GRC & DATA

TWO SIDES OF THE SAME COIN

GRC Be Connected

Cyber Security Coalition

28/03/2024

* Le monde est tel que nous le façonnons.

The world is how we shape it*

sopra steria | ORDINA a Sopra Steria company | TOBANIA a Sopra Steria company

Sopra Steria CyberSecurity

In the Top 15

European cybersecurity services companies

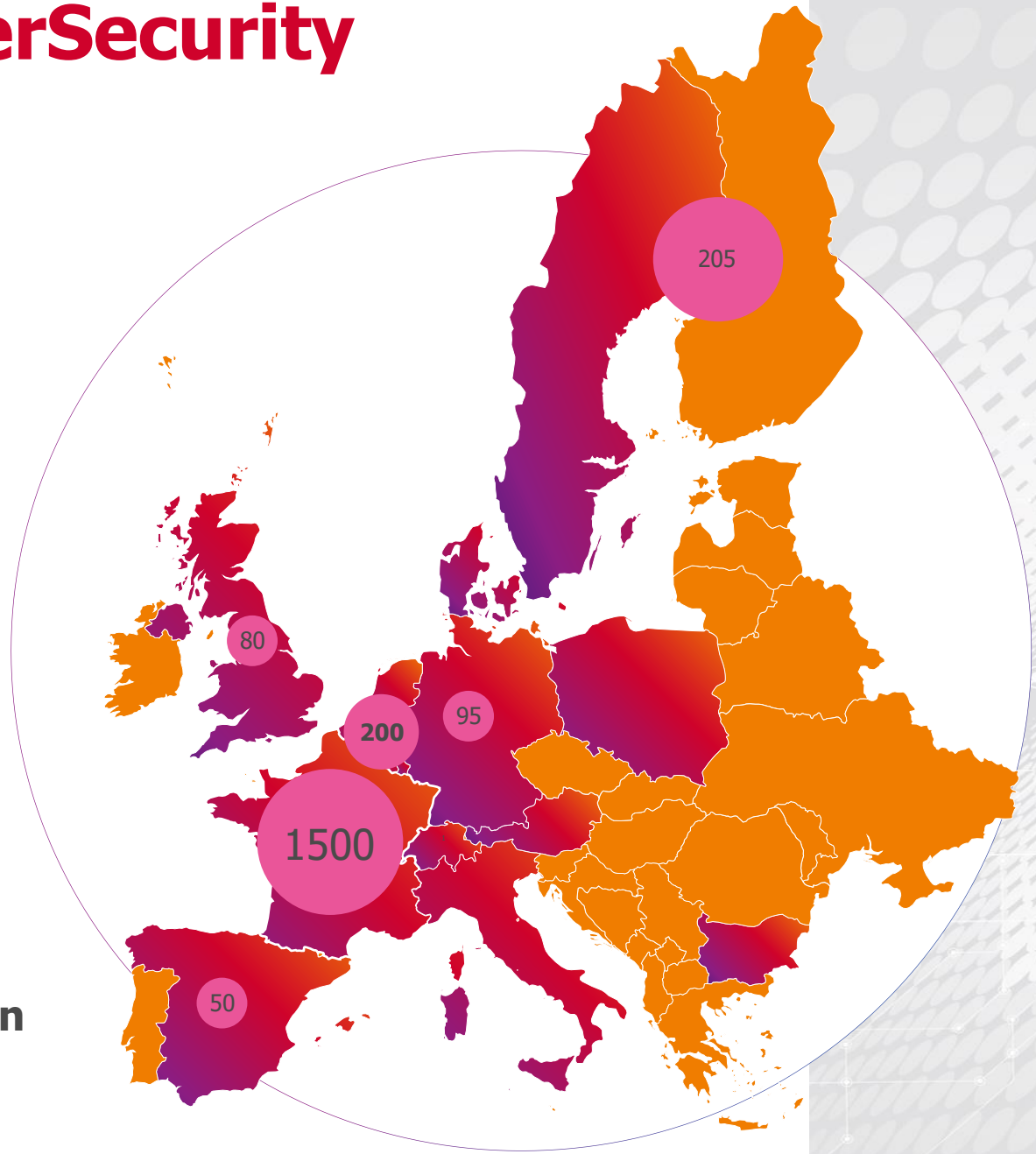
2400

Cyber specialists

~9

Countries

- **A seamless Delivery model**
- **Flexible & Evolutive**
- **Proximity & Industrialisation**



CAPTECH Cyber

PASSI

PDIS

DCS CAT

sopra steria

DATA IS THE NEW OIL

DATA IS THE LIFEBLOOD OF ORGANIZATIONS

DATA ASSET
AT THE CORE OF GRC

sopra steria

Data, an uncontrolled asset

Risk and cost rising situation within organizations

20%

Annual data volume growth, both structured and unstructured.

2.2 Billion

Records exposed to data breach in 2022. Growing tendency in 2023

33%

Data considered as redundant, obsolete or trivial.

Chaotic situation generating

Costs

- Infrastructure
- Operational
- Sustainability impact

Risks

- Financial fines for non-compliance
- Company reputation
- Top management questioned
- Operational blockage
- Employee frustration impacting retention

New legal constraints and challenges

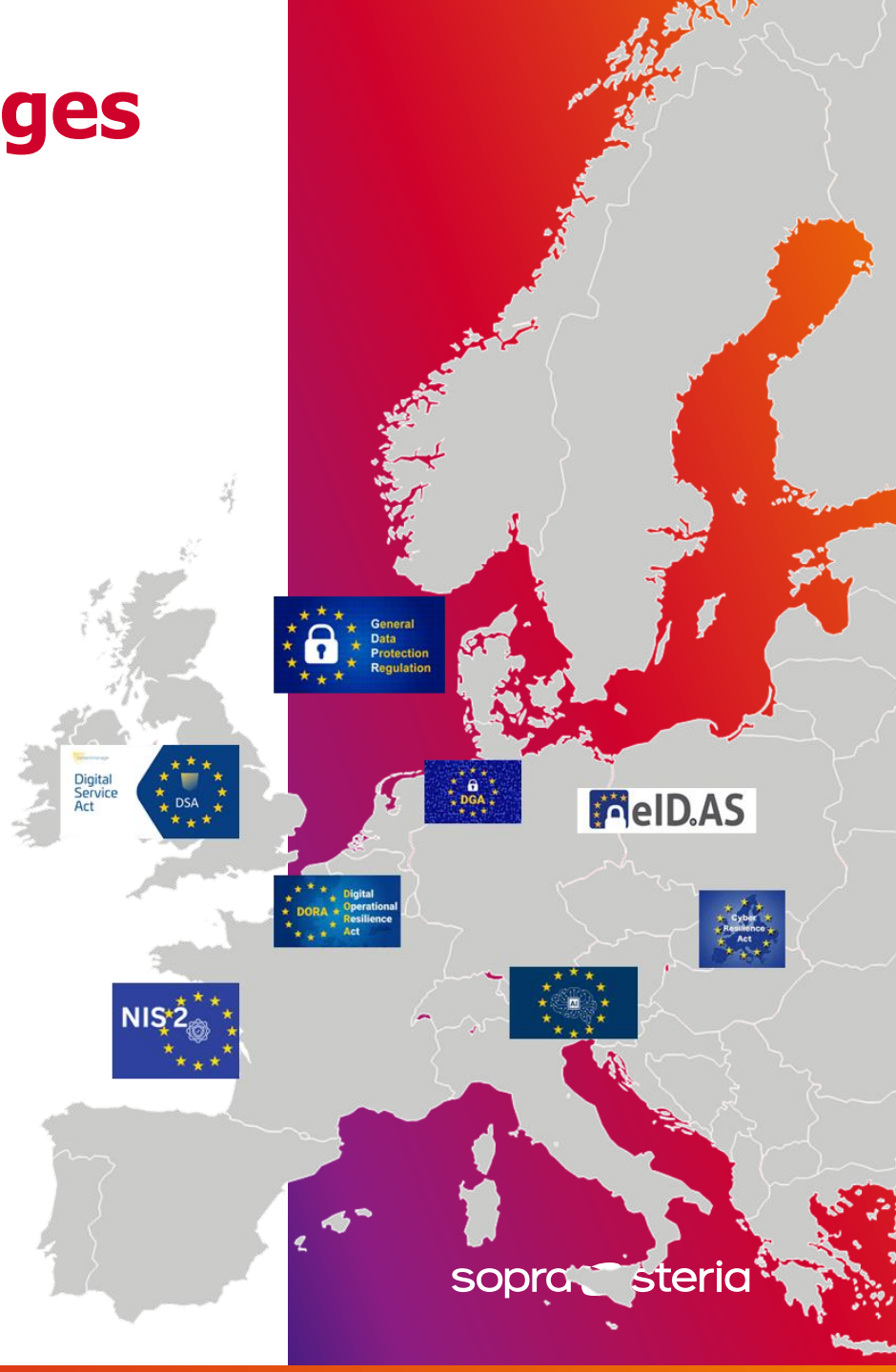
Regulations, as a strategic political leverage for EU

+ 20

New EU regulations related to data within the last decades :
GDPR, eIDAS, NIS 2.0, ², Data Act, Data Governance Act, ESG regulations, …

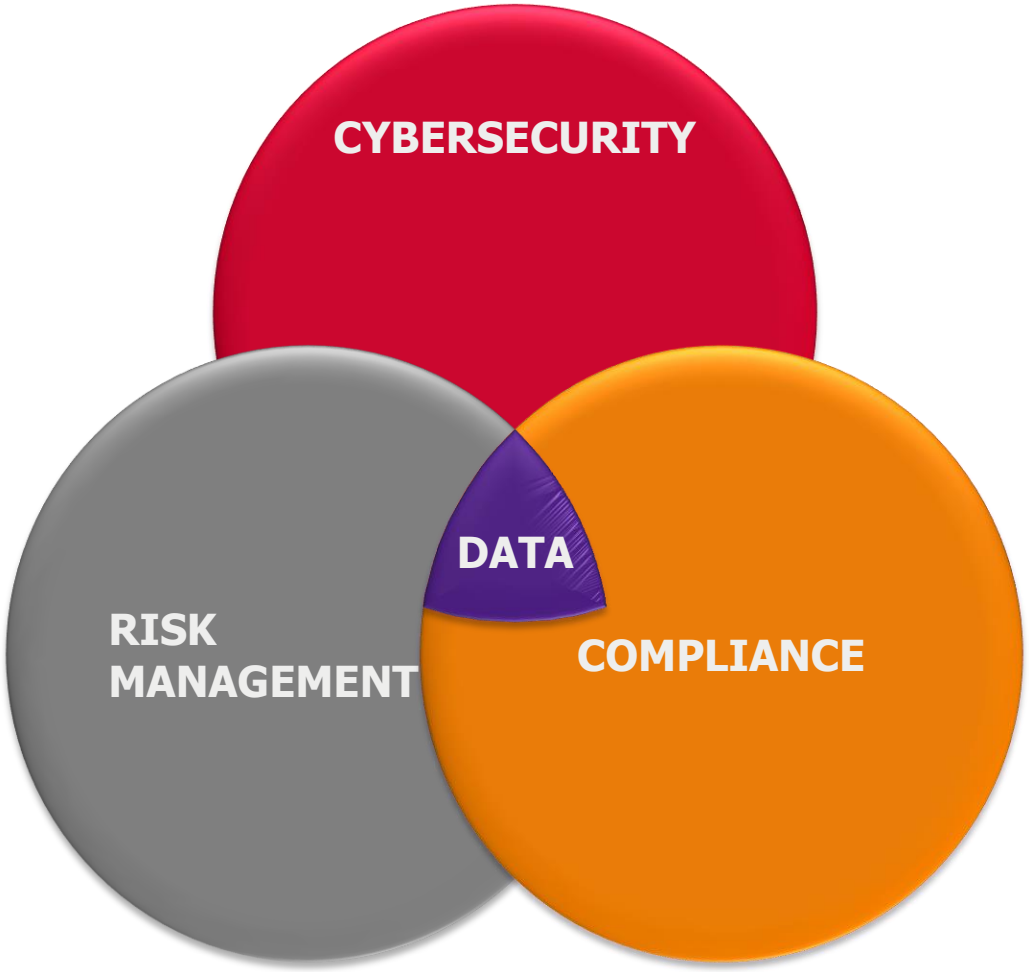
Common ground of regulations

- What data do you have ?
- For which purpose ?
- Where are they stored ?
- For how long ?
- Who may access them ?
- What it the data flow ?



GRC at the crossroads

Cyber, compliance and corporate risk to manage data assets



RULES

- Based on asset and risks
- Guidelines and policies

GOVERNANCE

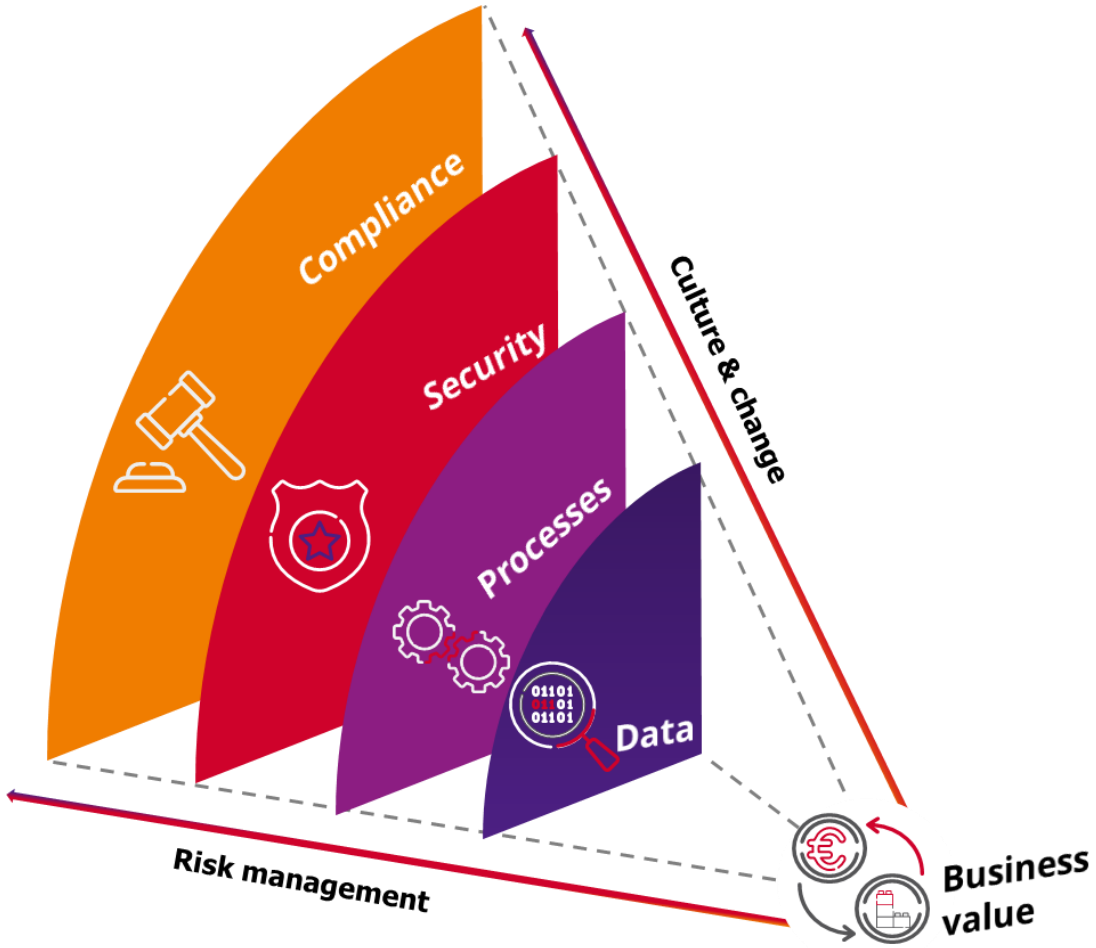
- Roles and responsibilities
- Building long-term processes

CULTURE

- Users accountability
- Company culture

Changing the focal point

Data and process centric approach



From data to compliance

- ❖ Focusing first on data and operation, to enable a long-term compliance
- ❖ Implementing pragmatical measures on both technical and functional side
- ❖ Ensure a short amount of adaption when new regulation enter into force.

Holistic & strategical approach

- ❖ Risks based approach focusing on added-value for business to ensure commitment and involvement
- ❖ Align GRC initiatives with company vision & strategy
- ❖ Improve efficiency by linking and coordinating all GRC components and initiatives

DATA & PRIVACY
USE CASES

Flipping the coin: DATA ANALYTICS

The world is how we shape it

sopra steria | ORDINA a Sopra Steria company | TOBANIA a Sopra Steria company

In numbers

91%

organizations

reported achieving measurable value from data and analytics investments in 2023.

61%

CDOs expressed they have shaping and delivering on data strategy in their top 3% for 2024

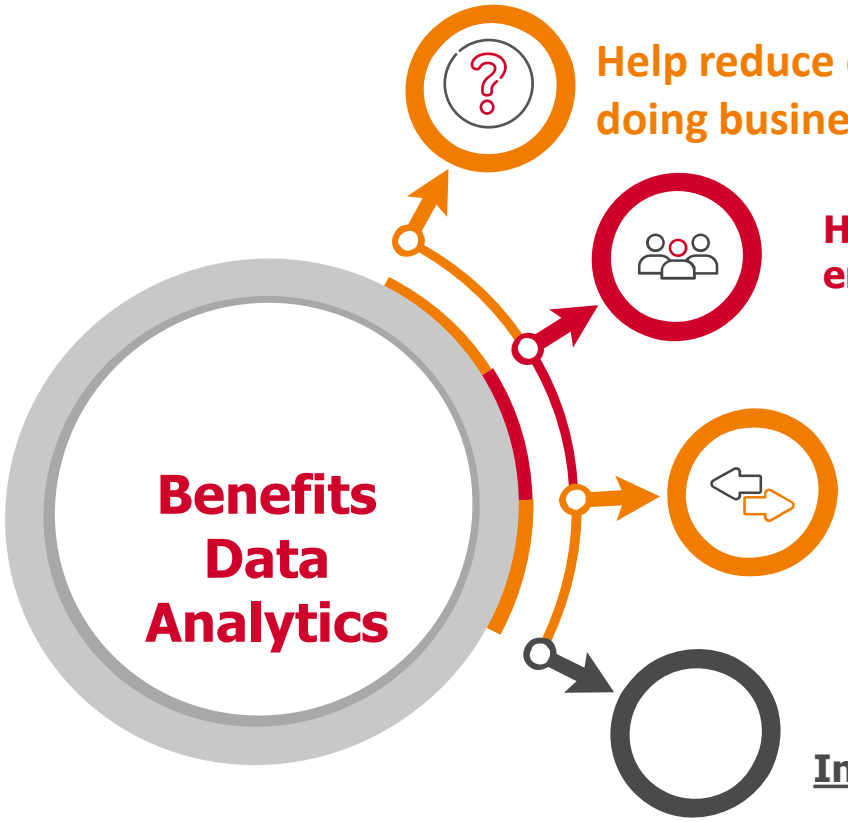
56%

Data leaders plan to increase their budgets in 2024

Data Analytics

The science of analysing raw data to make conclusions about that information.

Leading organizations to make smarter, better, well-informed decisions



Help reduce costs by identifying more efficient ways of doing business

Harness power of data, optimize processes and enhance overall performance

Raw data turned into meaningful insights

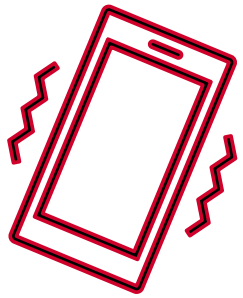
BUILDS COMPETITIVE EDGE AND IDENTIFIES OPPORTUNITIES

Involves more Data Protection aspects that you would expect !

> I had seen a pair of shoes somewhere online and I really like them. I didn’t know where I can buy them, but suddenly I am seeing proposals to buy them everywhere online.

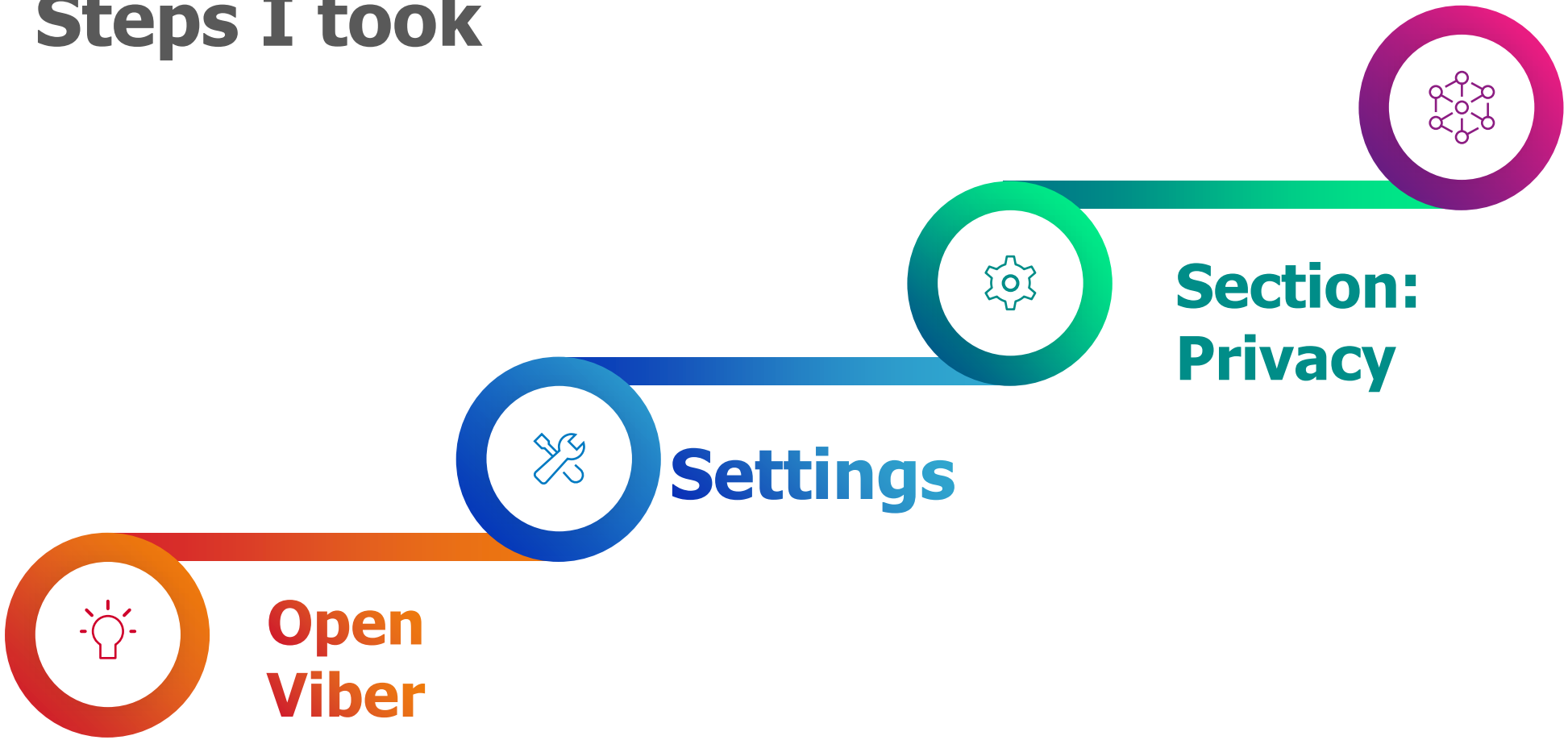
How does this happen?

Unlocking the Viber example



A practical example on data analytics & data protection elements

Steps I took


Open Viber
Settings
Section: Privacy
Scrolled down and clicked „Personal data” section

Viber story

What I saw when I opened Personal data section

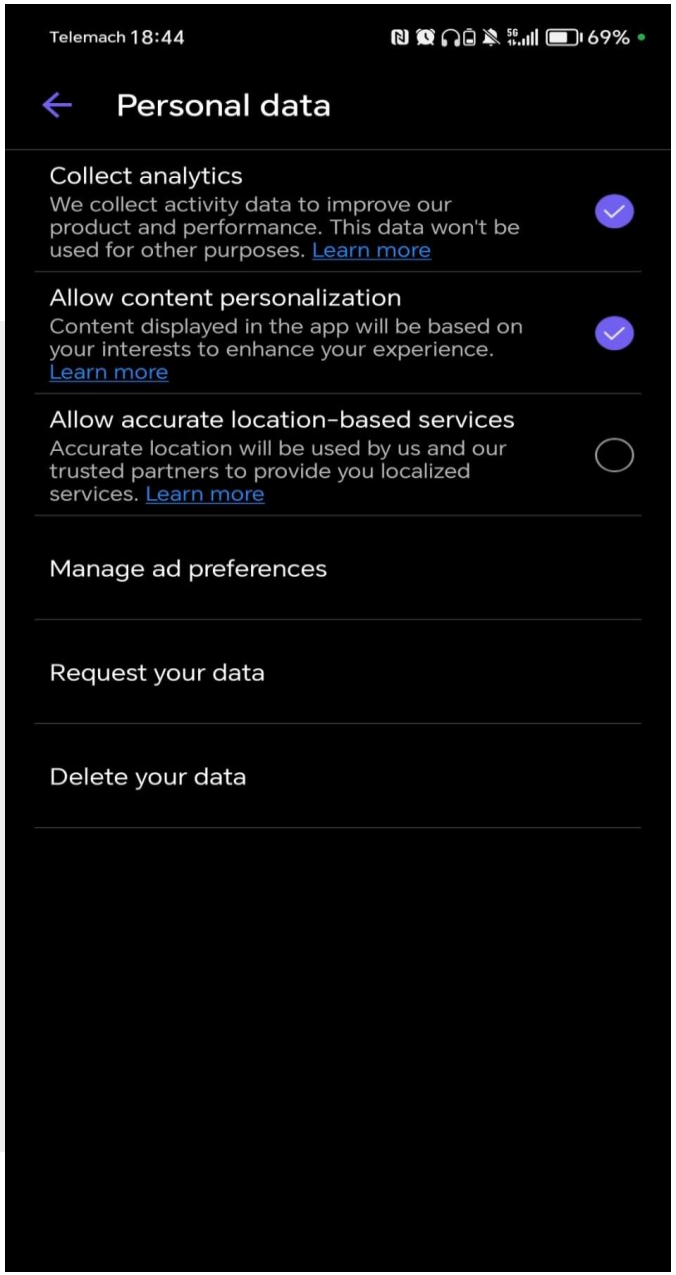
Analytics part ON by default

Pre-default choices set up

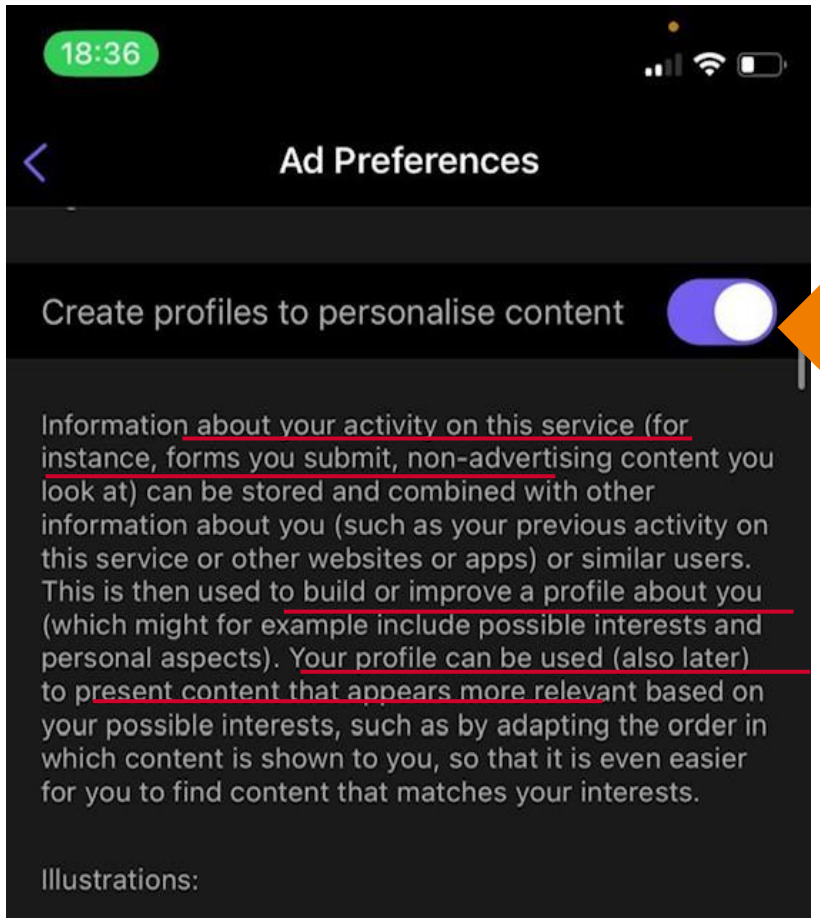
Possibility to perform DS rights

Data retention

Data categorisation provided



Moving further: playing part of the puzzle for others
Key aspect for data analytics is to have **access to data** from different sources – **Various data collection**



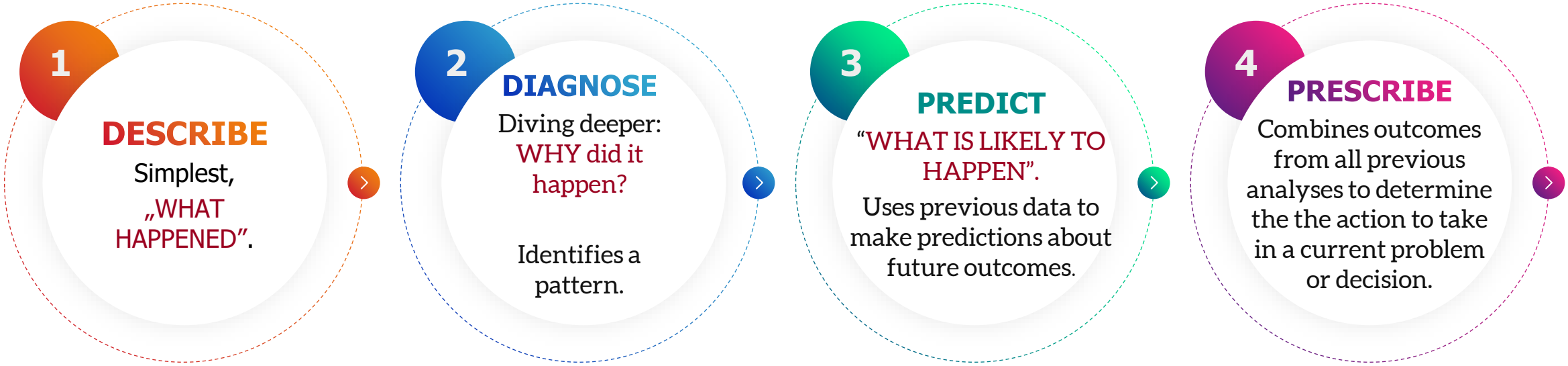
An apparel company wishes to promote its new line of high-end baby clothes. It gets in touch with an agency that has a network of clients with high income customers (such as high-end supermarkets) and asks the agency to create profiles of young parents or couples who can be assumed to be wealthy and to have a new child, so that these can later be used to present advertising within partner apps based on those profiles.

When processing your data for this purpose, 485 of our trusted partners listed below rely on your consent; and none of our trusted partners listed below rely on their legitimate interest.

?

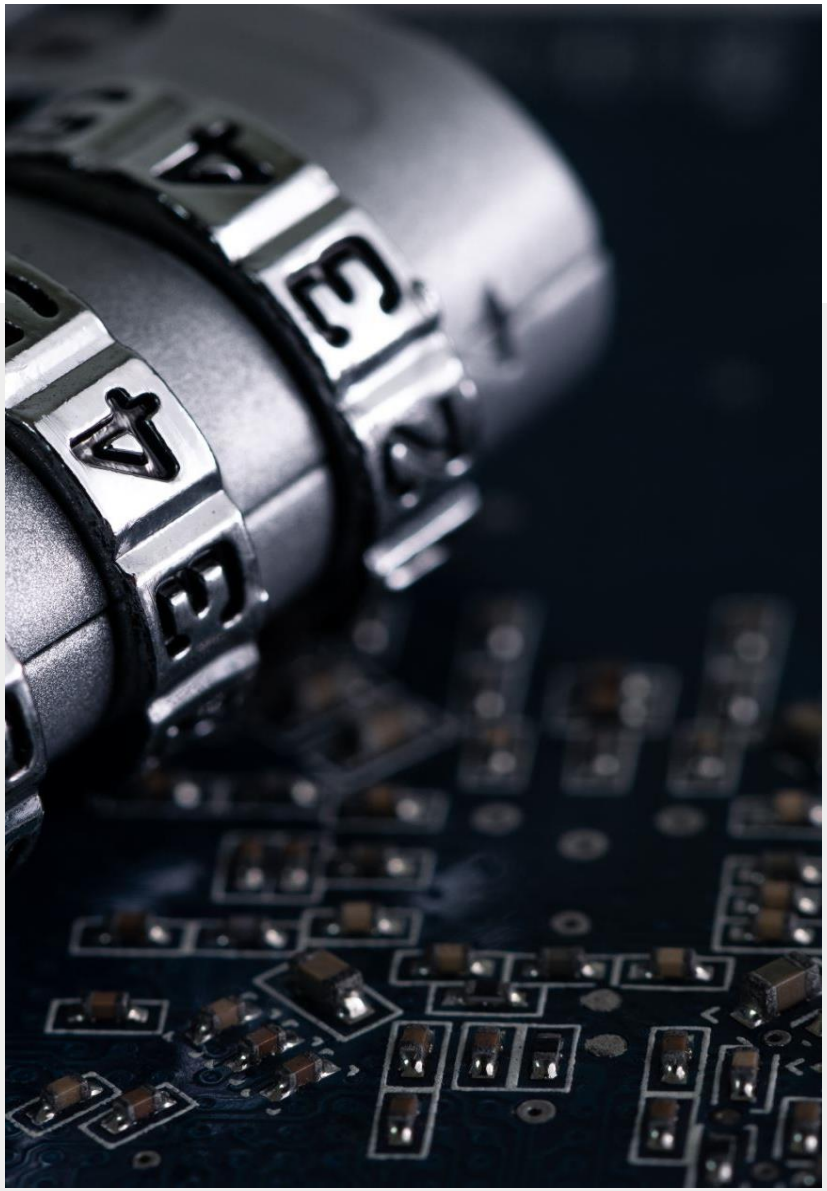
The important things is not only access to data, BUT the way data is being analyzed and interpreted

4 groups that create the puzzle of the data analytics to achieve their objectives

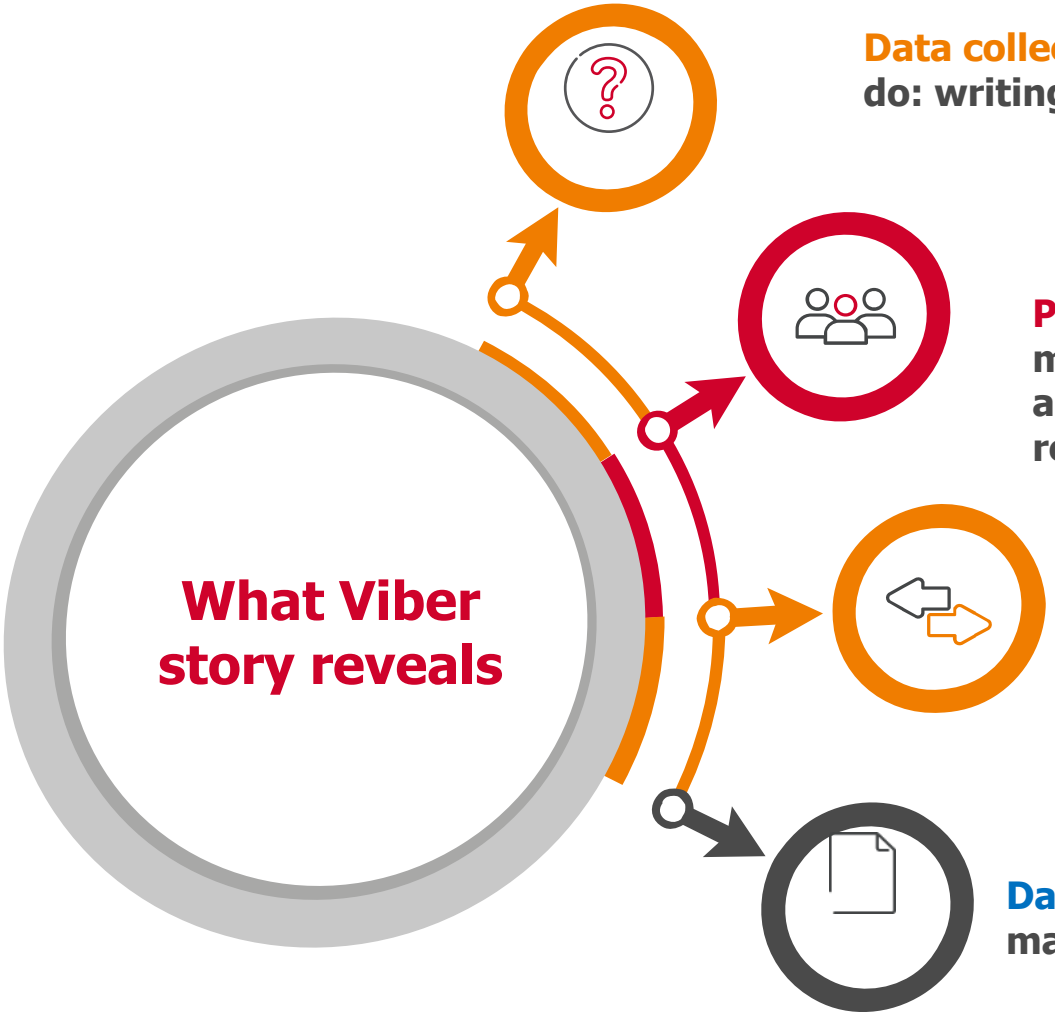


Switching the coin: DATA PROTECTION

Why I see those good shoes everywhere?



sopra steria



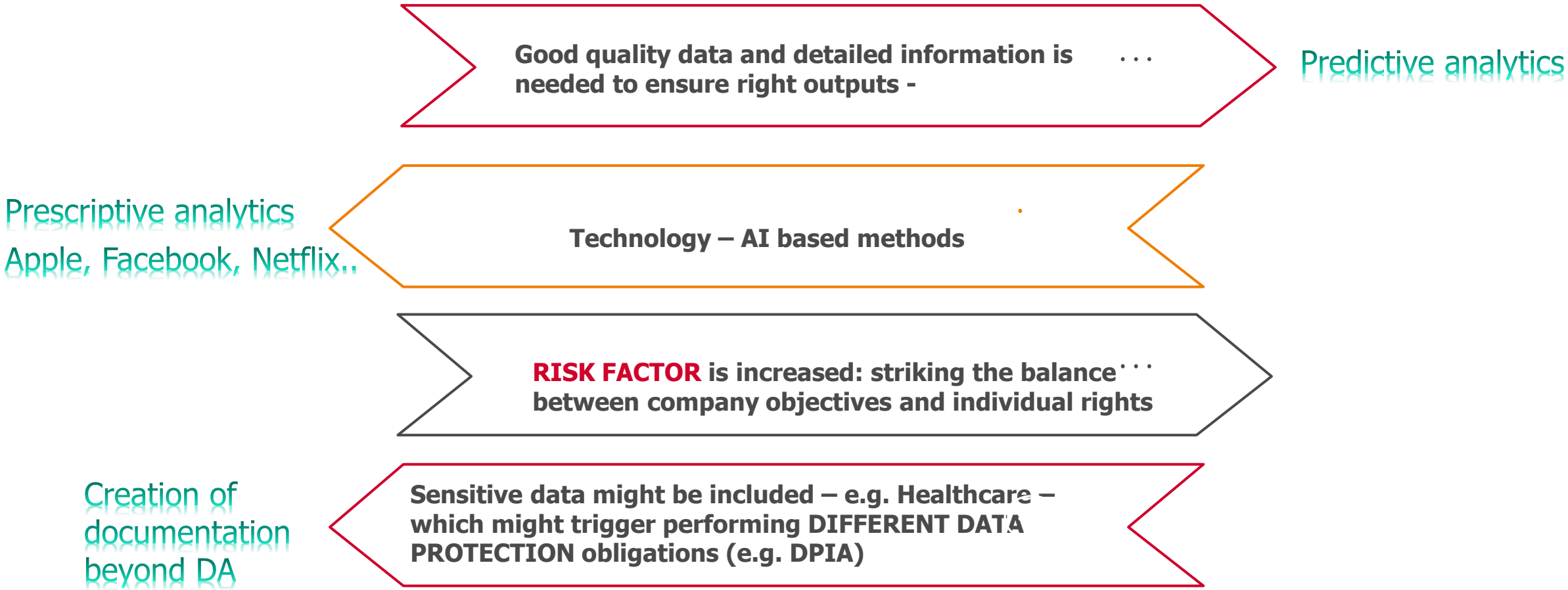
Data collection in various ways: Data is collected by different set of activities I do: writing about shoes, clicking links, sharing links, watching content…

Purposes to achieve business objectives: I see more and more ads of those or similar shoes as the goal is to maximize advertising, personalised content, sales, customer retention…

Personal data of individuals: various personal data and identifiers are collected, my name, gender, location, age, information about my online behaviour and pattern detecting that I spend lots of time watching good shoes over different platforms

Data is involved in different activities: collection, sharing, matching, combining, reporting…

Remember this when using DA that trigger DP



When companies do not…

Understand **WHAT data they have**

Specify, inform, document **WHAT they do with data and HOW did they obtain data**

Question purposes for which they analyse the data to achieve their objectives

Think about rights of individuals (their customers) when engaging in data analytics projects

Deploy CIA measures to data in question risking data being compromised

Things can go really wrong….

THEY CAUSE DATA BREACHES

Violation	Sum of Fines
Non-compliance with general data processing principles	**€ 2,036,593,079** (at 533 fines)
Insufficient legal basis for data processing	**€ 1,649,046,212** (at 607 fines)
Insufficient technical and organisational measures to ensure information security	**€ 385,102,475** (at 349 fines)
Insufficient fulfilment of information obligations	**€ 237,304,420** (at 184 fines)
Insufficient fulfilment of data subjects rights	**€ 98,199,170** (at 188 fines)
Unknown	**€ 9,250,000** (at 9 fines)
Insufficient cooperation with supervisory authority	**€ 6,149,429** (at 92 fines)
Insufficient fulfilment of data breach notification obligations	**€ 1,781,082** (at 32 fines)
Insufficient data processing agreement	**€ 1,057,110** (at 11 fines)
Insufficient involvement of data protection officer	**€ 919,300** (at 15 fines)

2,054,054,062 €

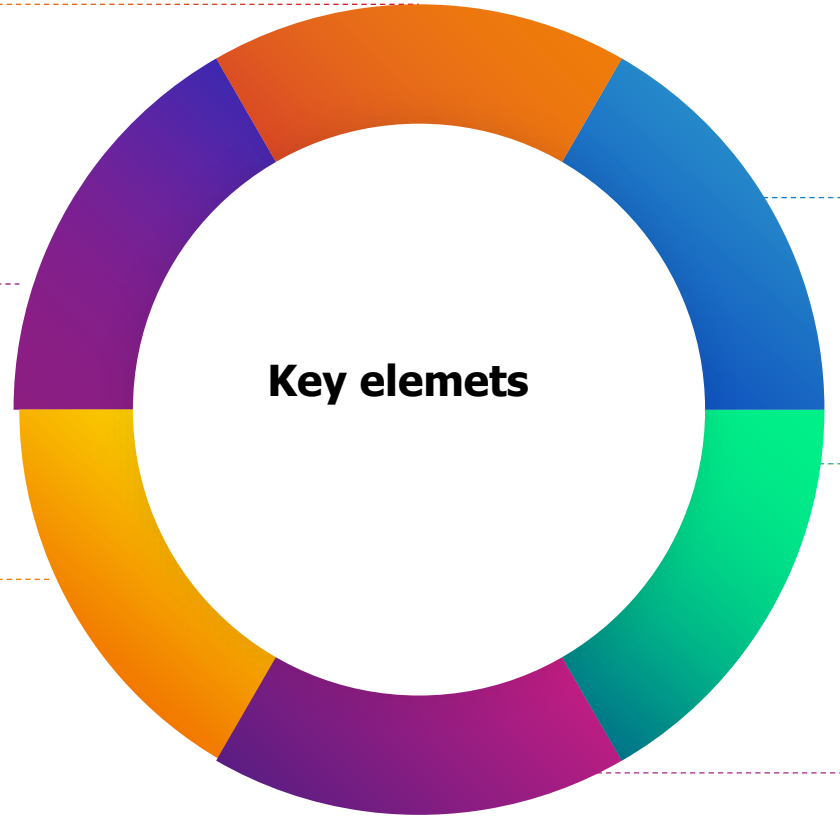
Sum of fines issued in 2023 only.

Obligations from data protection for data analytics

Upholding DO principles: data minimisation, purpose limitation

Data security

Documentation of activities and processes – including impact/risk assessments

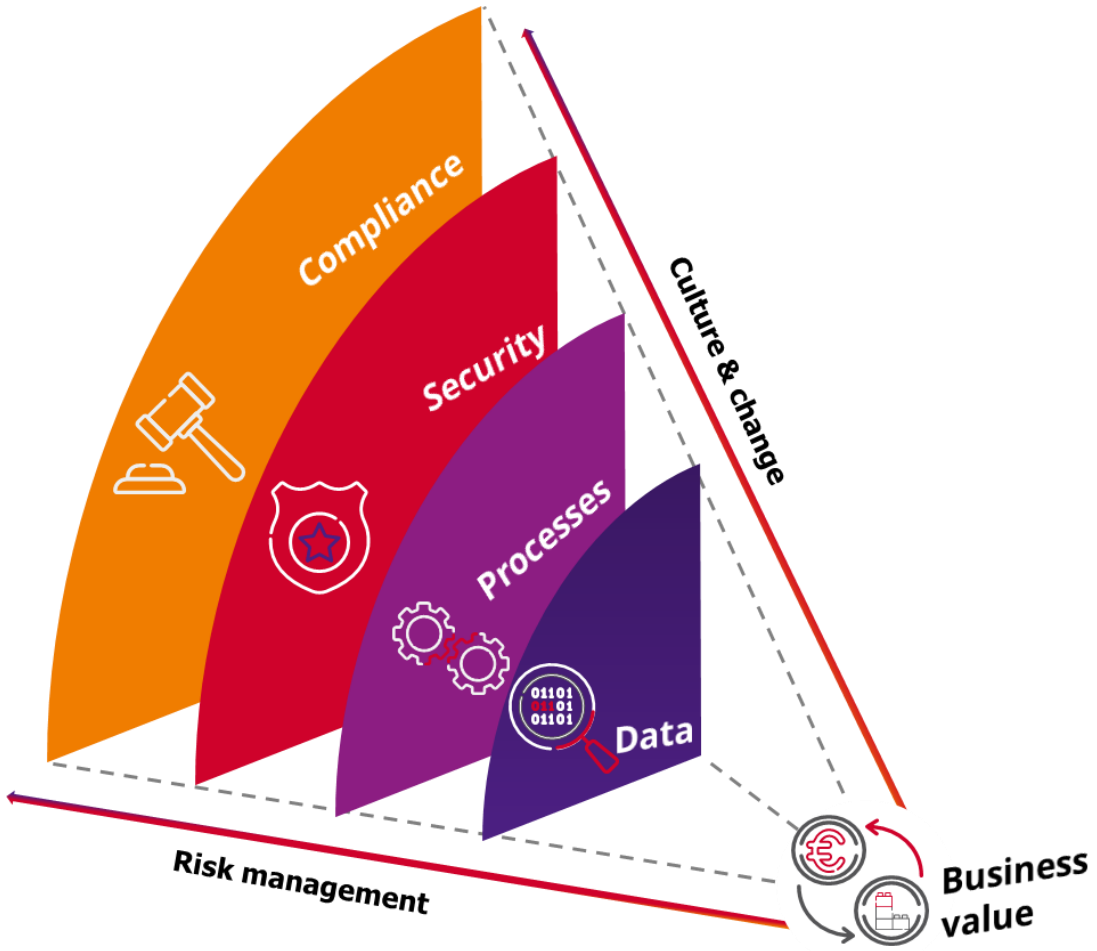


Lawful and transparent data collection and processing;

Data accuracy and data sensitivity

Risk-based and „By design" approach

Coming together: How do you do it?



From data to compliance

While the **way you analyze data** is key for **data analytics, access to data** for the analysis and **how you approach activities to perform data analysis** is answered by data protection.

Data Protection is key counterpart to ensure data analytics to be done in correct and proper way.

Consulting DPO professionals and asking CDO to integrate DP in his practices will help you.

KEY
TAKE AWAYS

Key take away

The two sides of the same coin

DATA ARE MORE TARGETED

AI COMPLEXIFY CYBERATTACKS

ACHIEVING GOALS IN A COMPLIANT WAY

REGULATION CHALLENGES

D&A SUPPORT KPI MANAGEMENT

SIMILAR GOVERNANCE METHODOLOGY

Ivana BUTORAC

EU Compliance lead

Florian DELABIE

Data Governance & Security lead