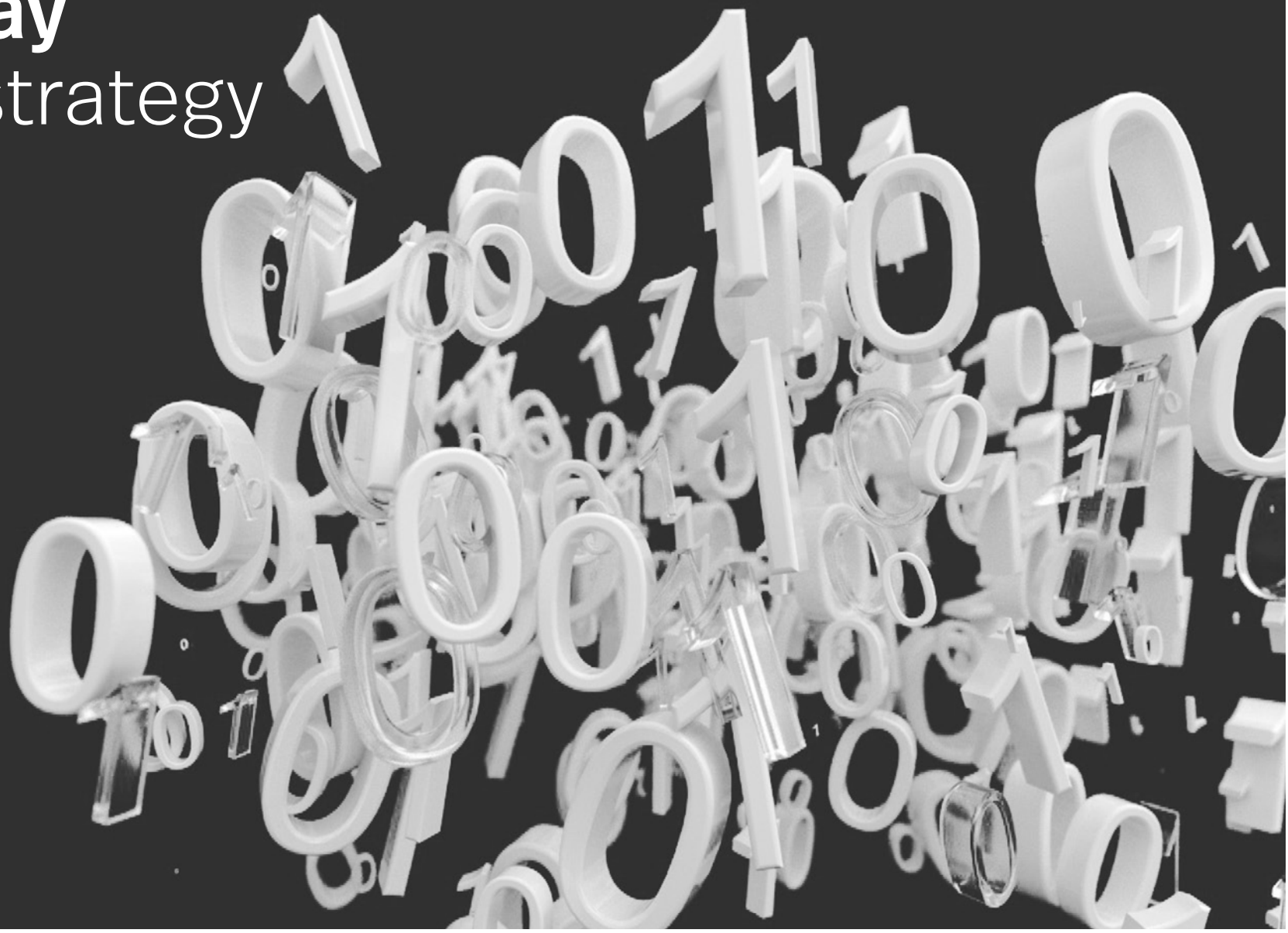
Munich digital day

Creating a data strategy – key practical and legal issues

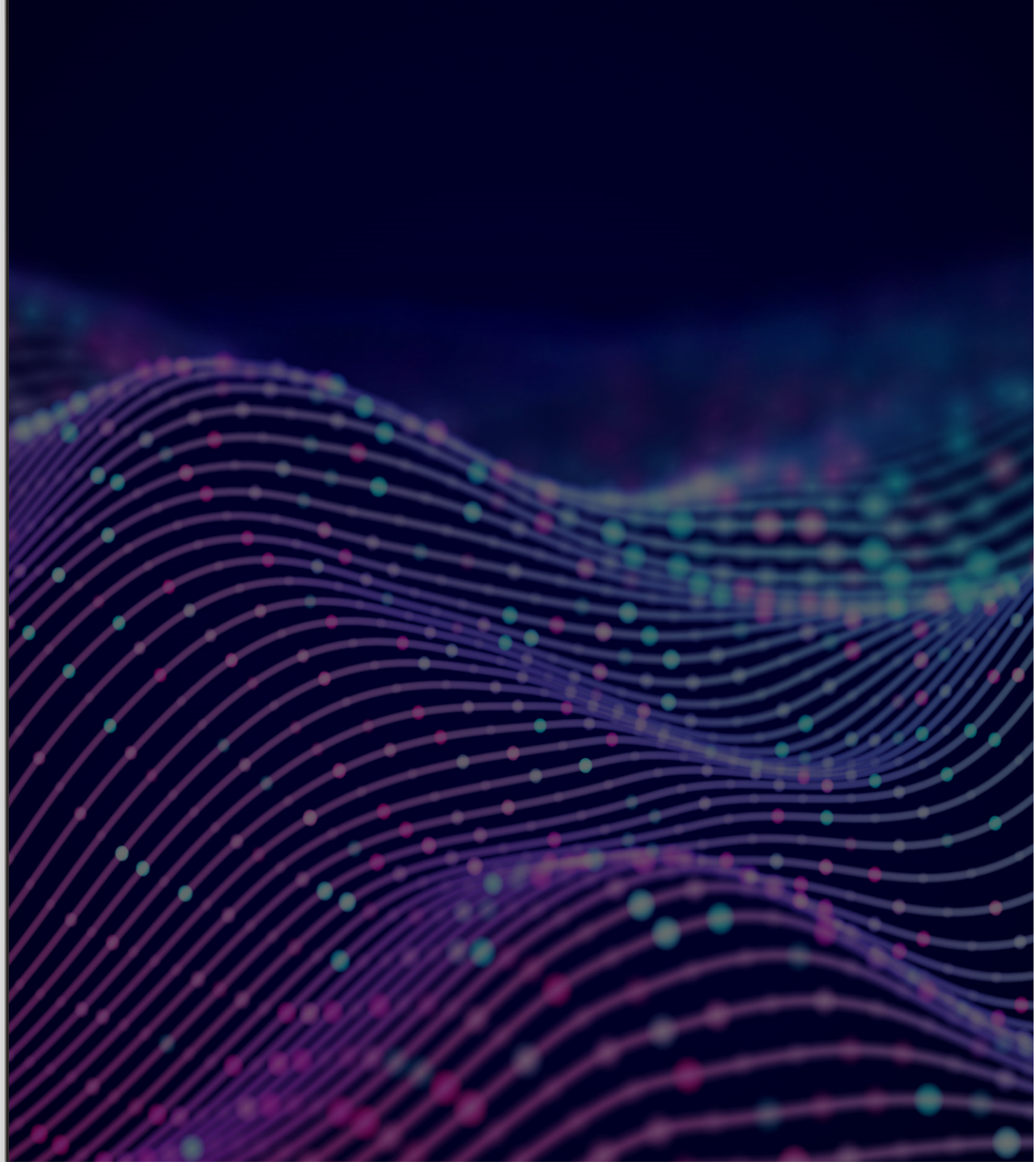
Christopher Götz
Alexander Brown
Sue Diver
Peter Lee



Agenda

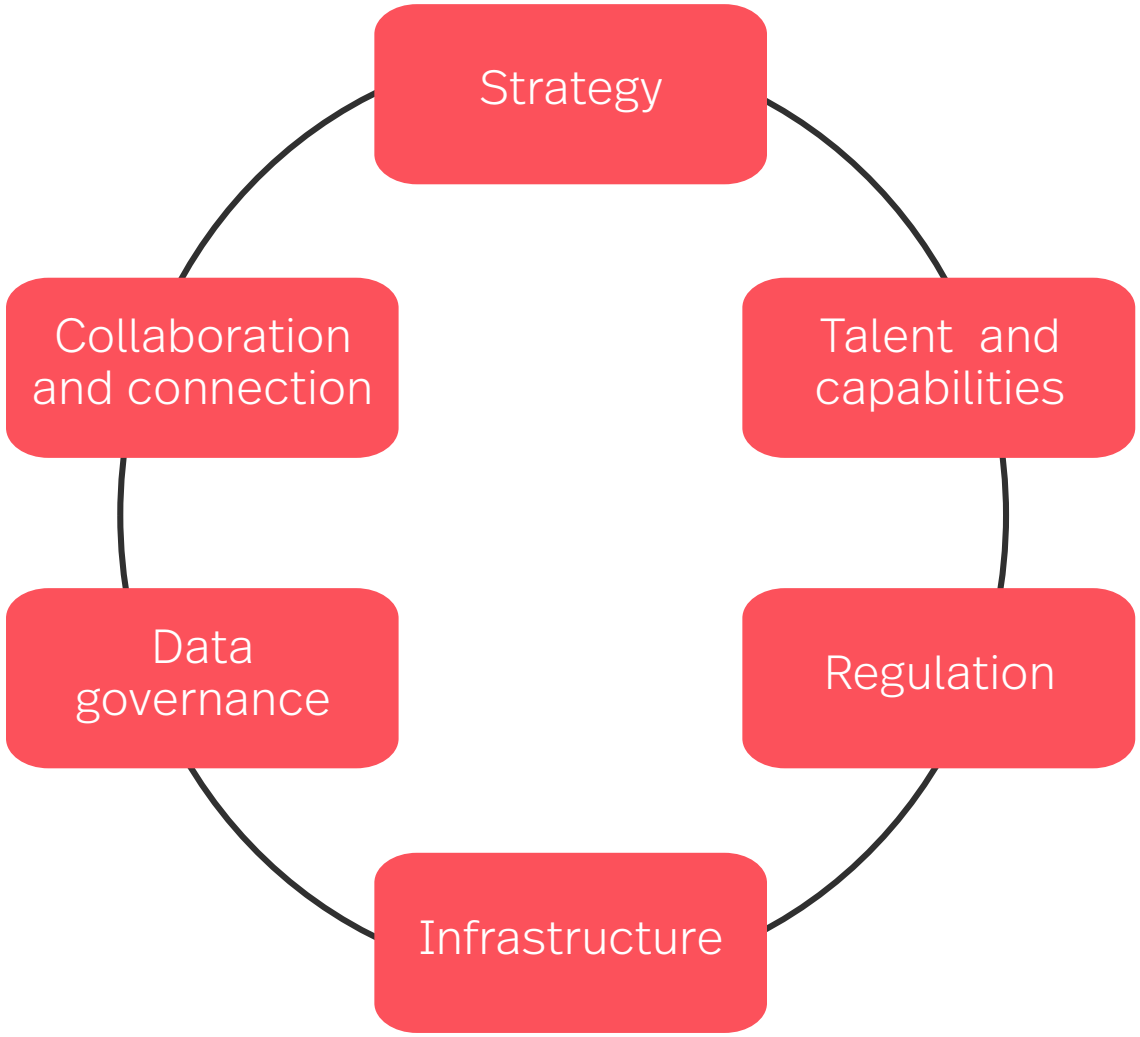
In the course of this session we will share with you insights from:

- Our ‘Big Data Race’ research
- Our own ongoing journey
- Our experience in supporting clients through their journeys
- Key legal & regulatory considerations



Data commercialisation maturity framework

§ Strategy



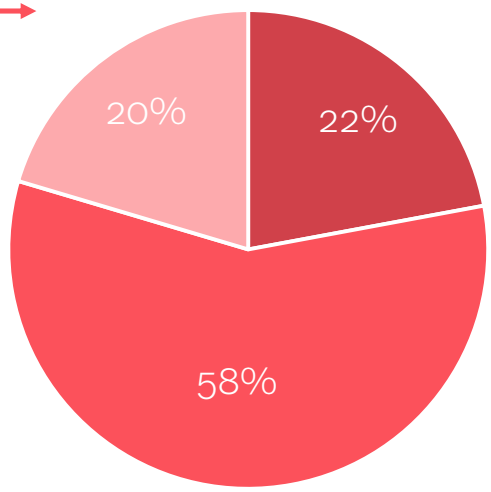
Disjointed strategies

The majority (78%) of companies have data commercialization strategies, but only 20% have an overarching strategy that coordinates activity

Data commercialisation strategy

- We have a data strategy that addresses governance and compliance rather than data commercialisation
- We have a number of data commercialisation strategies but they are typically not aligned across different business units
- We have an overarching data commercialisation strategy that guides and coordinates all our data commercialisation efforts

28% of businesses in Western Europe (excl. UK) and 26% of businesses with a $1bn+ revenue have an overarching data commercialisation strategy



74% say that their data commercialisation strategy aligns with an overarching business strategy

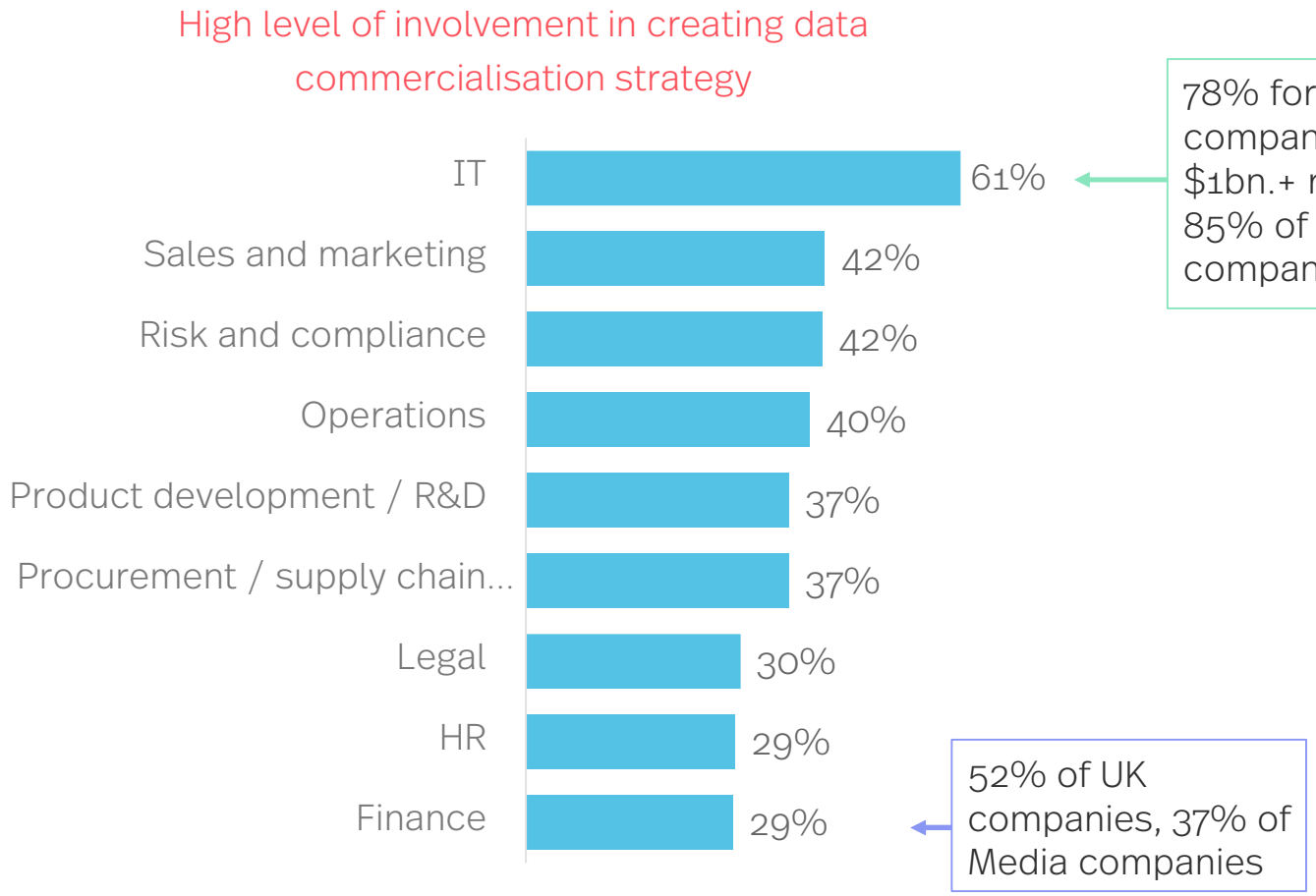
65% conducted a comprehensive risk assessment on various data commercialisation projects when developing their organisation's strategy

70% say their data commercialisation strategy includes strict governance processes around the consideration and approval of specific data commercialisation projects

45% say that their data commercialisation strategy involves a certain amount of risk taking

An IT-centric approach

Legal, HR and finance functions rarely input into data commercialisation strategies.



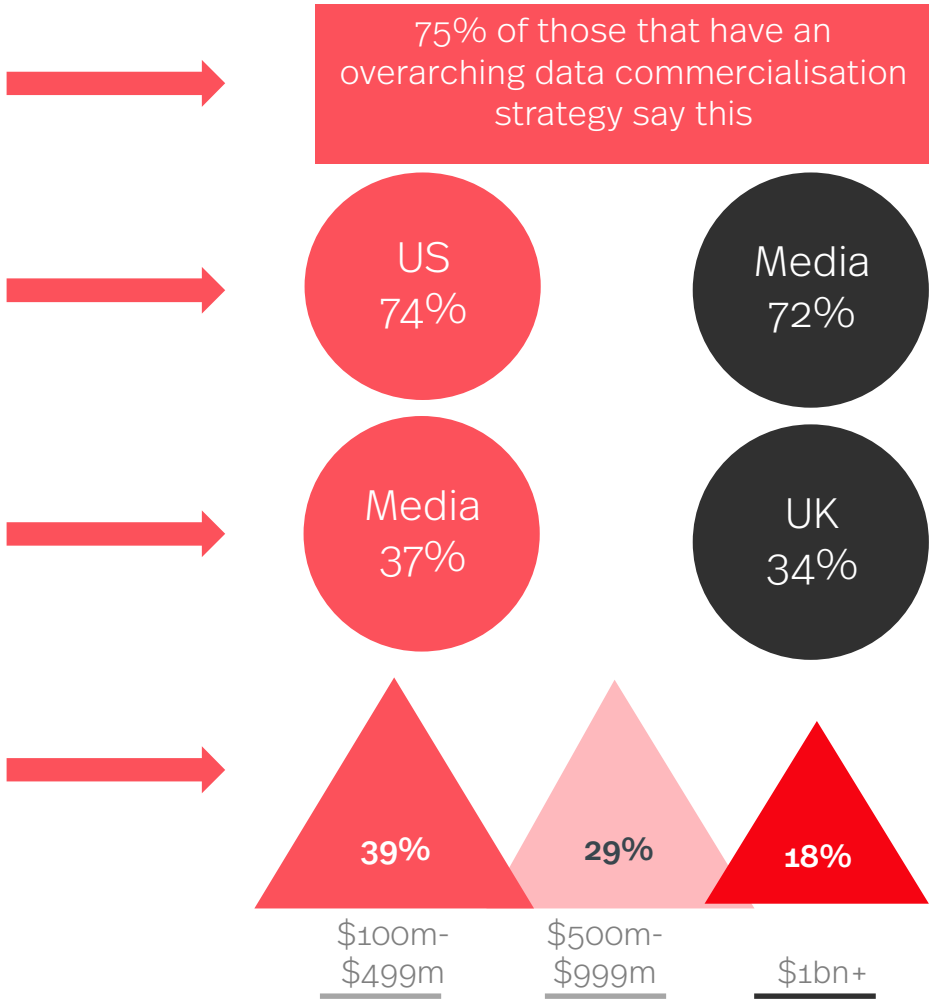
73% extensively consulted external experts when developing and implementing their data commercialisation strategy

55% consulted customers when developing their data commercialisation strategy

A data-driven workforce

A large proportion (40%) of companies do not have all the skills they need to meet their data commercialisation objectives. And data-driven decision making has some way to go.

- **60%** We currently have all the skills we need to meet our data commercialisation objectives
- **66%** Our company has launched special initiatives to recruit specialist skills needed for data commercialisation
- **45%** Executives at our company change their mind if the data makes a compelling case for doing so
- **31%** of executives DO NOT have the information they need to effectively manage the business



Why have a Data Strategy?

Successful organisations recognise the need to be empowered by data in all parts of their enterprises to enable them to predict client needs, track clients, proactively map performance, drive improvements in efficiency and determine leading and lagging indicators of practice performance.

In addition, almost all global markets are undergoing significant change; in most geographies new competition has entered the market, bringing with them new propositions for the way products are developed and services are delivered.

Our own data strategy programme aims to address all these needs, is executive led, includes all areas of the business, but also aims to robustly collect and protect high quality data throughout its lifecycle.

There are fascinating details highlighting the difference in approaches between the Leaders and Laggards within our Big Data Race whitepaper. (Take a look – it's free!).

Poll question #1

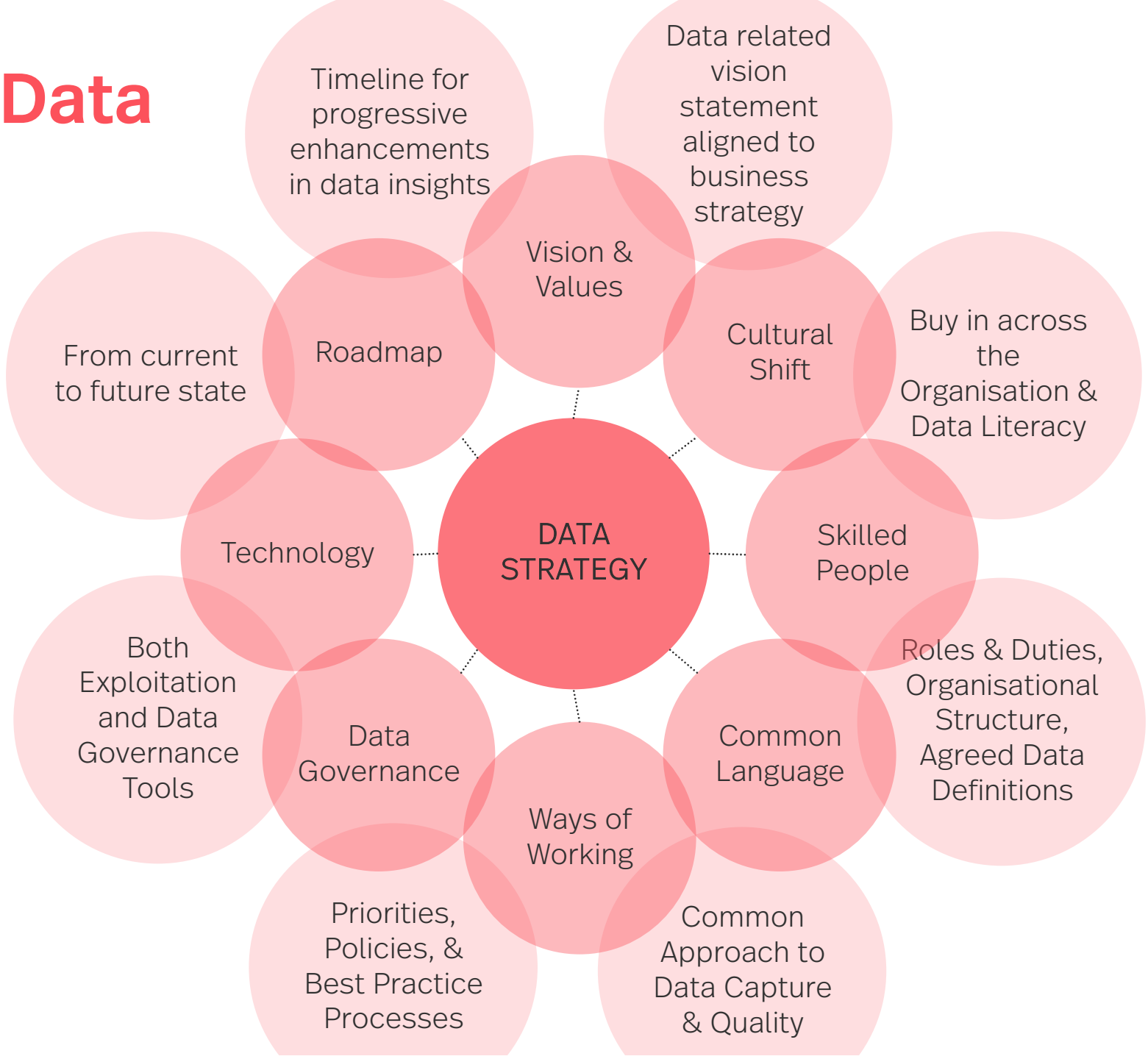
Does your organisation have a data strategy?

simmons+simmons

Poll question #2

Do you have a data strategy for your legal department?

What is a Data Strategy?



Your legal function

Data strategy

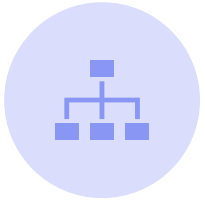
Facilitate business and transactions

Help manage risk

Work smarter (more for less and safer)

Unlock new value and information

Measure and manage



Allocate tasks (internal and external)

Demonstrate value of legal

Display and visualise legal information

Key Points For Success

Your Data Strategy should clearly articulate how it will support your strategic business plan:

- Have clearly defined and prioritised business use cases

Identify & deliver quick wins using data already available:

- But ensure you are clear about the quality of the data

Recognise it is a data value journey:

- Descriptive Analytics - *What* has happened
- Diagnostic Analytics – *Why* it has happened
- Predictive Analytics – What *could* happen
- Prescriptive Analytics – What *should* happen

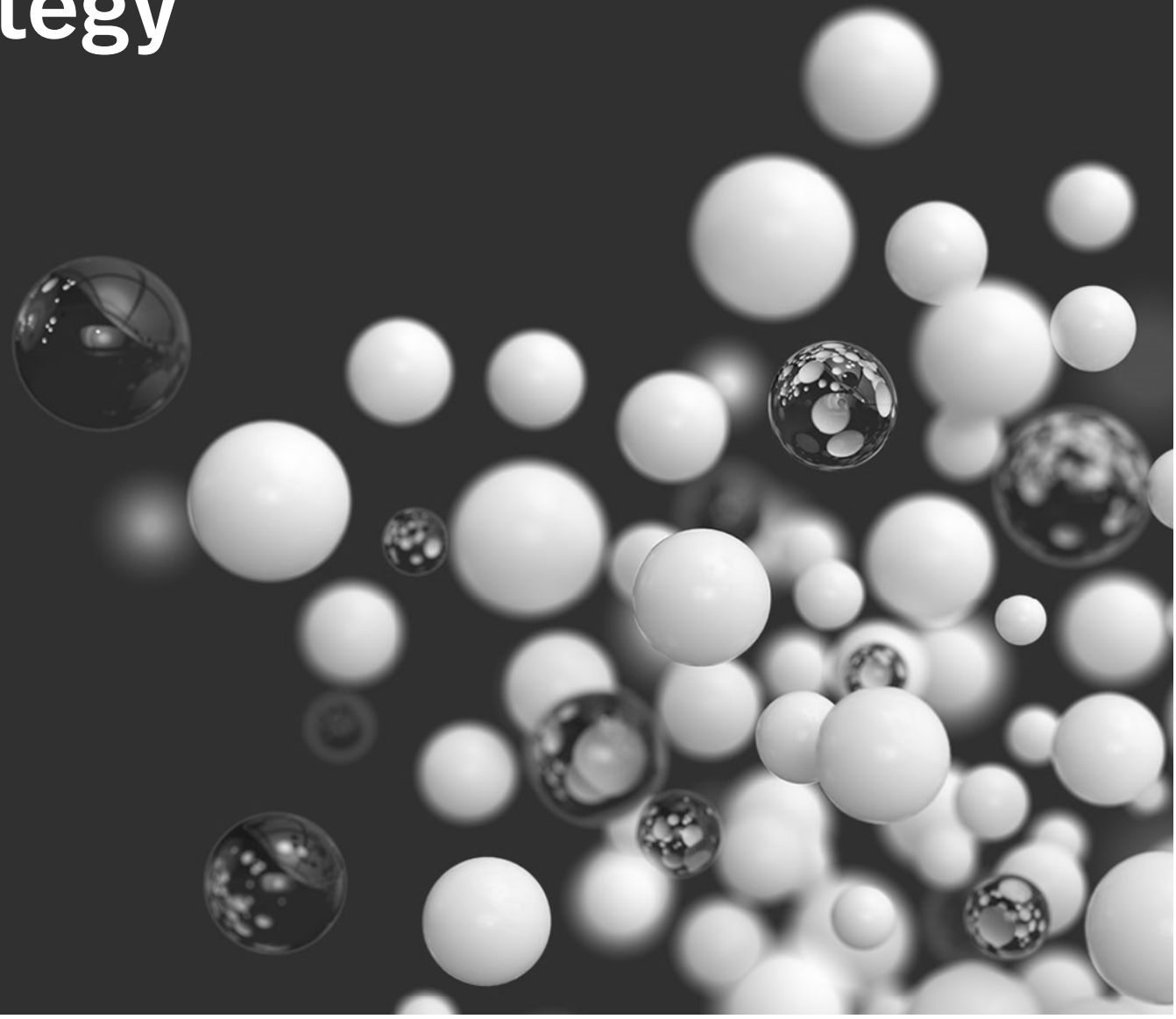
Business buy in is critical:

- Find a key team / department & work with them to demonstrate value

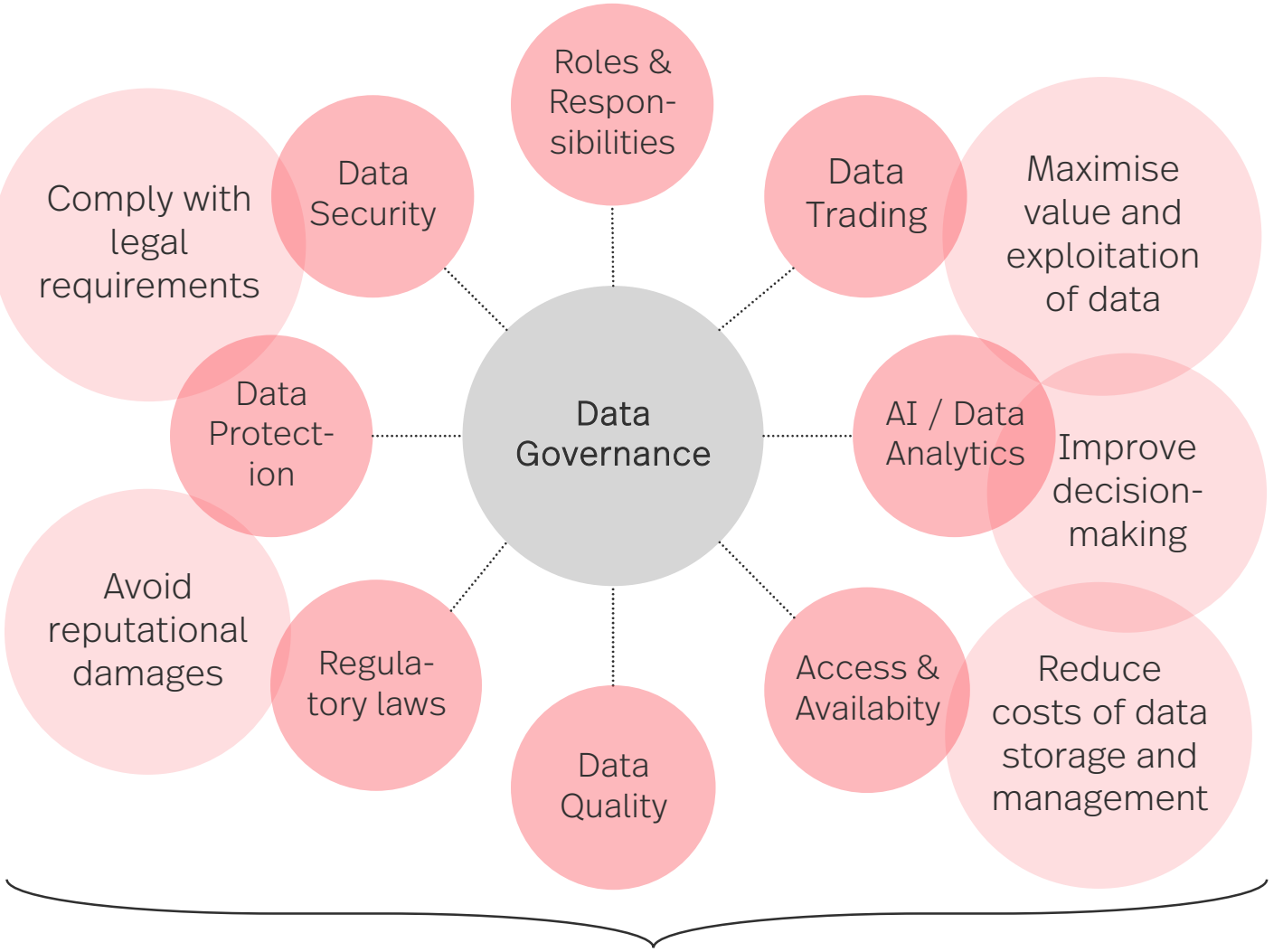
simmons+simmons

Developing a Data Strategy

Key legal issues



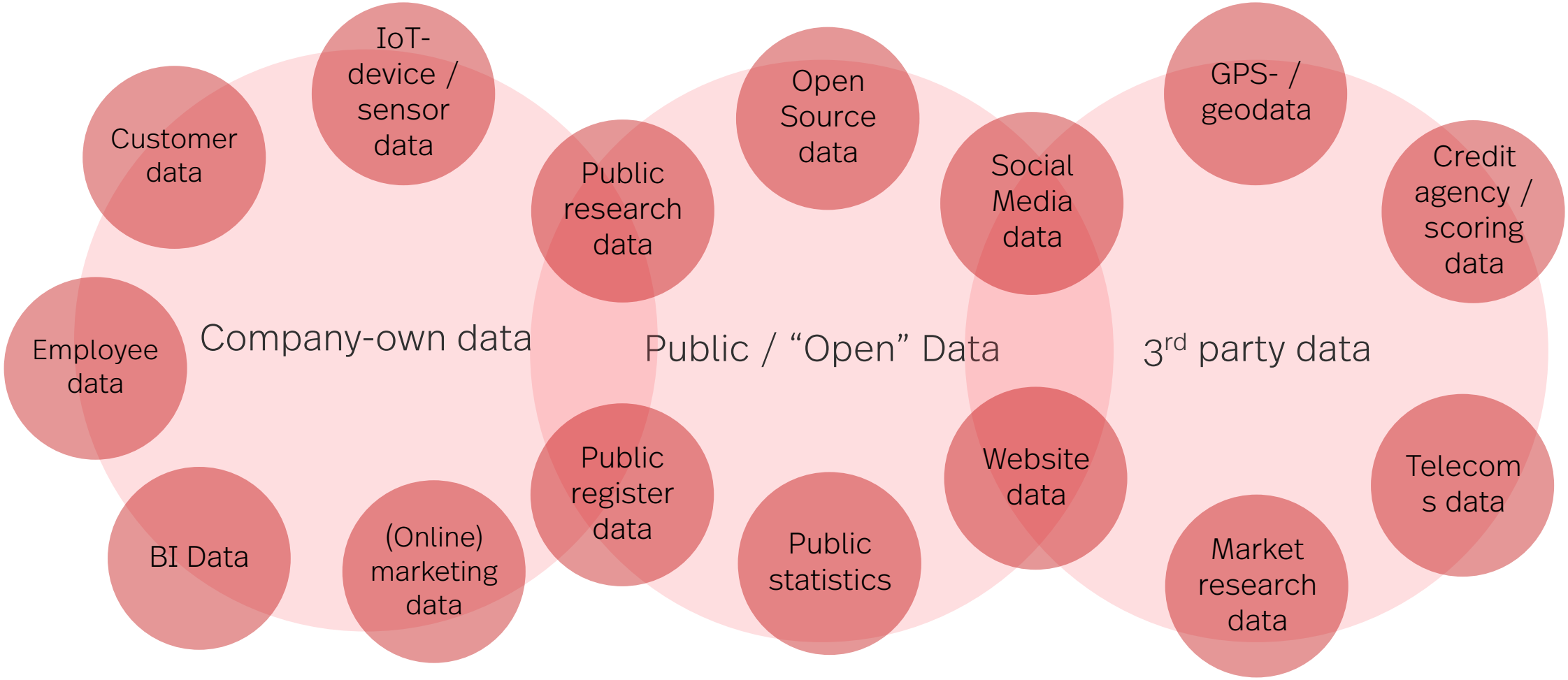
Data Governance



Planful balancing risks and chances

Data Sources

Organisations derive data from an increasing variety of different sources



Data Sources

- Need for legal basis
- Purpose limitation
- Need for data security
- Data Subjects' Rights
- Record of processing
- Retention periods
- Data Protection Impact Assessment
- Compliant global data transfers

- Does any IP-protection apply?
- Need to get any license from employees/ contractors?
- Does intended use create independent IP-protection?

Data Sources

- Need for legal basis
- **Purpose limitation**
- Need for data security
- Data Subjects' Rights
- Record of processing
- Retention periods
- Data Protection Impact Assessment
- Compliant global data transfers

- Does any IP-protection apply?
- Need to get any license from employees/ contractors?
- Does intended use create independent IP-protection?

Purpose Limitation

When collecting personal data, (a) specific purpose(s) for their subsequent use must be defined at this time already.

Personal data once collected must not be used for any purpose(s) than those defined upon data collection, unless:

- Processing for the new purpose(s) is likewise covered by a legal basis for data processing and (unless such legal basis is data subjects' consent)
- The new purpose(s) are compatible with the original purpose (to be demonstrated by data controller!)

Data Sources

Self-created data

Personal data

GDPR Compliance

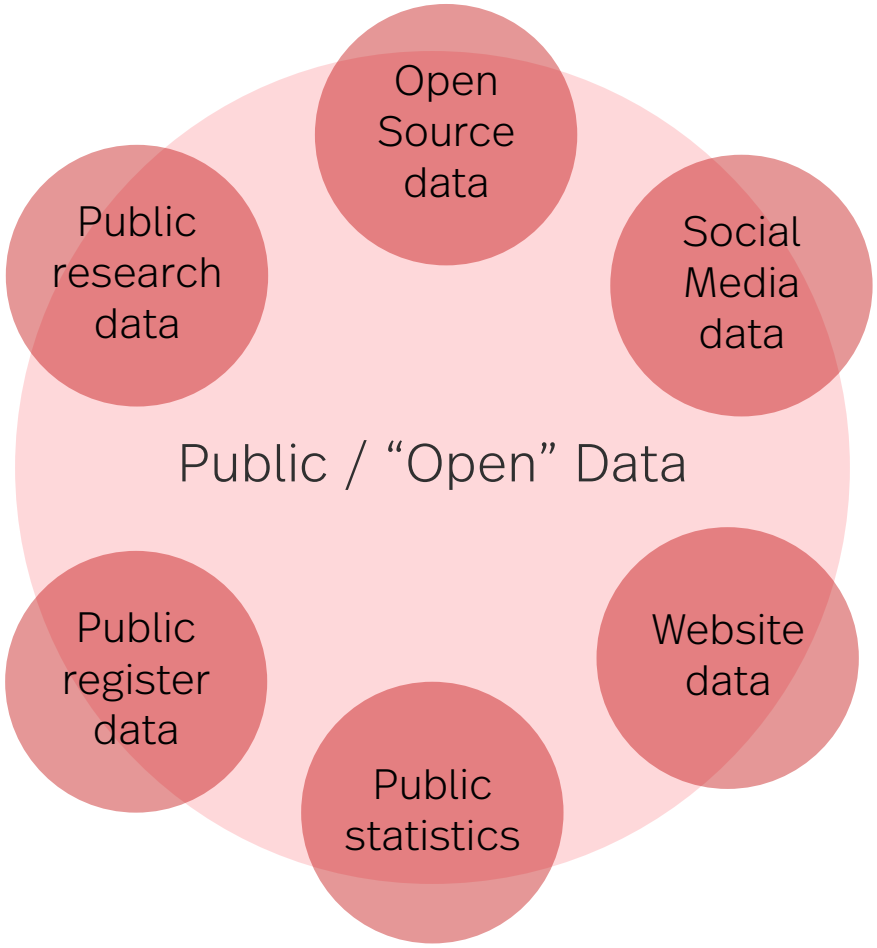
- Need for legal basis
- Purpose limitation
- Need for data security
- Data Subjects' Rights
- Record of processing
- Retention periods
- Data Protection Impact Assessment
- Compliant global data transfers

Other data

IP Protection

- Does any IP-protection apply?
- Need to get any license from employees/ contractors?
- Does intended use create independent IP-protection?

Data Sources



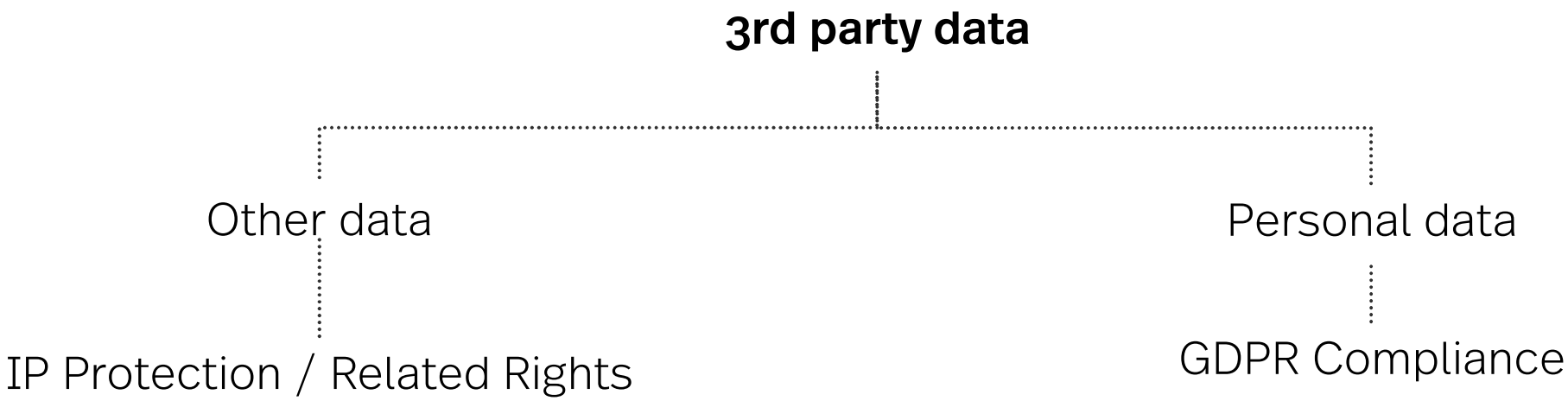
IP Rights & related rights

- Copyright
- Database rights
- Contractual limitations

Data Protection

- Legal basis (Art. 9 (2e) GDPR?)
- Purpose limitation
- Information requirements (Art. 14 GDPR)

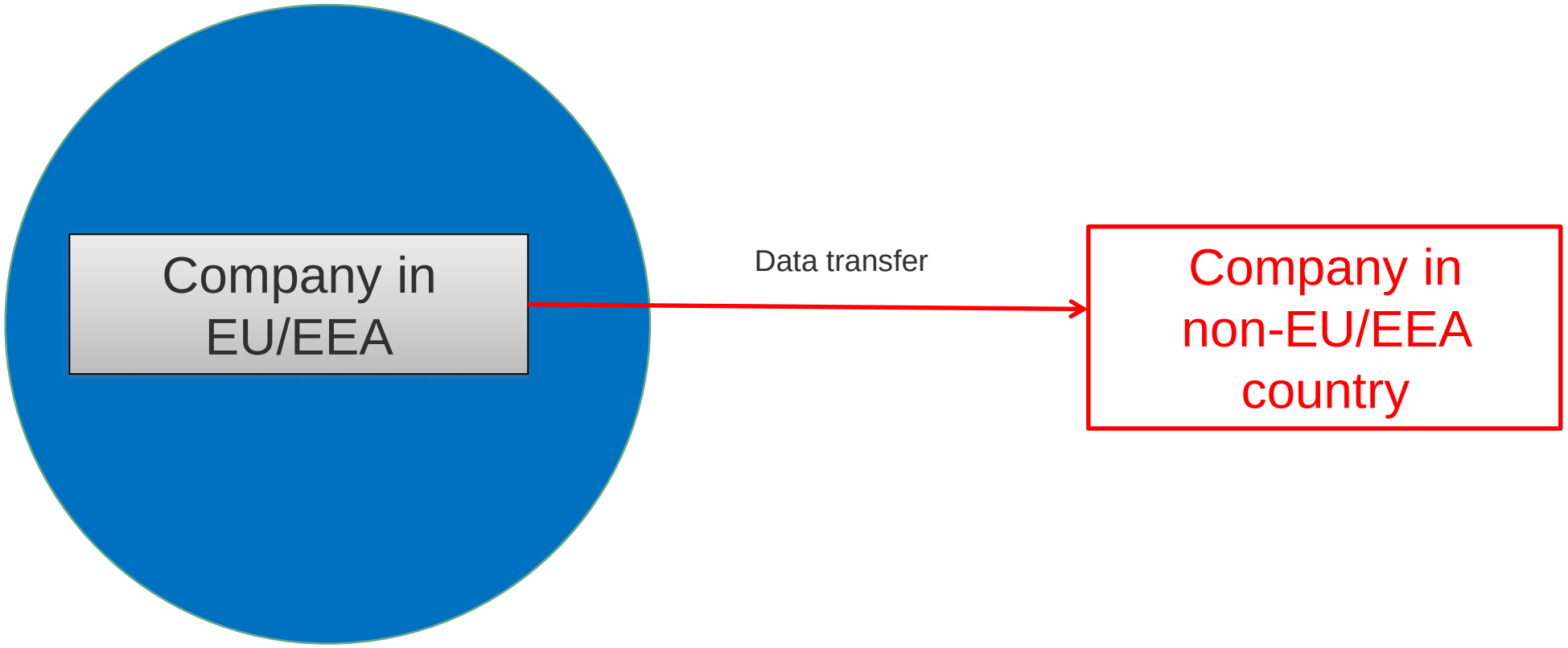
Data Sources



- Data subject to 3rd party rights (database / sui generis)?
- Contractual limits on data use (licensing agreement, NDA)?
- Need for license / use rights management
- Warranty / Indemnity

- Warranty/indemnity that data can be used for intended purpose?
- Need for data processing/joint controller agreement?
- Who/how to deal with data subject rights?

(Personal) Data transfer to a country outside the EU



To do’s for global organizations

1) Preparatory due diligence / process - exporters:

- Create a list of international transfers of personal data and importers of the personal data (both intragroup and external).
- Within that list indicate which are
  - transfers to a non-EEA country subject to adequacy decision / SCCs / BCRs - for SCCs and BCRS, an “adequacy assessment” (as described below) should be carried out; and
  - transfers to a non-EEA country without adequate protection being in place

2) “Assessment of adequacy” (do laws in data importing country comply with EU standards)

3) Implement supplementary measures, if necessary and possible

4) Alternatives

5) Ongoing Due Diligence

Ctrl Transfer

Risk assessment of cross-border data transfers

(Big) Data Management

Access & Availability	Purpose & Storage Limitation	Pseudonymisation / Anonymisation	Cybersecurity
• Restriction of access/write-rights on “need-to-know” basis. • Ensure quick retrievability of (individual) datasets	• Timely deletion of personal data required, • Personal data must not be collected when its future use is (still) unclear.	• Pseudonomize / Anonymize datasets whenever possible.	• Ensure cybersecurity by means of technical and organisational measures

These requirements (and others) also apply in case of establishing “data lakes”

Data Quality

Why data quality matters from a legal perspective ...

1 **Data Accuracy**

Inaccurate or outdated data itself may impair GDPR compliance in several dimensions (data subject rights, data breaches, storage limitation)

2 **Algorithmic decisions**

Poor data quality regularly leads to poor decision-making, which in turn may negatively impact on humans (discrimination, financial damages etc.)

3 **Regulatory requirements**

Where important decisions are data-driven, regulatory laws and standards already today provide for detailed requirements on data quality (even for non-automated decision making).

Artificial Intelligence

Some fundamental legal requirements when it comes to using “artificial intelligence”:

1	Fundamental/Human Rights	5	Technical & Organisational Safeguards
2	Data Quality	6	Transparency
3	Comprehensibility & Human Oversight	7	Accountability
4	Data Minimization	8	Robustness of Algorithms

Artificial Intelligence & Explainability

§ Data Protection Law

- "Artificial intelligence shall be transparent, comprehensible and explainable"
  - Easy accessibility & comprehensibility of information about the data processing and, if applicable, the processing of training data (Art. 12 ff. GDPR)
  - Traceability & explainability of decisions made by AI-system with regard to
    - results,
    - relevant processes and
    - the decision-making process (→ **logic-system** involved!)
      - presentation of the basic logical principles is sufficient
      - no impairment of business secrets necessary

➢ Relevant for privacy statements!

Artificial intelligence & DPIA

Accountability

§ Data Protection Law

- **Data protection impact assessment** (Art. 35 GDPR) regularly necessary
  → reason: "**dual use**" of artificial intelligence!
  - description of the planned processing operations / purposes
  - assessment of the necessity / proportionality of processing in relation to purpose
  - **corrective measures to address possible risks** (guarantees, safeguards, procedures to ensure data protection)
- If high risk for data subjects and no suitable remedial measures
  → consultation of the supervisory authority, Art. 36 GDPR

Trading Data

"Right of ownership" to data?

- Current state: No
- Future? Unlikely – German Data Ethics Commission Report, 23 October 2019

➢ Data ≠ object (*Sache*), therefore not subject to ownership

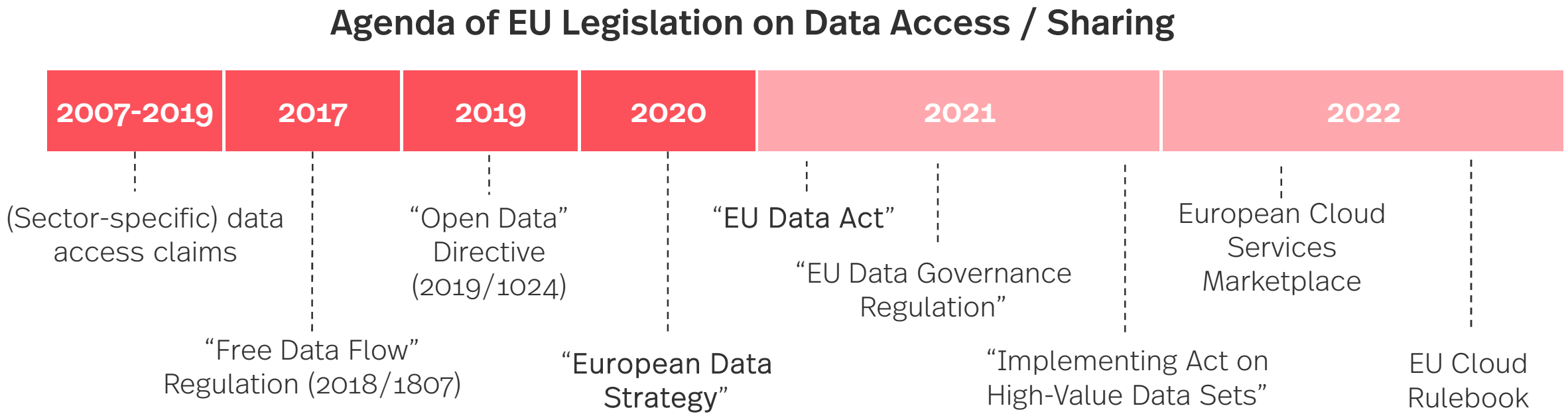
But:

Protection of Data

- Contractual law
- Database rights suis generis
- Business Secret Protection Act
- Criminal Code, inter alia,
  - data espionage, Sec. 202a
  - data tampering, Sec. 303a
  - computer sabotage, Sec. 303b

Data Sources

Data marketplaces in (forthcoming) EU legislation:



Questions?

Please contact us

Contact

Alexander Brown

Partner, Sector head - TMT
Simmons & Simmons LLP
E alex.brown@simmons-simmons.com

Sue Diver

Global Head of Information Governance
Simmons & Simmons LLP
E sue.diver@simmons-simmons.com

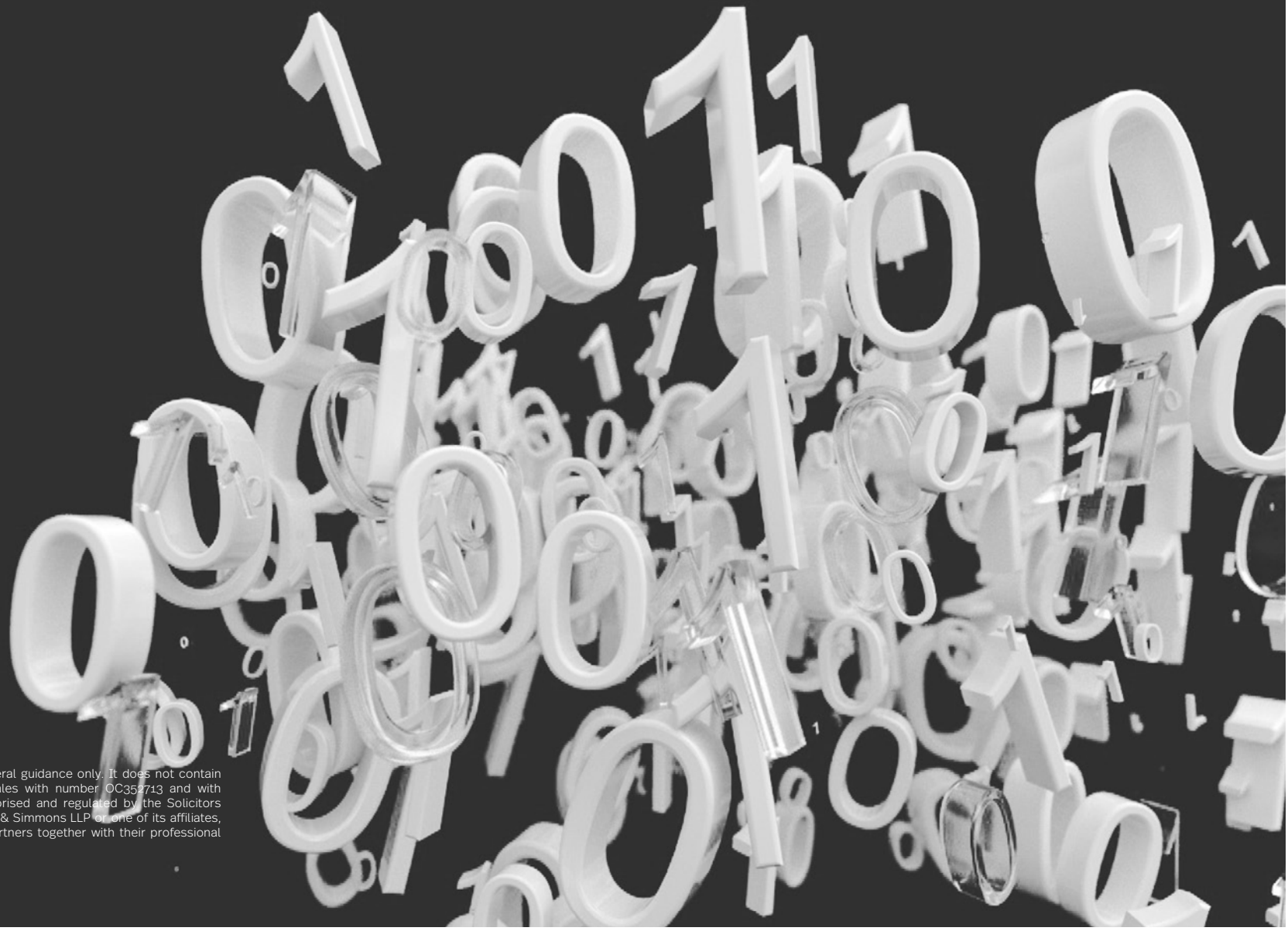
Christopher Götz, LL.M. (New York)

Partner, Head of Digital Business Germany
Simmons & Simmons LLP
E christopher.goetz@simmons-simmons.com

Peter Lee

Partner and CEO
Simmons Wavelength
E peter.lee@simmons-simmons.com

simmons+simmons



simmons-simmons.com

STRICTLY PRIVATE AND CONFIDENTIAL