

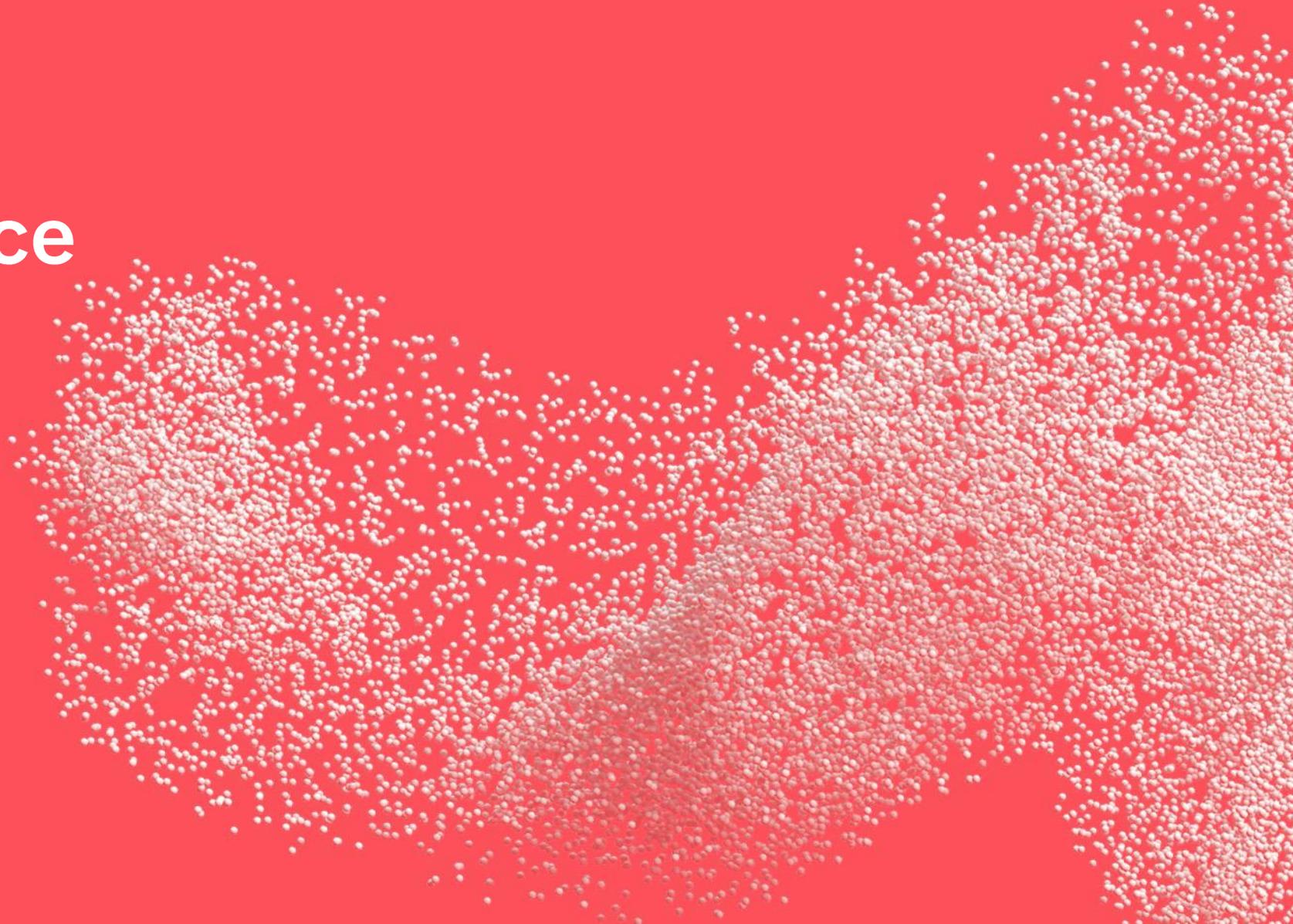
# The Big Data Race

5 November 2019



# The Big Data Race

Our survey





The Big Data Race is our review of the market's approach to data commercialisation.

Our global survey findings show what's necessary to successfully deploy a data commercialisation strategy and what the key success factors are.

They also enabled us to create a benchmark index that companies can measure themselves against.

# Demographics



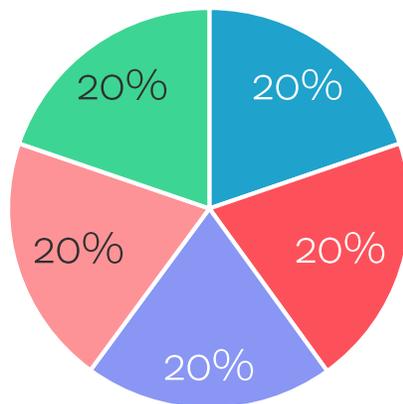
We surveyed 358 respondents

- 20% were part of the c-suite
- 80% were in senior roles

Global revenue in USD

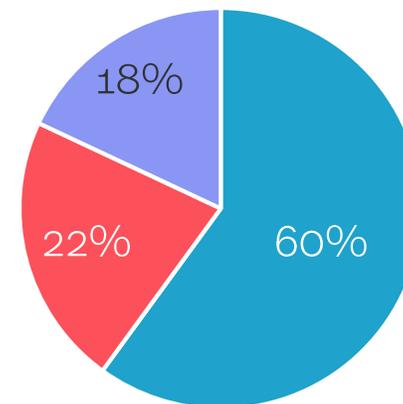


Regional break



■ US ■ UK ■ Western Europe ■ Middle East ■ Asia

Industry break



■ Technology ■ Media ■ Telecoms

# Big Data is transforming all sectors



## Financial Institutions



- Huge volumes of transaction and customer data
- New, sophisticated and personalised products and services
- Improved risk management

## Asset Management + Investment Funds



- Big data for high frequency trading
- Use of alternative data sources

## Healthcare + Life Sciences



- Improved patient-centric treatment and follow-up
- Improved diagnosis
- Prediction of epidemics

## Technology, Media + Telecommunications



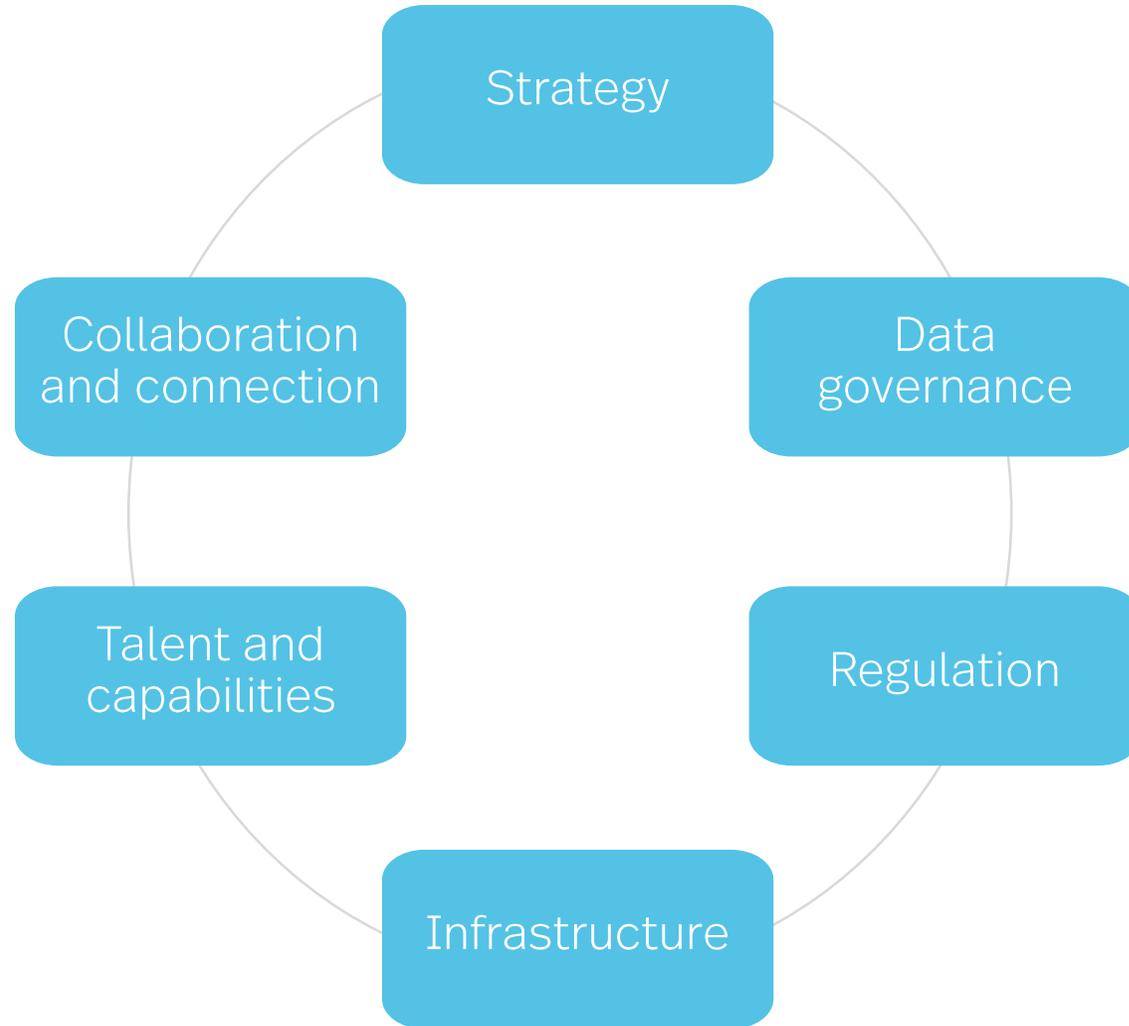
- Driving new technologies like AI + IoT
- “Understanding the customer”
- Predicting customer activity

# The Big Data Race

## Our findings



# Data commercialisation maturity framework



# Section 1

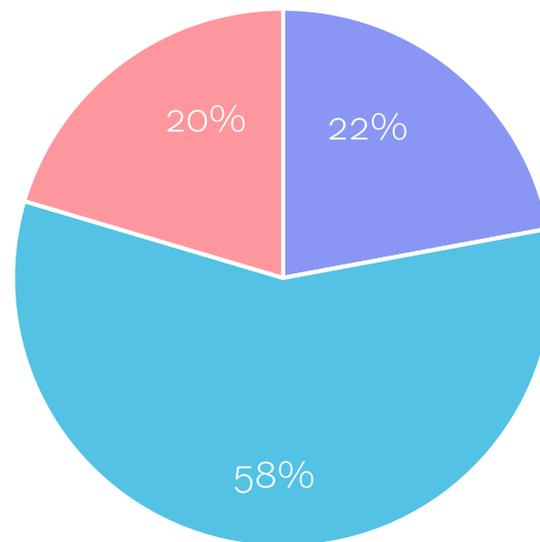
## Strategy

# Disjointed strategies



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

- 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



**45%**

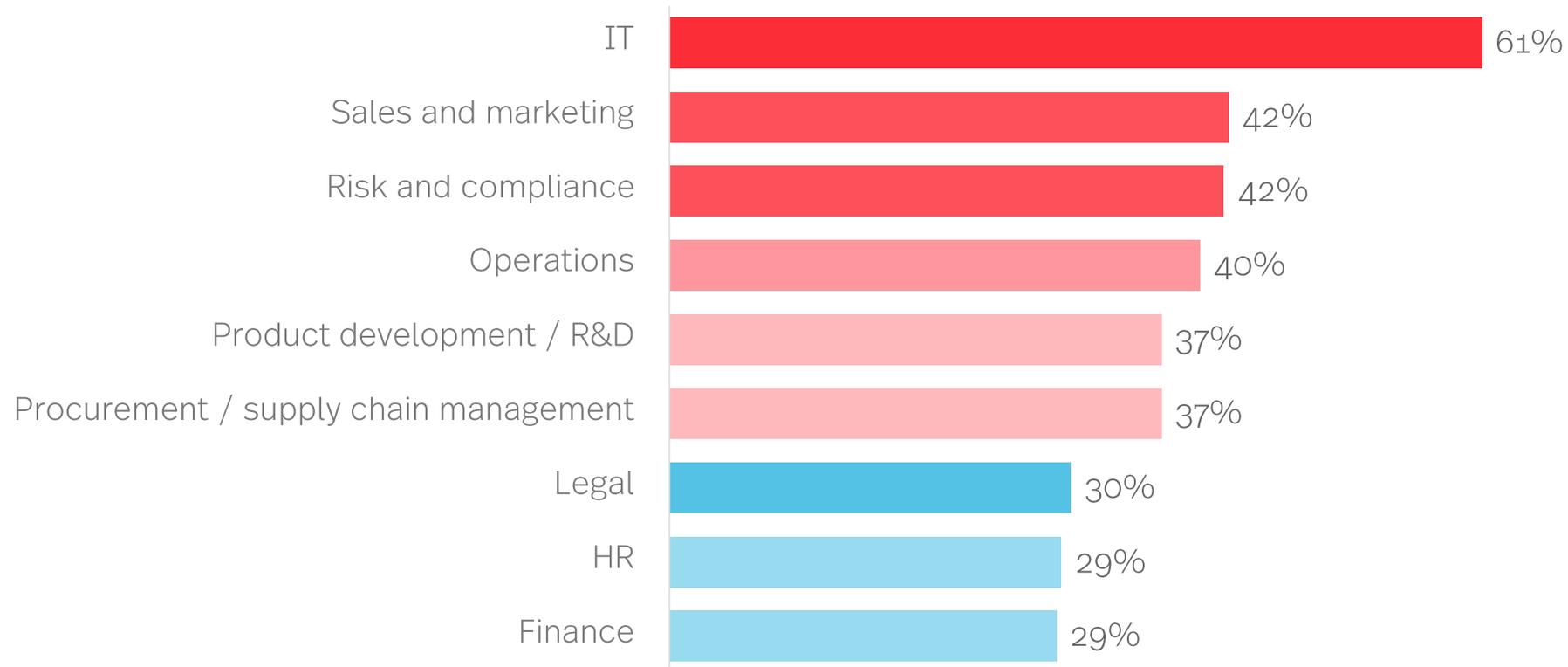
say that their data commercialisation strategy involves a certain amount of risk taking.

# An IT-centric approach



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

## High involvement in creating data commercialisation strategy

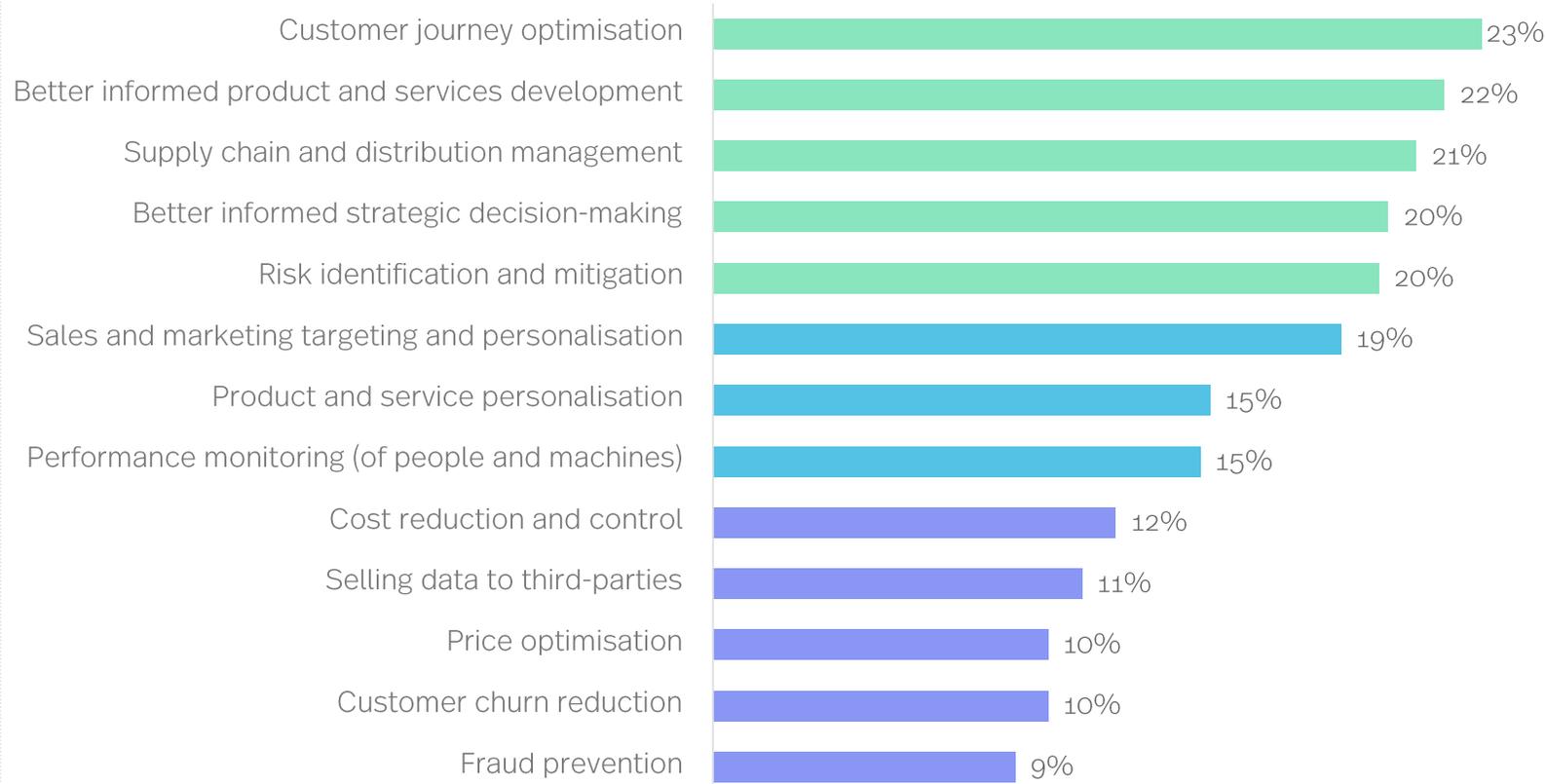


# Unfulfilled potential

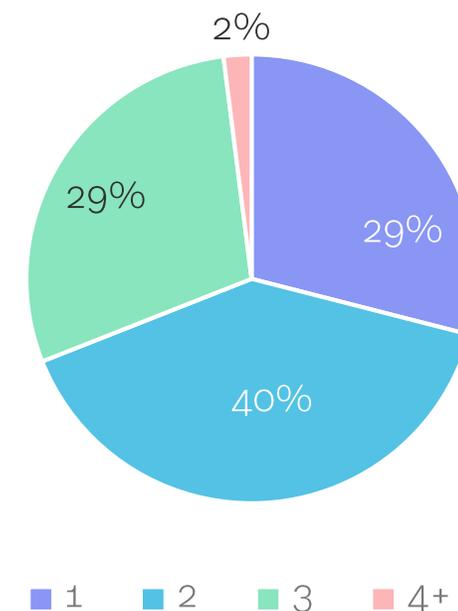


Most TMT companies only focus on a small number of data commercialisation objectives.

Objectives for data commercialisation



Number of data commercialisation objectives



## Section 2

### Data governance

# Governance: the foundation of data commercialisation



Those with an overarching data commercialisation strategy are more likely to have suitable data governance, but others may not.

**35%**

Our data governance is not fit for purpose in enabling data commercialisation

**38%**

There is not a clear set of procedures and standards that define which staff can access which data

**49%**

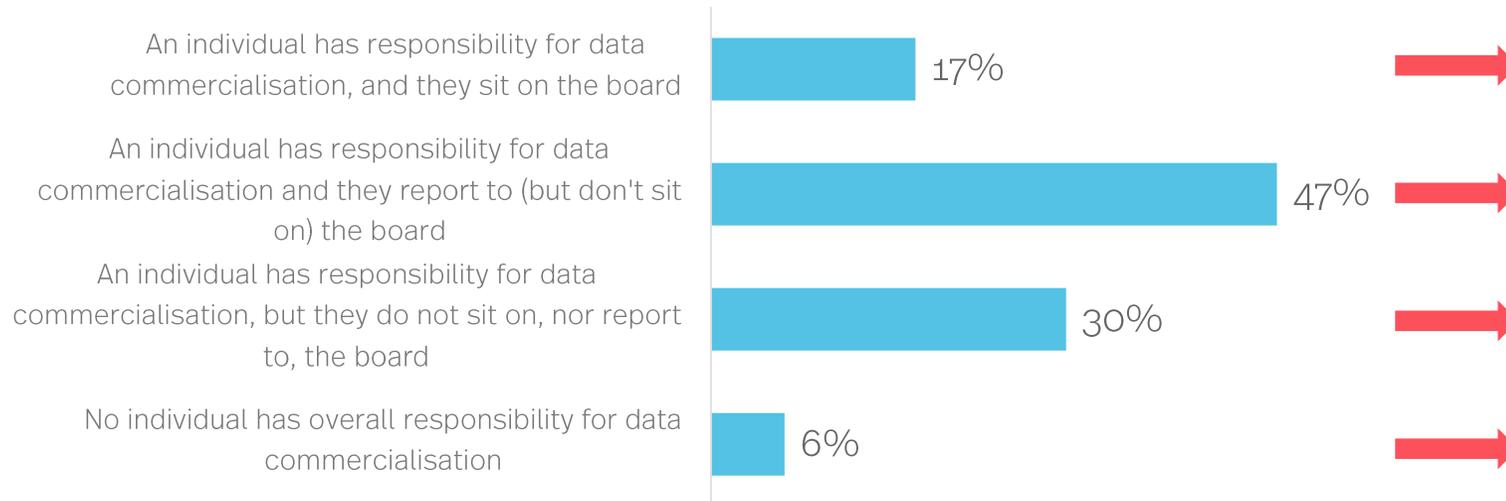
Individuals are not assigned data stewardship responsibility to oversee and enforce data compliance, accuracy and completeness

# Why data governance is not fit for purpose



64% of companies either have the relevant person sitting on the Board or reporting to the Board

## Responsibility for driving data commercialisation

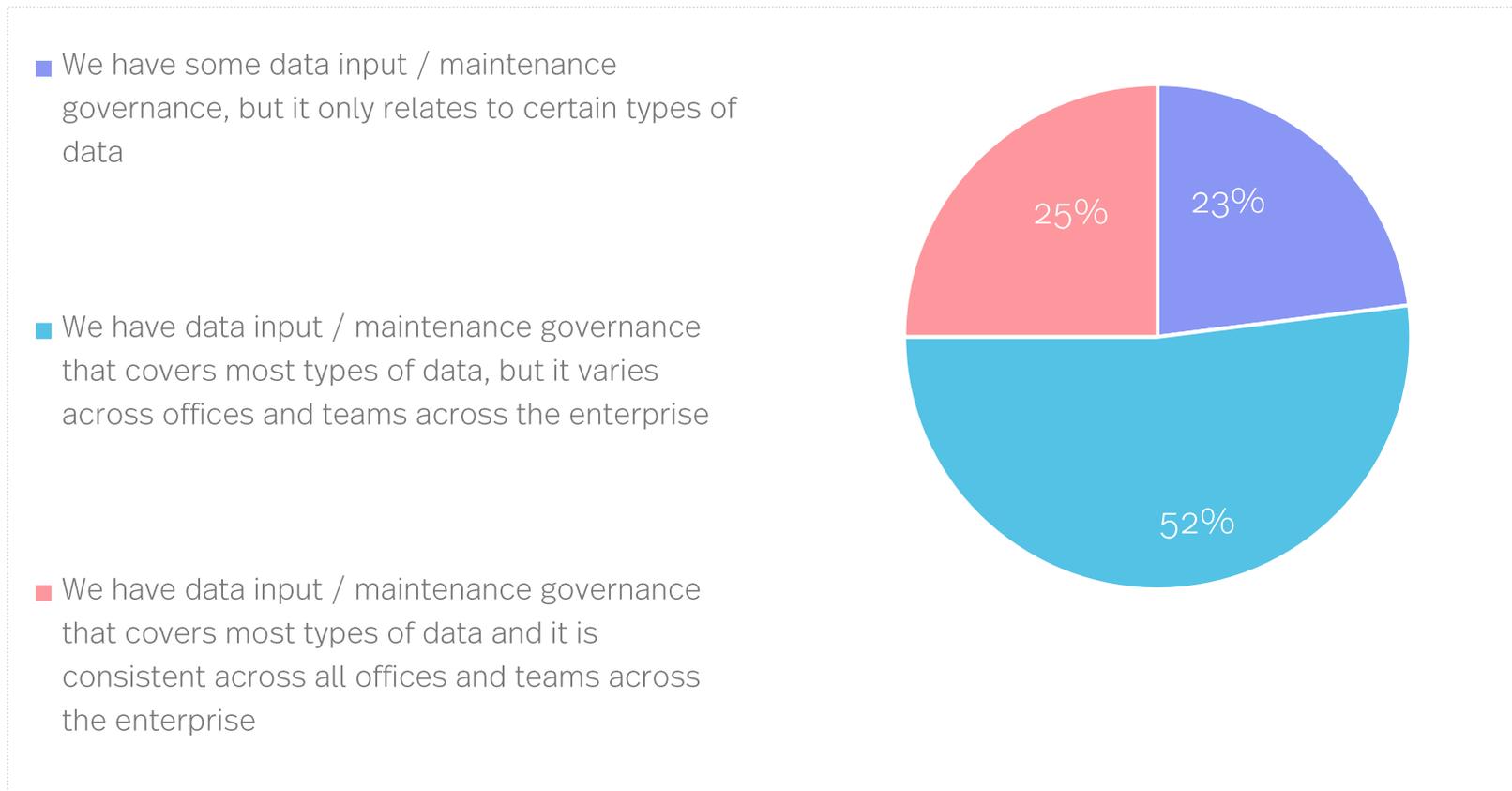


	No strategy	Overarching strategy
An individual has responsibility for data commercialisation, and they sit on the board	5%	34%
An individual has responsibility for data commercialisation and they report to (but don't sit on) the board	27%	48%
An individual has responsibility for data commercialisation, but they do not sit on, nor report to, the board	51%	15%
No individual has overall responsibility for data commercialisation	18%	3%

# Why data governance is not fit for purpose



75% of companies have a patchwork or incomplete approach to data input and maintenance governance



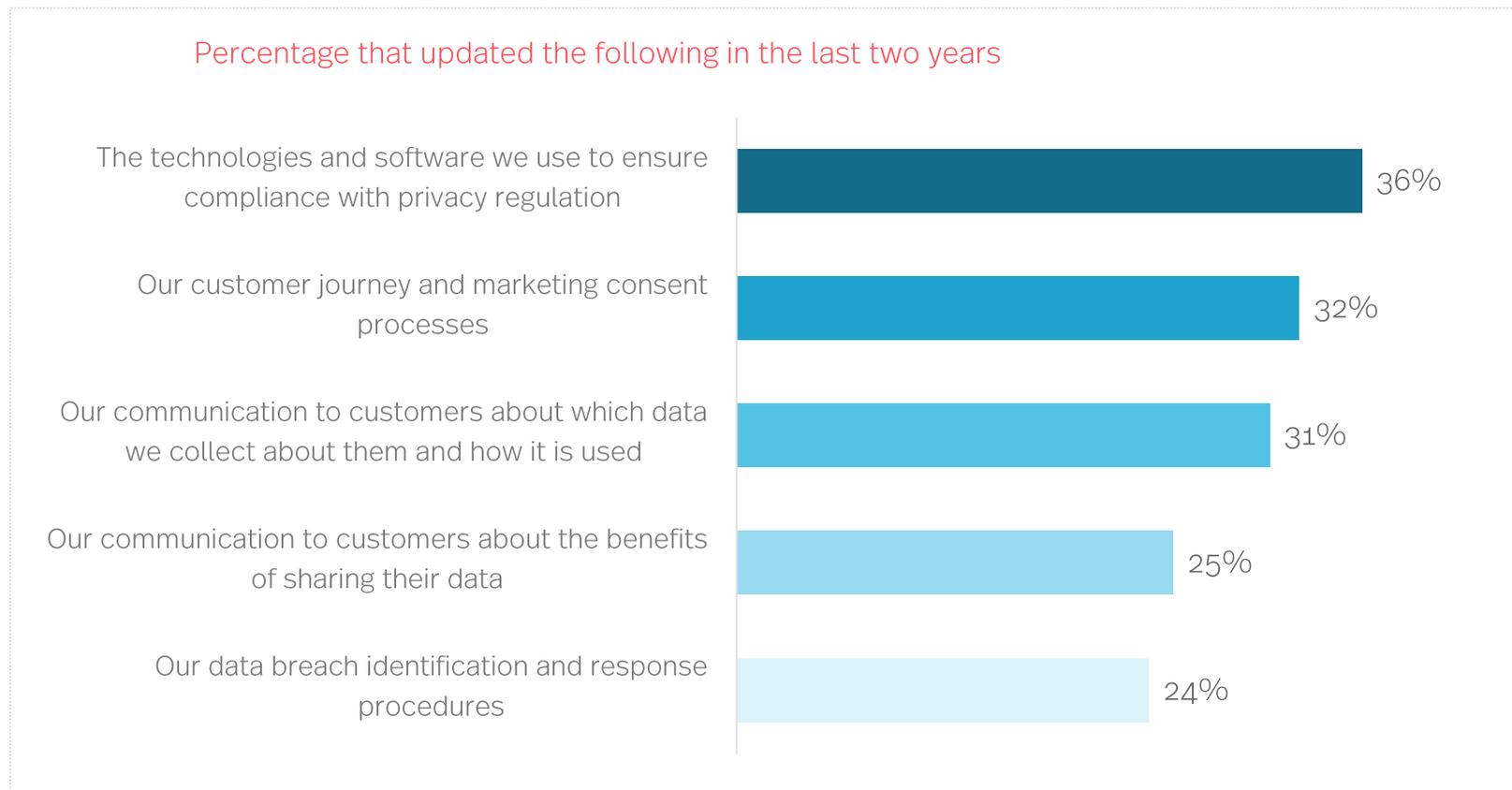
# Section 3

## Regulation

# Don't forget regulation

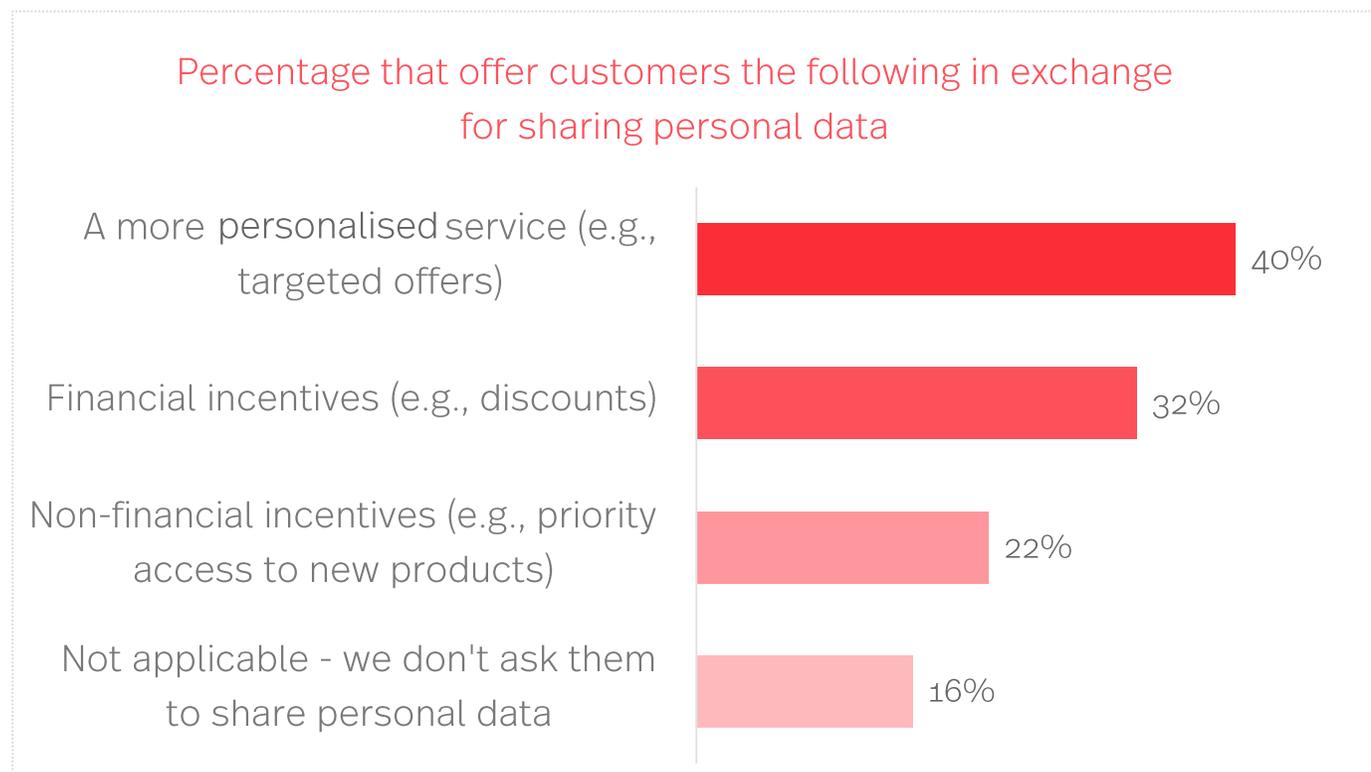


Only the minority of TMT companies have updated key data privacy and compliance technologies and processes in the last two years.



# Data commercialisation is still mostly about the company, not the customer

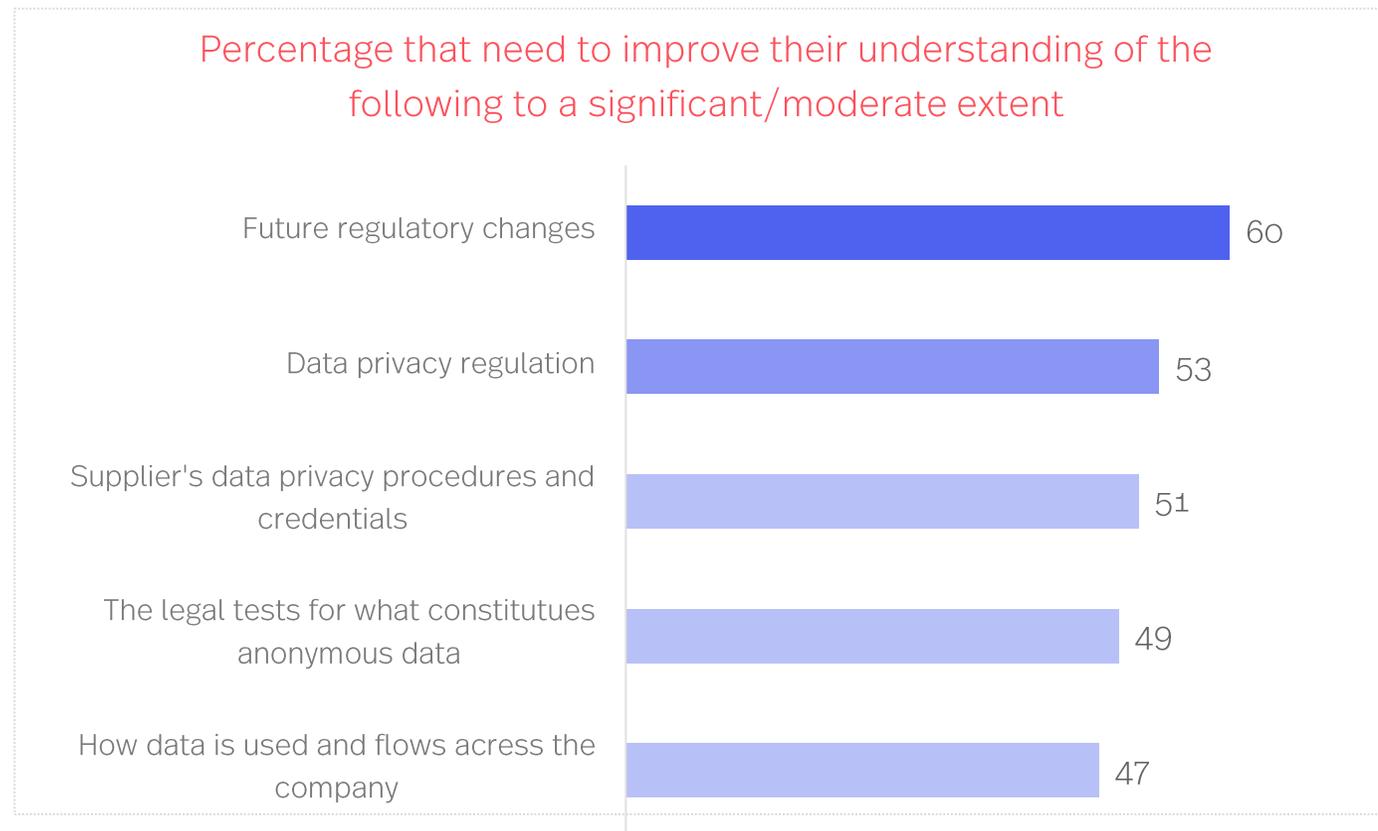
Most companies only offer one “incentive” for sharing personal data, and that is most commonly targeted marketing.



# The urgent need to bolster regulatory understanding



A significant proportion of survey participants need to improve their understanding of regulation relating to data commercialisation and how regulation might change.

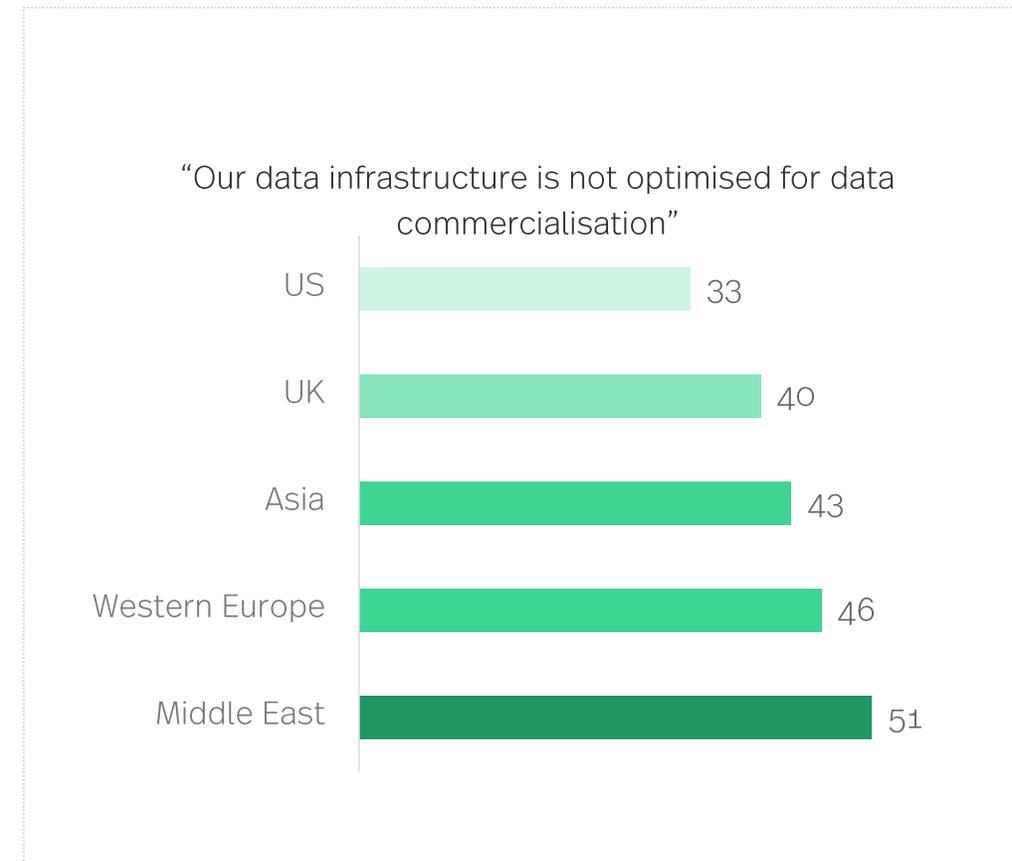
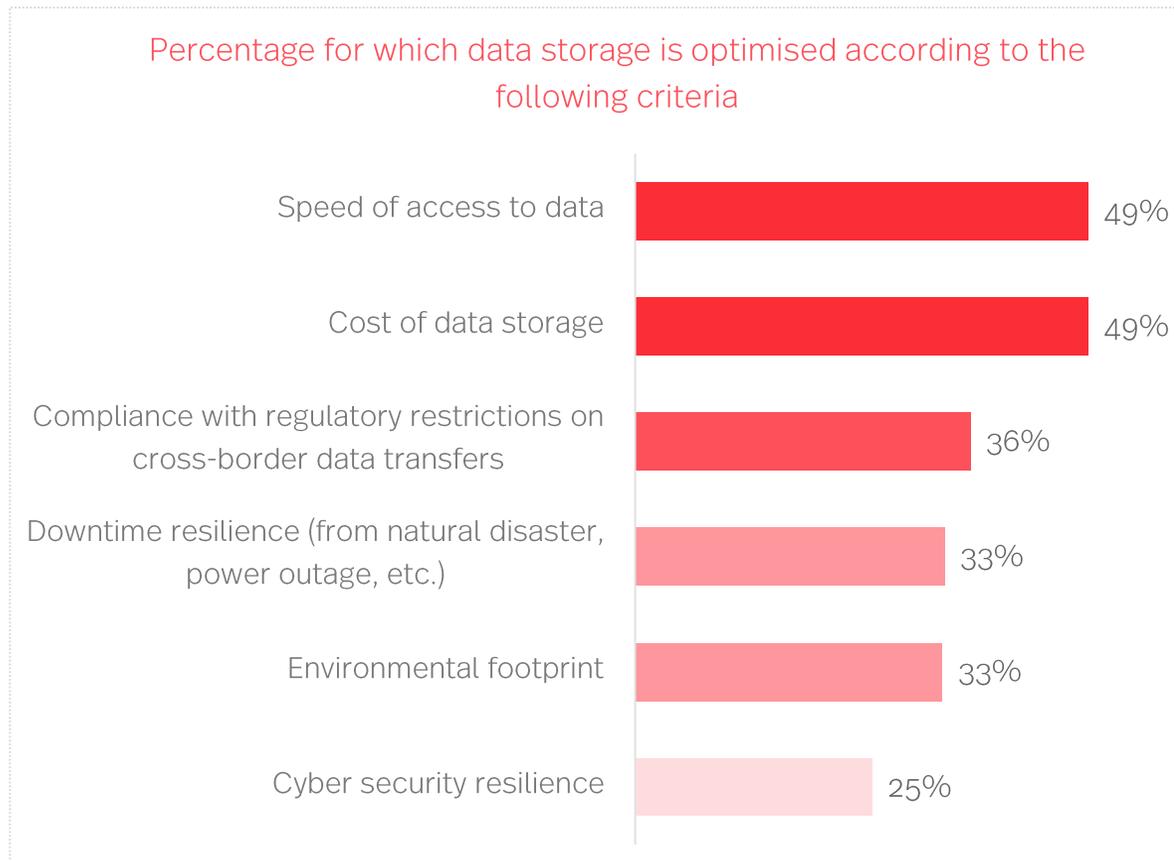


# Section 4

## Infrastructure

# Data storage priorities: fast and cheap

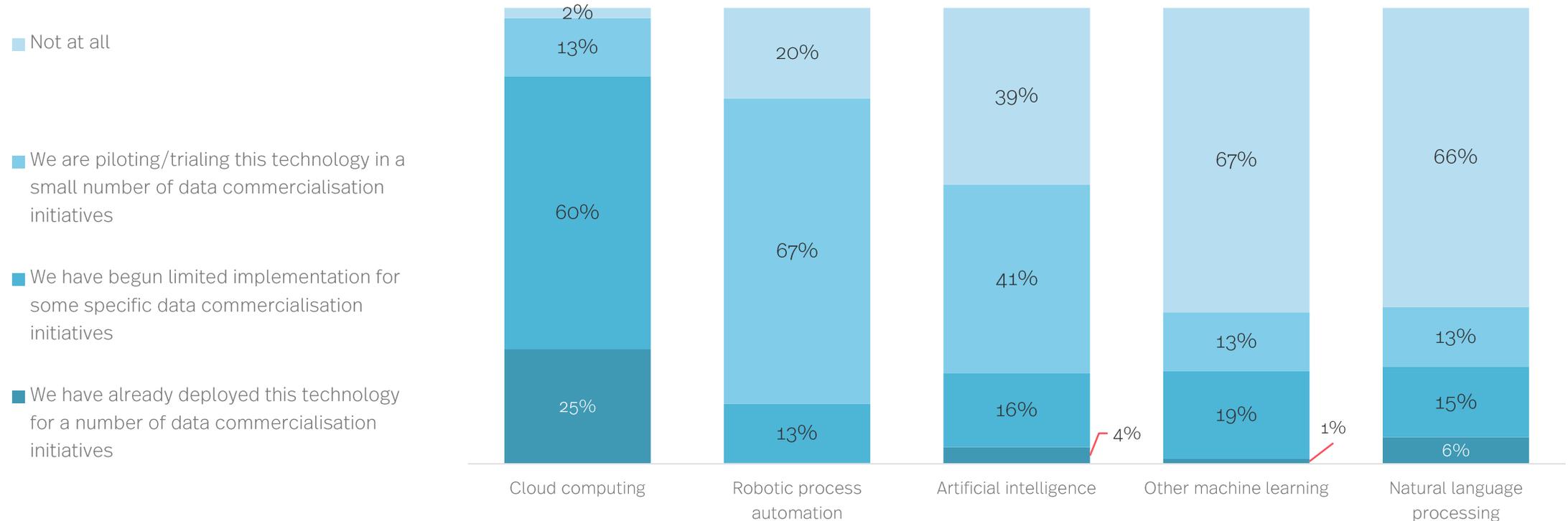
43% of participants say their data infrastructure is not optimised for data commercialisation. This is partly because data storage creates vulnerabilities and inefficiencies.



# The digital technology tipping point?

Use of advanced digital technologies for data commercialisation initiatives is limited, but changing. Large numbers are trailing/piloting RPA and AI.

Limited use of sophisticated digital technologies in data commercialisation



# Section 5

## Talent and capabilities

# A data-driven workforce



A large proportion (40%) of TMT 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

**45%**

executives at our company change their mind if the data makes a compelling case for doing so (55% won't change their minds vs 66% in the UK)

**31%**

executives DO NOT have the information they need to effectively manage the business

**66%**

Our company has launched special initiatives to recruit specialist skills needed for data commercialisation

**90% vs 42%**

Leaders are twice as likely to have the skills needed to meet their data commercialisation objectives

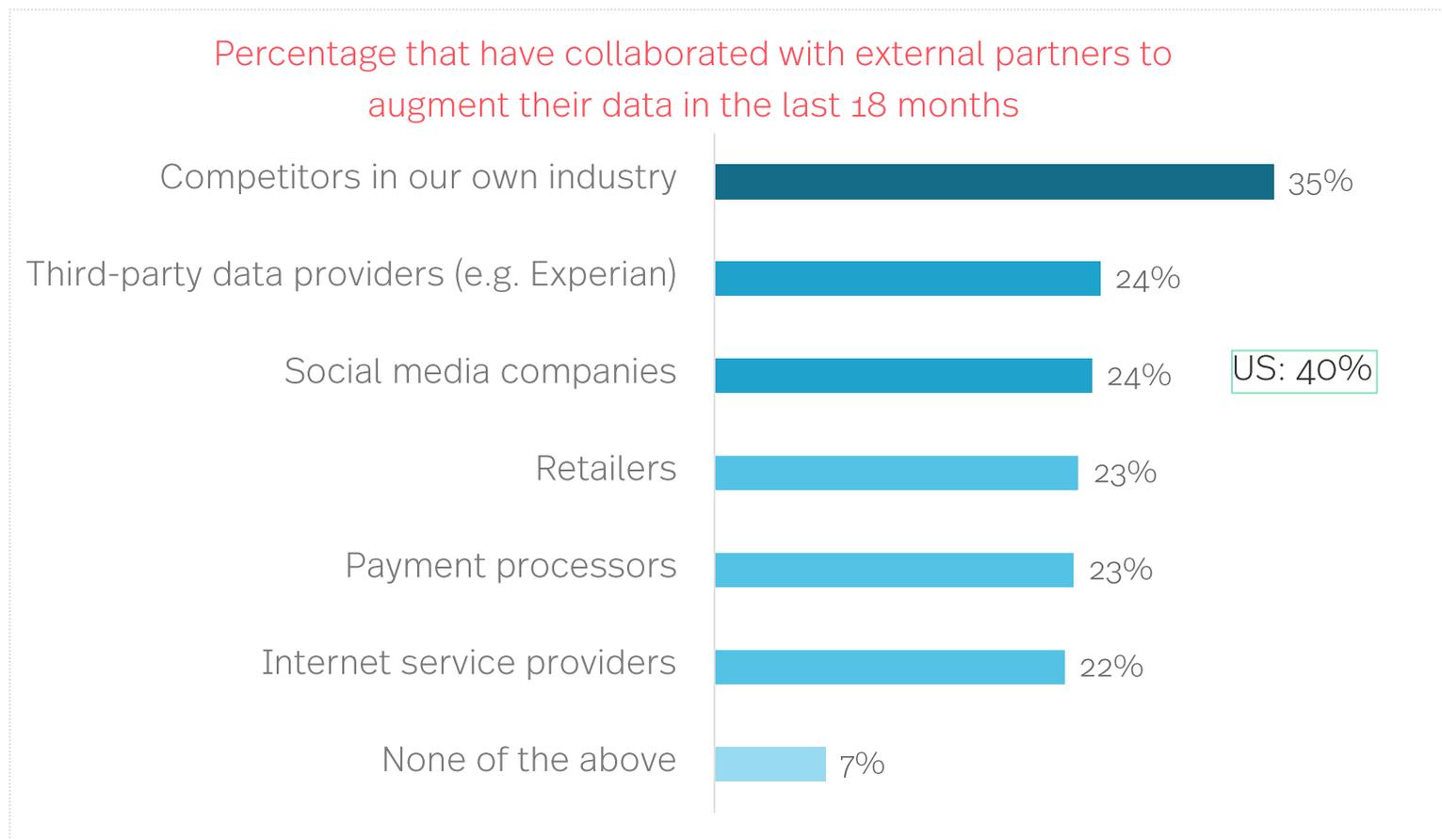
## Section 6

Collaboration and  
connection

# Competitors unite to augment data



But rarely collaborate with more than one type of organisation. Co-operation with social media companies is most prevalent in the US.



# Data remains siloed



Data and insights are not freely shared across the majority of enterprises. Devising an overarching strategy helps remediate this.

**50%**

'All business functions are **NOT** able to generate their own data driven insights using self-service data analytics tools'

**73%**

**CAN'T** access and use data collected by all areas of the business

**34%**

'Data libraries have **NOT** been established to help employees understand the information that is available to them'

**36%**

'The 'sensitivity' of data with respect to privacy, security, regulatory and ethical considerations is **NOT** considered when deciding which data is made available to functional teams'

# The Big Data Race

Our benchmarking  
tool



# Are you making the most of your company's data assets?



Assess and compare your own data maturity against the market with our new benchmarking tool.

**simmons**  
**simmons** The Big Data Race



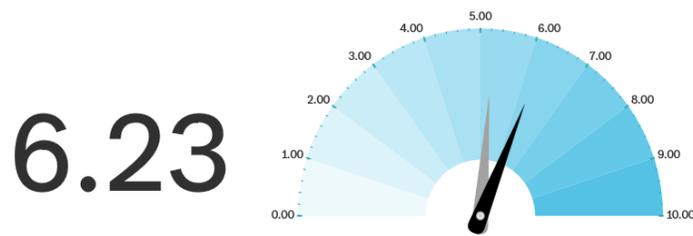
STEP 1 Strategy    STEP 2 Talent and capabilities    STEP 3 Regulation    STEP 4 Infrastructure    STEP 5 Data governance    STEP 6 Collaboration and connection    **STEP 7 Results**

## Your total score

We have sent an email to the address you specified with a link to these results.

Compared to most other companies, you are very advanced in your ability to realise commercial value from your data. You have widely adopted best practice on the fundamental pillars of data commercialisation and, while there remain a small number of areas where you can do more, you are well on the way to maximising the value of your data.

Discover how leading organisations are commercialising their data assets and pulling ahead in the Big Data Race. Visit our dedicated website [here](#).



The global average score is **5.24**

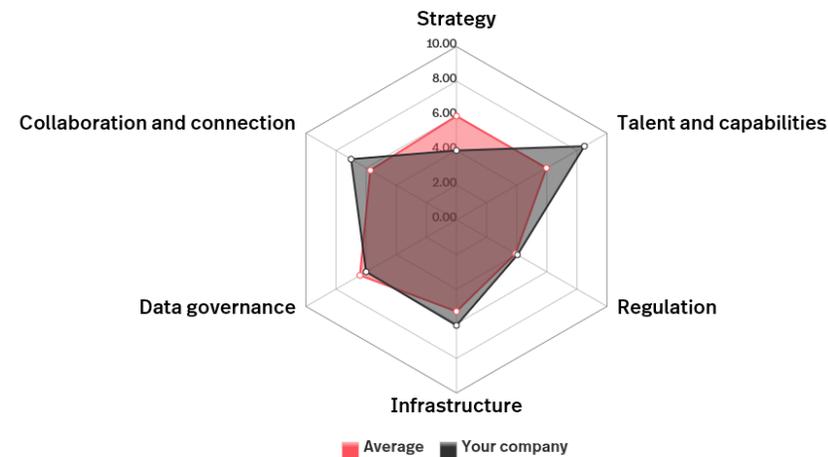
**simmons**  
**simmons** The Big Data Race



STEP 4 Strategy    STEP 2 Talent and capabilities    STEP 3 Regulation    STEP 4 Infrastructure    STEP 5 Data governance    STEP 6 Collaboration and connection    **STEP 7 Results**

## Compare your scores

**All**    Leaders / Laggards    Your sector    Your region



Share your score:

# The GDPR

Key takeaways after  
almost 2 years



# At European level

## EDPB guidelines



- Endorsement of GDPR WP29 Guidelines and related documents (25 May 2018)
  - Guidelines on consent under Regulation 2016/679, WP259 rev.01
  - Guidelines on transparency under Regulation 2016/679, WP260 rev.01
  - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01
  - Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01
  - Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01
  - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01
  - Guidelines on Data Protection Officers ('DPO'), WP243 rev.01
  - Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01
  - Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR

## Endorsement of GDPR WP29 Guidelines and related documents (25 May 2018)

- Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP 263 rev.01
- Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264
- Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265
- Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01
- Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01
- Adequacy Referential, WP 254 rev.01
- Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253

## Guideline 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 GDPR (4 June 2019)

- Aims to identify overarching requirements and criteria relevant to all types of certification mechanisms issued in accordance with Articles 42 and 43
- Relevant for variety of actors, ranging from national supervisory authorities, the Commission, the EDPB itself as well as data controllers and processors

## Guidelines 2/2018 on derogations of Article 49 under GDPR (25 May 2018)

- Interpretation of Article 49: derogations in the context of transfers to third countries
- When considering such transfers of personal data, exporters must provide certain guarantees
- Derogations must be interpreted restrictively
- Largely update the previous work of the WP29

## Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (12 November 2019)

- Criteria for determining territorial application of GDPR
- Illustrate various scenarios in which issues of territorial application may arise

## Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR (4 June 2019)

- Recognise that certification provides an authoritative statement of certification bodies, generating trust in the certification mechanism
- Provide guidance on how to interpret and implement the provisions of article 43
- The goal is to help Member States, supervisory bodies and national certification bodies establish a consistent and harmonised baseline for the accreditation of certification bodies

## Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under GDPR (4 June 2019)

- Clarify the rules and procedures for the submission, approval and publication of codes of conduct
- Set out content-related factors regarding the question whether a code actually contributes to the proper and effective implementation of the GDPR
- Set out the requirements for effective monitoring of compliance with the code

## Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (8 October 2019)

- Contracts for online services
- Outline the elements of lawful processing under article 6(1)(b) and considering the concept of “necessity”

# EDPB Guidelines



## Guidelines 3/2019 on processing of personal data through video devices (10 July 2019)

- Set out which uses of video devices may trigger GDPR application
- Reiterate the general rules of GDPR in relation to video devices: lawfulness, purpose limitation, processing special categories of data, transparency of the processing, storage periods and security measures.

## Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (13 November 2019)

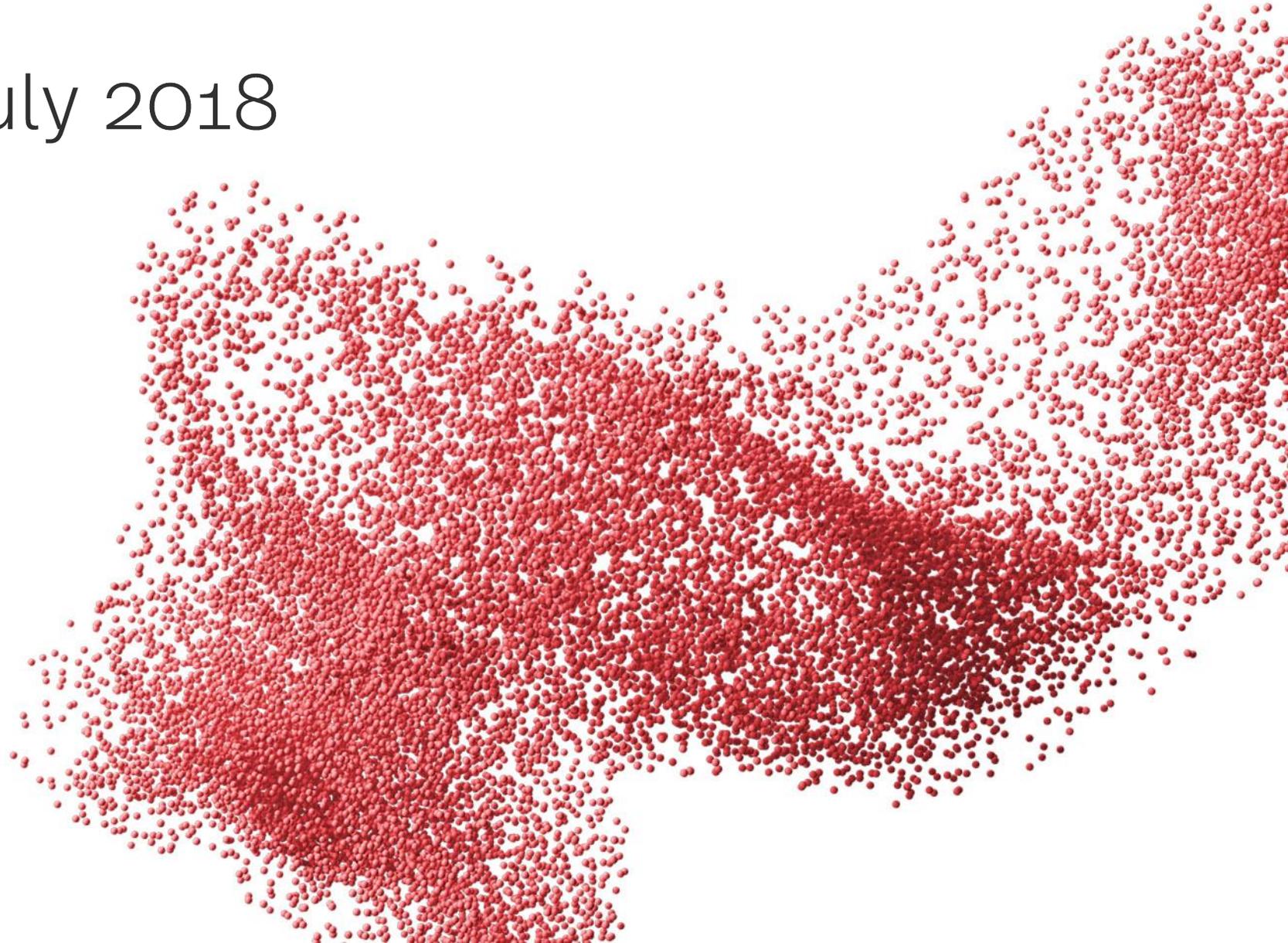
- Focus on the implementation of article 25 by data controllers
- Explain the legal obligations entailed by the principle and provide examples
- Possibility to establish a certification mechanism to demonstrate compliance
- Explain how those principles can be successfully enforced and implemented

## Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (2 December 2019)

- Background: CJEU Costeja González judgment of 13 May 2014
- Article 17 (3) GDPR: the right to be forgotten implies a right to request for delisting of links to webpages upon search of data subject
- Discuss the six grounds on which the request can be made
- Discuss the exceptions to the right to request a delisting

# At Belgian level

Belgian law 30 July 2018  
&  
BDPA



# Belgian Law of 30 July 2018



- Belgian Law of 30 July 2018 relating to the protection of individuals regarding the processing of personal data
- Entry into force as of 5 September 2018
- “Implements” some topics (“open clauses”) of the GDPR and repeals the previous Belgian privacy law of 8 December 1992 and its implementing royal decree of 13 February 2001

# Belgian Law of 30 July 2018



- Very bulky (286 articles); however:
  - Most provisions concern the processing of personal data by **public authorities**
  - Only a small part applies to **private entities**, and it does not impose many new obligations as regards to those under the GDPR
- Interesting provisions for companies include:
  - Processing of **genetic data, biometric data and data concerning health**
  - Processing for archiving purposes in the public interest, **scientific** or historical **research purposes** or statistical purposes
  - **Remedies & sanctions**

# Belgian Law of 30 July 2018



Processing of genetic data, biometric data and data concerning health

## GDPR (article 9(4))

Stipulates the possibility for Member States to introduce additional measures with regard to the processing of:

- genetic data,
- biometric data or
- data concerning health

## Law of 30 July 2018 (article 9)

Provides that the controller/processor must take the following additional measures when processing those data:

- List of categories of persons having access to those personal data + description of their function (made available to the DPA)
- Those persons must be bound by confidentiality obligations

# Belgian Law of 30 July 2018



Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

## GDPR (articles 5(1), b and 89)

- Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered as incompatible with initial purposes if it complies with **specific safeguards**
- Derogations from certain rights can be provided by Member States in so far as such rights are likely to render impossible or seriously impair the achievement of those purposes

# Belgian Law of 30 July 2018



Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

## **Law of 30 July 2018 (articles 186 to 208) – Safeguards include for example:**

- Appointment of a DPO when processing poses a risk to the rights and freedoms of individuals
- Obligation to include additional information in the records of processing activities (e.g. the public interest for archiving, the justification of (non-) coding of data, the reasons why the exercise of data subjects' rights would make impossible or would seriously impair the achievement of the purposes)
- Obligation to enter into specific agreement between the initial controller and the new controller
- Anonymising / pseudonymising of personal data

# Belgian Law of 30 July 2018



Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

- **Additionally:** Cascade system to anonymise / pseudonymise personal data, when processing for **research** or **statistical** purposes:
  1. Data should be anonymised (= impossible to re-identify)
  2. Failing that, data should be pseudonymised (= possible to re-identify with pseudonymisation key)
  3. Failing that, non coded data may be processed, provided that the non-anonymisation / non-pseudonymisation is justified in the record of processing activities

# Belgian Law of 30 July 2018



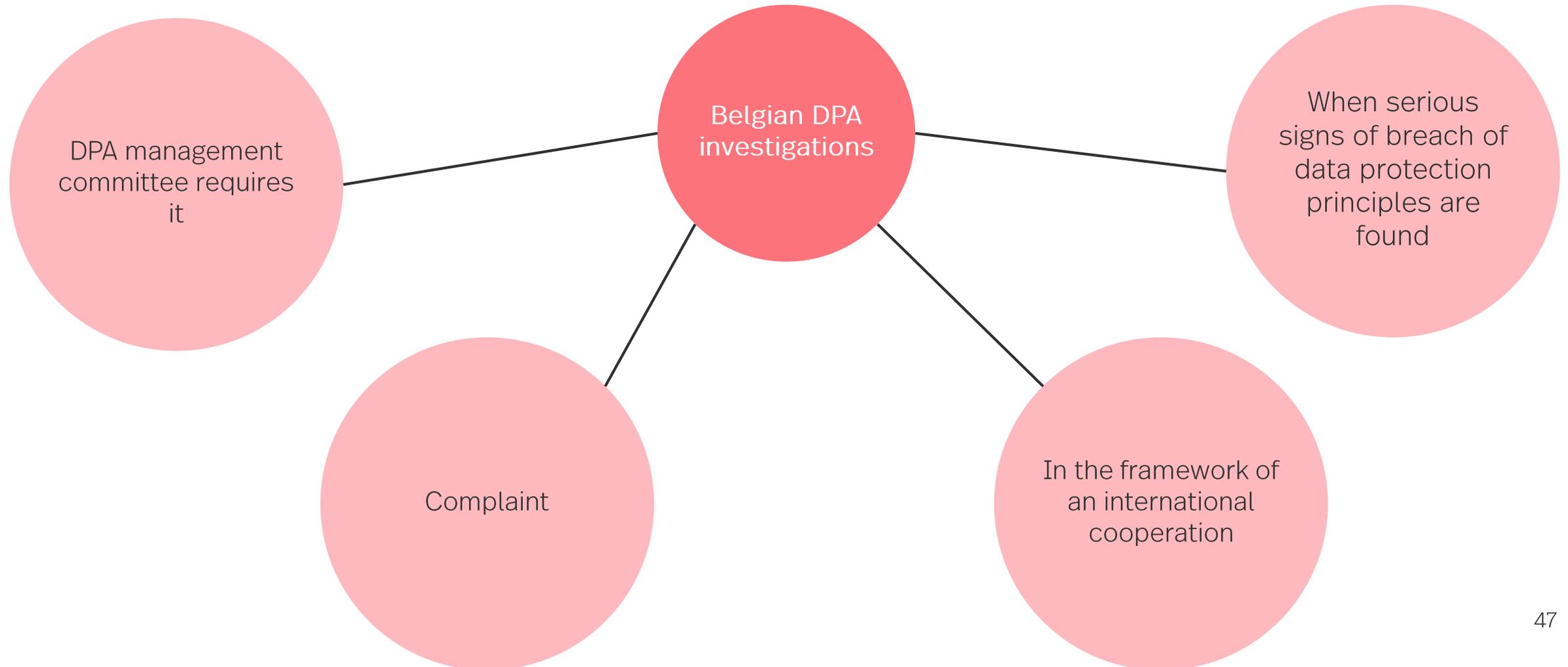
Belgian Law of 30 July 2018

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

- **Additionally:** Cascade system to anonymise / pseudonymise personal data, when processing for **research** or **statistical** purposes:
  - By **the first controller** of the data, before data are communicated to researcher
  - By **the researcher** if the researcher collects the data, but pseudonymisation key must be given to original controller
  - Further controller of data can not have access to pseudonymisation key
  - Anonymisation / pseudonymisation can be left to an **independent third party trustee**
  - Should occur **before analysing** the data

# Belgian Law of 30 July 2018

## Enforcement by the Belgian DPA



# Belgian Law of 30 July 2018

## Enforcement



### Remedies?

- Individual or DPA can lodge a legal action for injunction in case of breach
- Following an action for injunction, individual can also claim damages (through contractual or tort liability)

### Sanctions?

- In case of breach, the corrective powers of the DPA apply
- Significant administrative fines in GDPR: up to 20 million euros or 4% of the annual turnover
- In addition to administrative fines, the Law also provides for criminal fines from €8,000 to €240,000 (for individuals and/or companies)

## Key accomplishments

- Recommendations
- Decision of the General Secretariat no. 01/2019
  - List of cases subject to **mandatory DPIA's**
- First decisions on the merits:
  - Fine of **2,000 EUR** for non-compliance with some data subject rights (access and deletion)
  - Fines of **2,000 and 5,000 EUR** (use of personal data for another purpose)
  - Fine of **10,000 EUR** (for imposing the use of the ID card for a fidelity card)
  - Fine of **15,000 EUR** (for lack of information relating to cookies)
  - Several **reprimands**
  - **Imposing measures** to comply with GDPR obligations (e.g. compliance with data subjects' rights)
  - **Prohibition to process** data obtained with a camera

## Draft Strategic Plan

- New strategic plan for 2019-2025 (draft subject to consultation until 07 January 2020 – final version to be released soon)
- Clarifies the tasks, resources, organisation, vision, mission and values of the BDPA
- Set 3 categories of “**priorities**”:

### I. Relevant sectors

- Telecommunication & Media
- Public authorities
- Direct Marketing
- Education
- Small and medium-sized companies

### II. GDPR instruments

- Role of the DPO
- Lawfulness of the processing
- Rights of citizens (access, rectification, transfer of personal data...)

### III. Societal topics

- Pictures and cameras
- Online data protection
- Sensitive personal data

## Draft Strategic Plan

- In addition to the priorities, the Belgian DPA sets out **six strategic objectives** it wants to achieve:
  - Improved data protection through **awareness raising**
  - Improved data protection through **enforcement**
  - Improved data protection by **identifying and addressing certain evolutions** (e.g. AI, blockchain, data mining, facial recognition, etc.)
  - Improved data protection through **collaboration**
  - Improved data protection with **the DPA as a guide/leader and as centre of reference**
  - Improved data protection by **(internally) being a more efficient supervisor**

# Some key figures to conclude...

## In Belgium (compared to 2017)

- Complaints and requests + 67.73%
- Written information requests + 21.19%
- Requests for advice + 113.33%
- Data breach notifications + 3,527.27%

(Source: BDPA Draft Strategic Plan)



## In the EU (since 25 May 2018)

- Total fines: **Quiz!**
  - Top 3: FR, GE, AUS
  - No fine in Ireland yet!
- Total data breach notifications: **Quiz!**
  - Top 3: **Quiz!**

# Some key figures to conclude...

## In Belgium (compared to 2017)

- Complaints and requests + 67.73%
- Written information requests + 21.19%
- Requests for advice + 113.33%
- Data breach notifications + 3,527.27%

(Source: BDPA Draft Strategic Plan)



## In the EU (since 25 May 2018)

- Total fines: 114m EUR (incl. 50m EUR for Google)
  - Top 3: FR, GE, AUS
  - No fine in Ireland yet!
- Total data breach notifications: 161,000
  - Top 3: NL, GE, UK

**Thank you!**  
**Any questions?**



# Contacts

## Brussels office



Jérémie Doornaert

Managing Associate

T +32 2 542 09 79

E [jeremie.doornaert@  
simmons-simmons.com](mailto:jeremie.doornaert@simmons-simmons.com)



[simmons-simmons.com](https://simmons-simmons.com)

**STRICTLY PRIVATE AND CONFIDENTIAL**

© Simmons & Simmons LLP and its licensors. All rights asserted and reserved. This document is for general guidance only. It does not contain definitive advice. Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word "partner" refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.