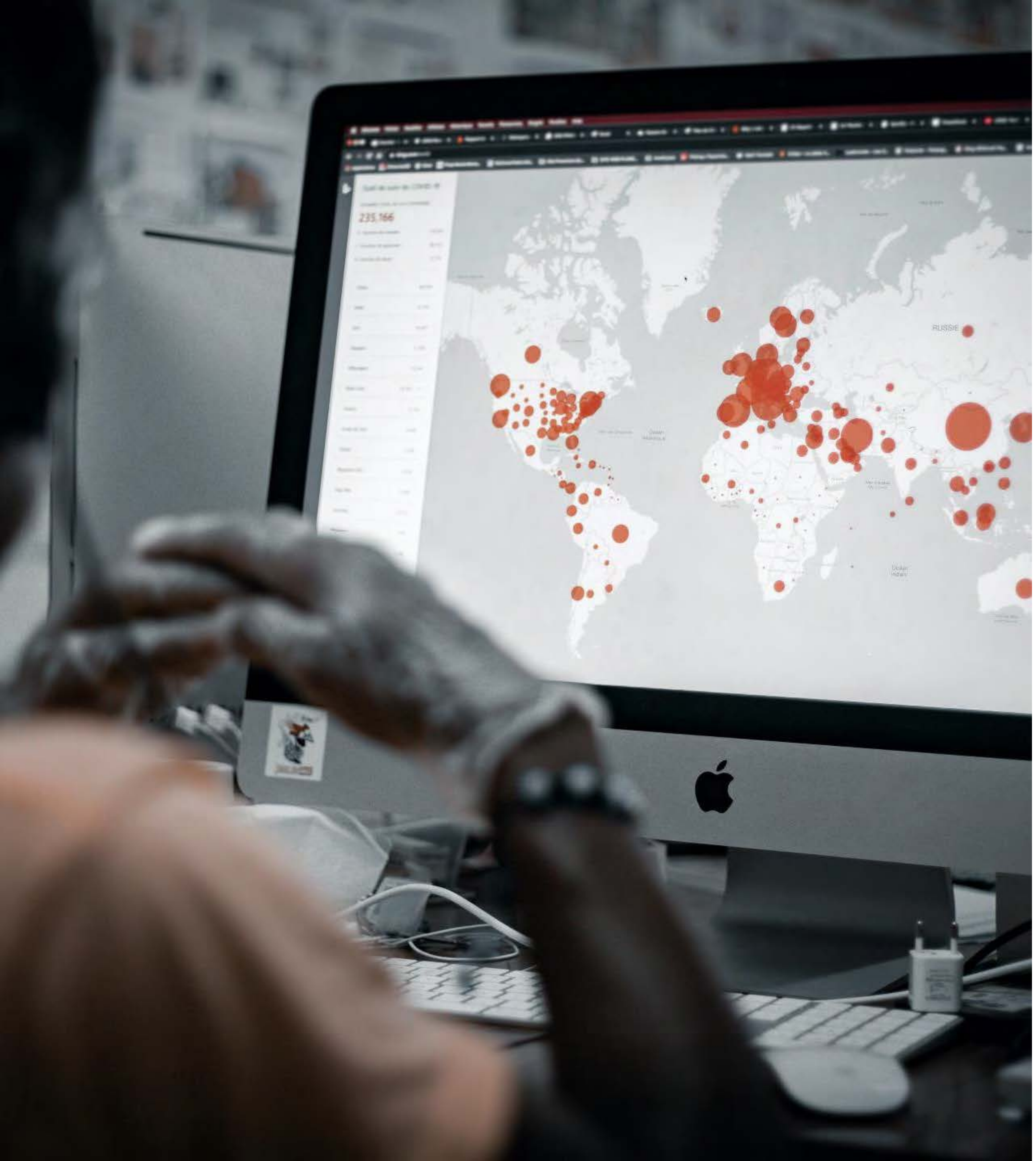
Récupérer (RC - Recover)	état	souhaité
Plan de restauration	1.0	2.5
Améliorations	1.0	2.5
Communication	1.3	2.5
RC Sous-classement	1.1	2.5



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB
1	Privacy Framework Roadmap																											
2	*Anno*	2020		2021				2022				2023				2024				2025				2026				
3	*Semestre*	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1
4	ANALISI INIZIALE (ASSESSMENT)																											
5	Fase preparatoria																											
6	Analisi iniziale (DPIA)																											
7	PROGETTAZIONE (BUILD)																											
8	Individuare il livello di rischio legato all'attività corrente																											
9	Coinvolgere l'alta dirigenza (management) nella tutela della privacy dei dati (ad es. presso il Consiglio di Amministrazione, Direzione Generale, Direzioni locali)																											
10	IMPLEMENTAZIONE																											
11	Fase 1. Adeguamento alla nuova normativa LPD																											
45	4. Incorporare la protezione dei dati e la privacy nell'operatività																											
73	Fase 2. Strategia TIC (standards minimi)																											
82	Fase 3. Certificazione - Compliance																											
83	Fase 4. Healthcare Privacy Innovation																											
84	GESTIONE (MANAGEMENT AND DEMONSTRATE)																											
85	3. Mantenere le politiche interne e la strategia sulla privacy dei dati																											
91	5. Mantenere il programma di formazione e sensibilizzazione del personale EOC																											
105	6. Gestire il rischio per la sicurezza delle informazioni																											
118	7. Gestire il rischio di terzi (third-party)																											
128	8. Mantenere e gestire i consensi																											
136	9. Rispondere a richieste e reclami di singoli individui																											
147	10. Monitoraggio delle nuove pratiche operative																											
155	11. Mantenere il programma / protocollo di gestione delle violazioni della privacy dei dati																											
164	12. Monitoraggio delle pratiche di trattamento dei dati																											
173	13. Monitorare e tracciare i criteri / fattori di rischio esterni																											
181																												
182																												





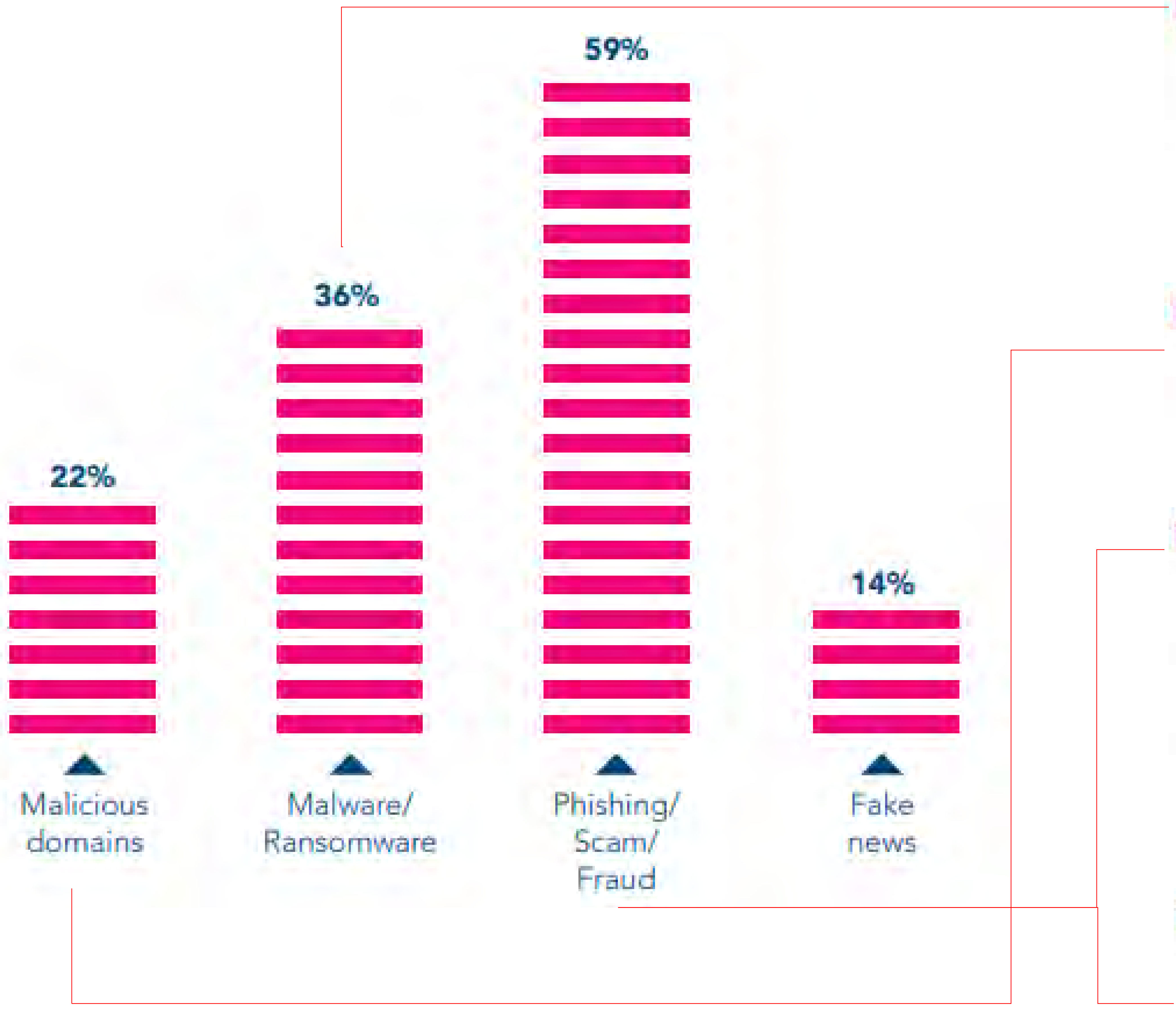


PRIVACY IN PRACTICE

PANDEMIC

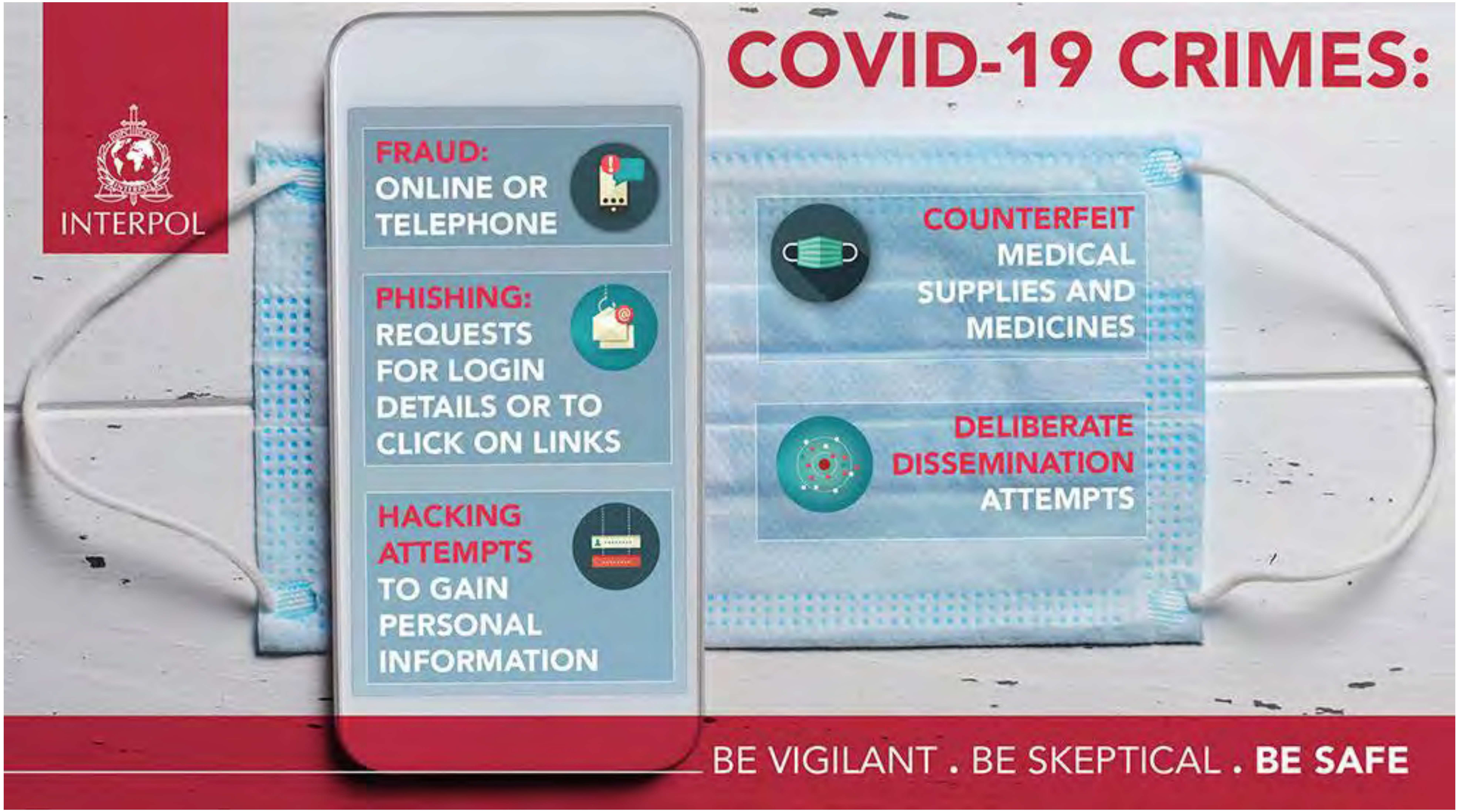
The COVID-19 Pandemic highlighted the 'gaps' and accelerated the need for synergy between privacy and public health interests.

STAY SAFE – PRIVACY IS A HUMAN RIGHT



- Cybercriminals are taking advantage of the pandemic to deploy ransomware against critical infrastructure and healthcare institutions responsible for COVID-19 response.
- Cloning of official government websites is increasingly occurring to steal sensitive user data, which can later be used in further cyberattacks.
- Social media is increasingly used by criminals for online child sexual exploitation. Specifically, offenders within online child abuse networks are locating and contacting their victims on social media taking advantage of the global lockdown. At the same time, the trade in child sexual exploitation images has intensified.
- As many companies in the Americas implemented teleworking, cybercriminals are increasingly targeting employees in order to gain control through remote access to corporate networks with a view to stealing sensitive information.

STAY SAFE – PRIVACY IS A HUMAN RIGHT



INTERPOL

COVID-19 CRIMES:

FRAUD: ONLINE OR TELEPHONE

PHISHING: REQUESTS FOR LOGIN DETAILS OR TO CLICK ON LINKS

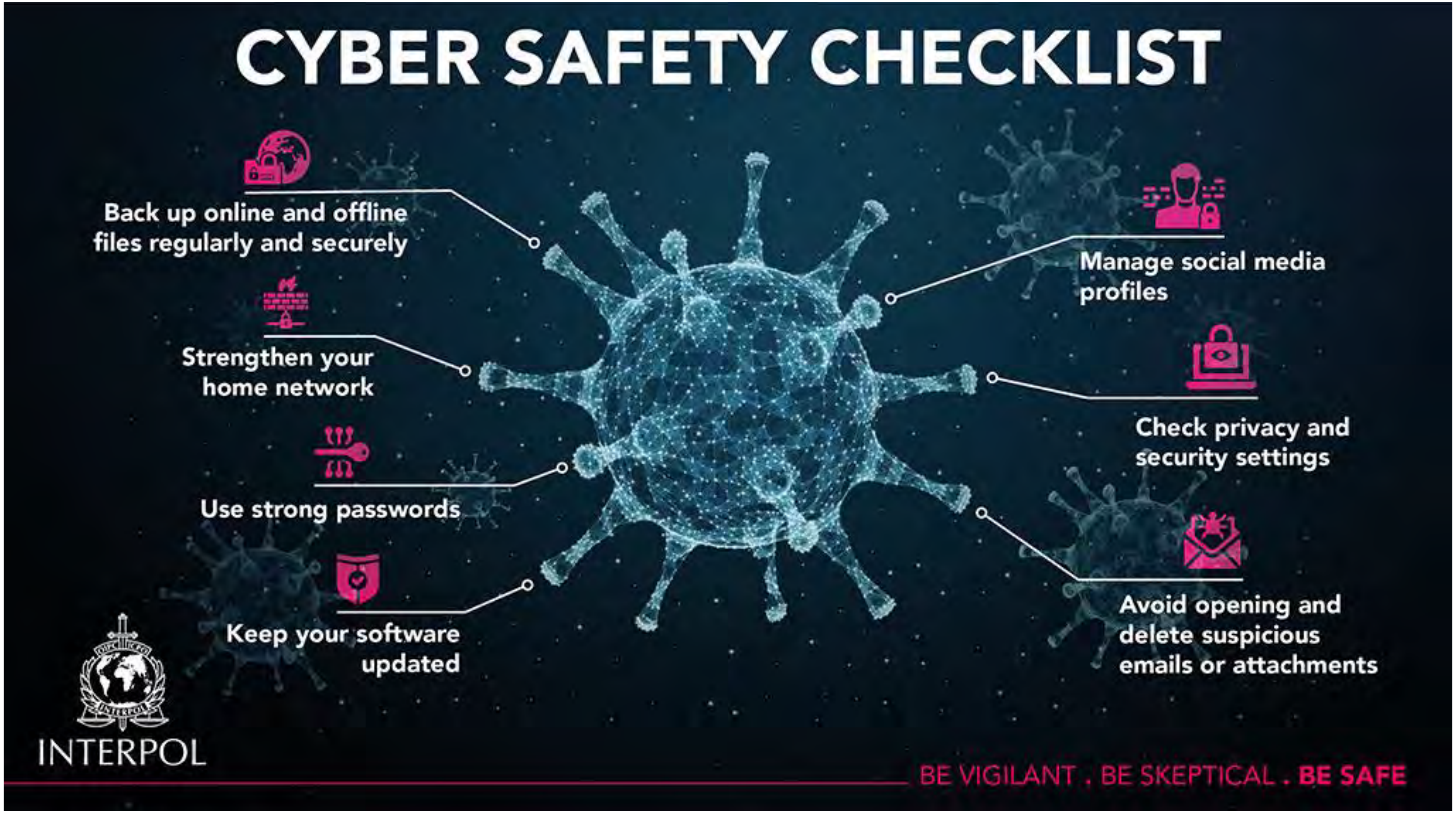
HACKING ATTEMPTS TO GAIN PERSONAL INFORMATION

COUNTERFEIT MEDICAL SUPPLIES AND MEDICINES

DELIBERATE DISSEMINATION ATTEMPTS

BE VIGILANT . BE SKEPTICAL . **BE SAFE**

STAY SAFE – PRIVACY IS A HUMAN RIGHT



CYBER SAFETY CHECKLIST

- Back up online and offline files regularly and securely
- Strengthen your home network
- Use strong passwords
- Keep your software updated
- Manage social media profiles
- Check privacy and security settings
- Avoid opening and delete suspicious emails or attachments

INTERPOL

BE VIGILANT . BE SKEPTICAL . **BE SAFE**

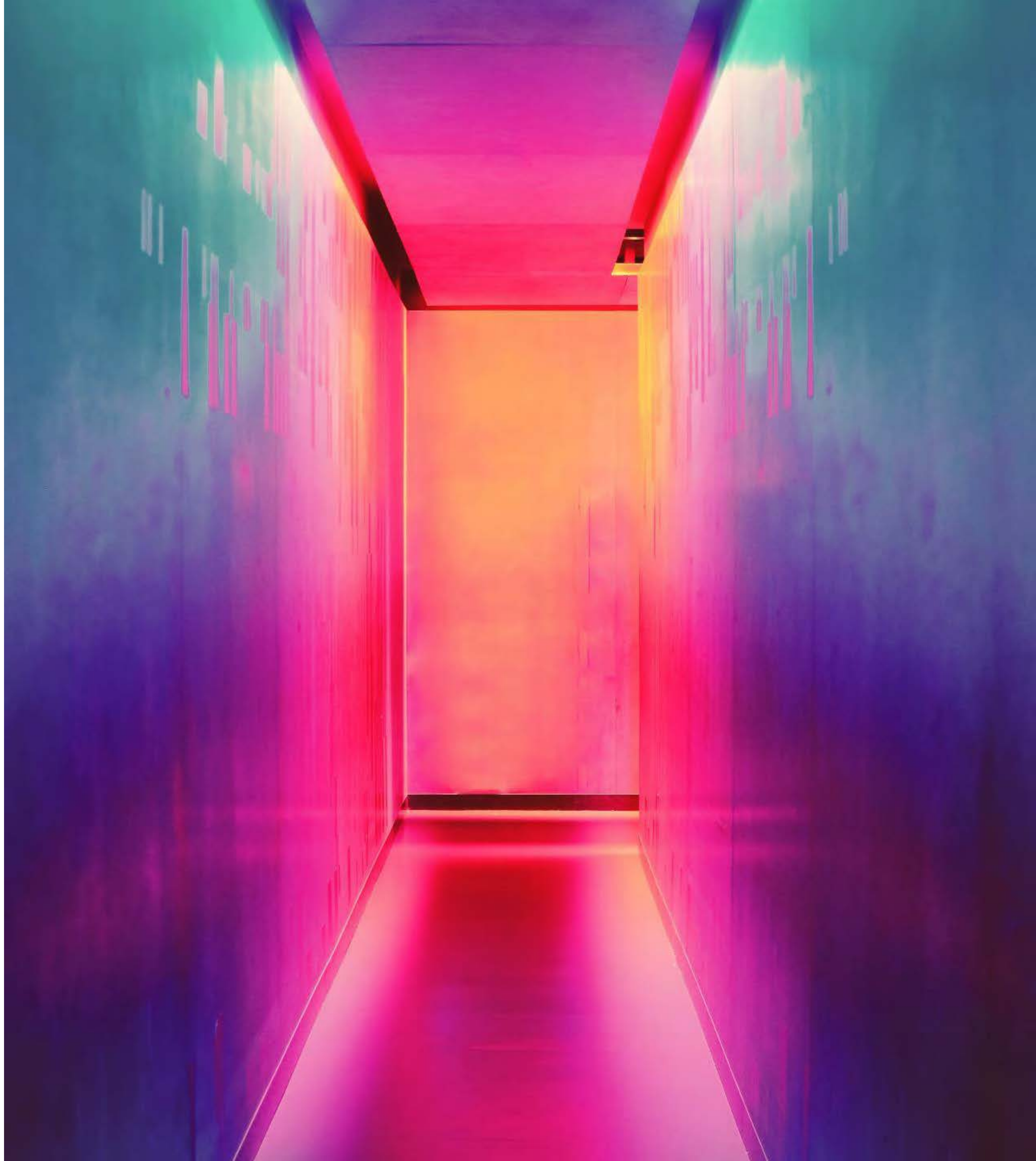
THE FUTURE OF PRIVACY

INTERNET OF BODIES (IoB)

Technological innovation, in particular wearables and integrated devices, are transforming the human body into a new technological platform - into what is now called the 'Internet of Bodies (IoB)'.

IoB devices track, record and store things like users' movements, bodily functions and what they see, hear or even think. Determining who can access, collect or interact with this type of personal and health data is a key consideration with any IoB device.

From a security point of view, the risk is also very hig. Particularly in the case of embedded medical devices, manipulation or blocking from the account could result in serious physical harm and even death.



In this world we do not see things as they are. We see them as we are, because what we see depends mainly on what we are looking for.

John Lubbock

THANK YOU!

BAROUM MRAD
DPO-HSG, MBA, LLM

✉ mrad.baroum@gmail.com

🌐 linkedin.com/in/baroum-mrad

📷 @barumgeorgis