OLIVER WYMAN

TECC

# THE APPROPRIATE USE OF CUSTOMER DATA
## HIGHLIGHTS FROM OUR WORK TO ESTABLISH GLOBAL PRINCIPLES

APRIL 11, 2019

Tom Ivell
Subas Roy



MARSH & McLENNAN COMPANIES

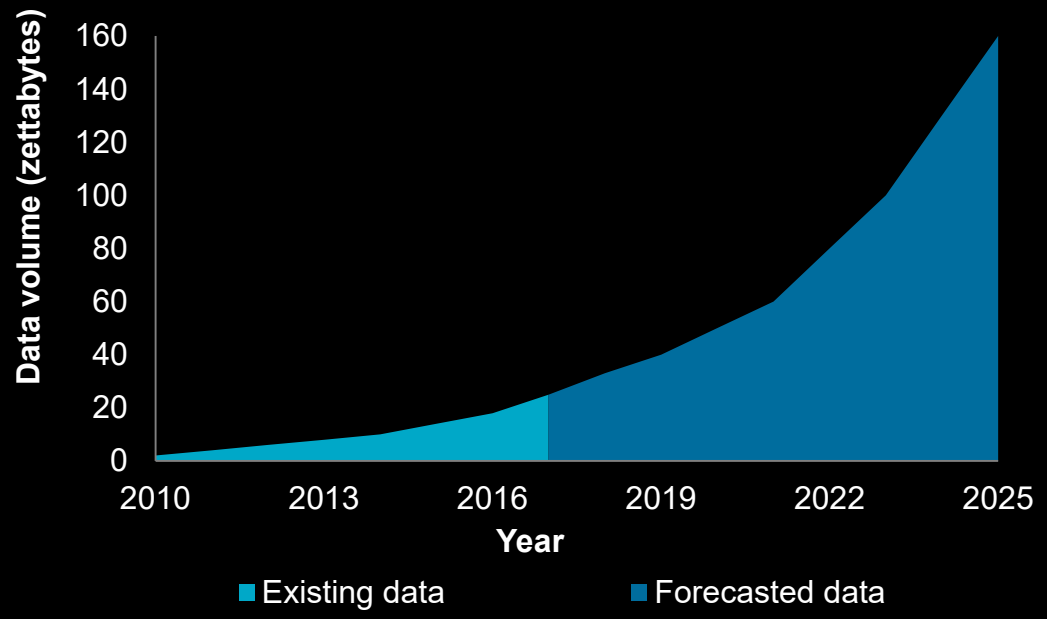
# CONFIDENTIALITY

Our clients' industries are extremely competitive, and the maintenance of confidentiality with respect to our clients' plans and data is critical. Oliver Wyman rigorously applies internal confidentiality practices to protect the confidentiality of all client information.

Similarly, our industry is very competitive. We view our approaches and insights as proprietary and therefore look to our clients to protect our interests in our proposals, presentations, methodologies and analytical techniques. Under no circumstances should this material be shared with any third party without the prior written consent of Oliver Wyman.

# Transformation of technology, consumer behaviour, and data science has exponentially increased the amount and types of customer data available to firms

## The amount of data collected has increased…




## …and the types of customer data collected have expanded

| | Traditional forms | Emerging forms |
|---|---|---|
| **Identity** | Public records, tax filings | Fingerprints, photographs, iris scans, digital IDs |
| **Health** | Medical records, insurance claims | Fitness tracking, sleep/eating habits |
| **Financial** | Bank statements, credit scores | Peer-to-peer payments, online budgeting |
| **Social** | Organization registries | Social media connections and activities |
| **Location** | Telephone books | Geolocation tracking |
| **Media behaviour** | Library checkout histories | Web browsing activities, content streaming |

Every **2** days we create more data than we did across the **20th century**

Certain marketing companies have **about 1,500 data points** on approximately **96%** of US citizens

**95%** of the top free mobile apps collect customer data (location, social networks, etc.)

Source: The Digitization of the World From Edge to Core (Seagate & IDC, 2018)

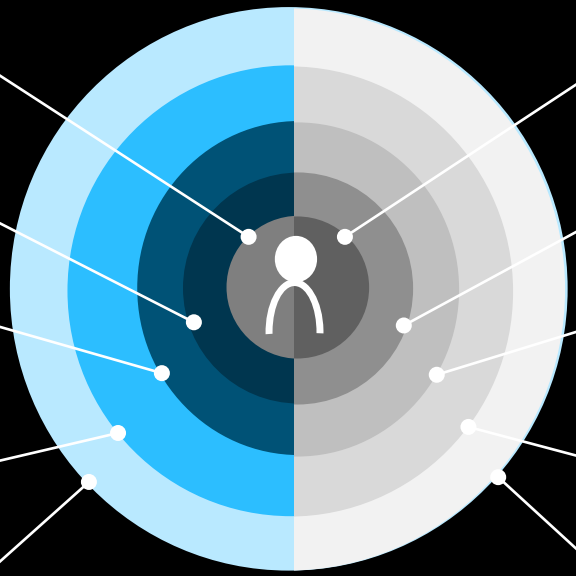
# Banks are reorienting their strategies and business models around data as an essential asset

| | Role and description | Potential crown jewels | Players that might have an advantage |
|---|---|---|---|
| **Platform provider**  | Aggregates and curates customer demand information and (component) supply information for the ecosystem | • Privileged access to customer information<br>• Privileged access to business information<br>• Expertise in modern data aggregation and synthesis | • Google, Facebook<br>• Amazon, Alibaba<br>• Banks with “whole wallet” customer relationship<br>• Industry data aggregators |
| **Demand aggregator**  | Engages directly with customers, surfaces options and facilitates decision-making | • Customer trust<br>• Customer reach<br>• Deep know-how in the spectrum of financial needs and products<br>• Experience design, informed by human insights and customer journeys<br>• Algorithm development to support the above | • Banks and insurers with high customer trust |
| **Component supplier**  | Delivers a specific “product” or capability when triggered by a specific need | • Highly efficient product factory<br>• Readily able to plug-in to demand aggregators’ solutions<br>• Able to adapt the product or capability to new information surfaced by the LifeMap<br>• Modern software engineering and architecture capability (using modern APIs, cloud services, et al) | • Large “monolines”, by geography<br>• Insurance carriers<br>• Fintech specialists |

# Digitisation improves customer centricity, but has to be complemented by risk management

**Business Growth & Competitive Advantage**

- Better Customer experience
- Better products & services
- Transparency
- Integrated Business models
- Competition



**Digital Transformation in Risk Management**

- Customer focus
- Products & services
- Policy & governance
- Monitor behaviours, conduct
- Traceability of actions

**Customer centricity** — **Customer trust and satisfaction**

# The risks associated with customer data could undermine the trust that is essential to financial system stability

**Customer –** *Appreciate that data about them help to create tailored products and services, but concerned about privacy and other risks from data misuse*

- ✓ New products and services tailored to individual needs
- ✓ Enhanced customer experience
- ✓ Financial inclusion for underserved individuals
- ✗ Financial losses due to fraud
- ✗ Loss of privacy if data are used without consent
- ✗ Exclusion from products or services due to real or perceived risks


**Business –** *Enthusiastic to leverage customer data to generate insights and profit, but unclear how to adapt to changing regulations and public sentiment*

- ✓ Development of new products and services
- ✓ Better risk management capabilities
- ✓ Cost savings from more efficient internal operations
- ✓ Opportunities to strengthen customer relationships
- ✗ Regulatory penalties or reputational damage from misuse of customer data (loss of customers)
- ✗ Operational losses from fraud or cyberattacks
- ✗ Market disruption for companies that depend on pooled risk or cross-subsidization

**Government –** *Eager to spur innovation and growth, but mindful of risks to customers that may weaken trust in the financial system*

- ✓ Clarifying expectations can encourage responsible and prudent innovation
- ✗ Imbalanced or poorly crafted policies can chill investment
- ✗ Uncoordinated policy within or across countries can burden firms
- ✗ Regulatory and oversight gaps can expose customers/firms to “bad actors”

There is significant opportunity for policymakers to articulate clear principles to govern the use of customer data to manage these risks

# Lack of clarity about how to define and enable data “ownership” challenges the development of an effective data governance framework

## Traditional concepts of “ownership” do not fit data well…

✗ **Data is intangible**

- It cannot be physically held or handled, as a car or computer can

✗ **Data can have multiple “owners”**

- A piece of data can be legitimately held by multiple entities at any given time
- Data is a non-binary good, so enabling multiple parties to possess and use the same data does not necessarily undermine its value

✗ **Customer data that is most valuable today is more personal, and therefore more sensitive, than ever before**

- Highly-detailed information about individual preferences and behaviour enables customization, but also increases our interest in protecting privacy and strengthening consumer control over how that data is used

## …instead, conceptualizing usage rights as a bundle of interrelated rights may provide a more effective framework

**Examples of usage rights (not exhaustive)**

- Right to know the information in the first place
- Right to retain it for extended periods
- Right to use it to make decisions
- Right to sell or otherwise transfer the data
- Right to make the data public

# Views about appropriate usage norms are still evolving

## Rapid changes in data use

- Increasingly diverse types of data are being used in increasingly complex ways
- Financial services data usage has potential to deliver “win-win” for key stakeholders, unlike some of the data debates focused on social media and other tech businesses

## Changing public opinion

- Widely-publicized data breaches and data collection scandals involving social media platforms have raised awareness of privacy risks and inability of consumers to control data usage
- Lack of consumer sophistication about how data is being used and how behaviour can affect access to products and services, among other issues, in the future

## Differences across nations

- Differing cultural norms relating to privacy shape each jurisdiction’s policy-making constraints and opportunities
- Challenge of – and need for – cross-border coordination heightened

# Our work to date

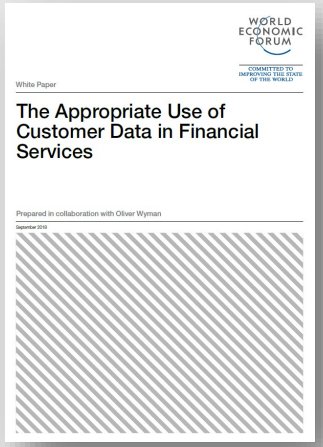
## Work to date

### Principles

- Conducted **40+ interviews** with subject matter experts on **principles for the appropriate use of data**
- Developed **principles** through working group meetings in **Singapore and New York,** along with individual stakeholder interviews

### Governance

- Reviewed **current state** of standards, regulations, oversight and supervision across regions for data use and ownership
- Developed set of **suggested next steps for implementation of principles and explored potential trade-offs**




*A detailed summary of working group findings, principles, and next steps can be found in the recently published white paper, "The Appropriate Use of Customer Data"*

# Stakeholders aligned on five key principles, opining on topics like portability and the underlying conditions for the appropriate use of customer data

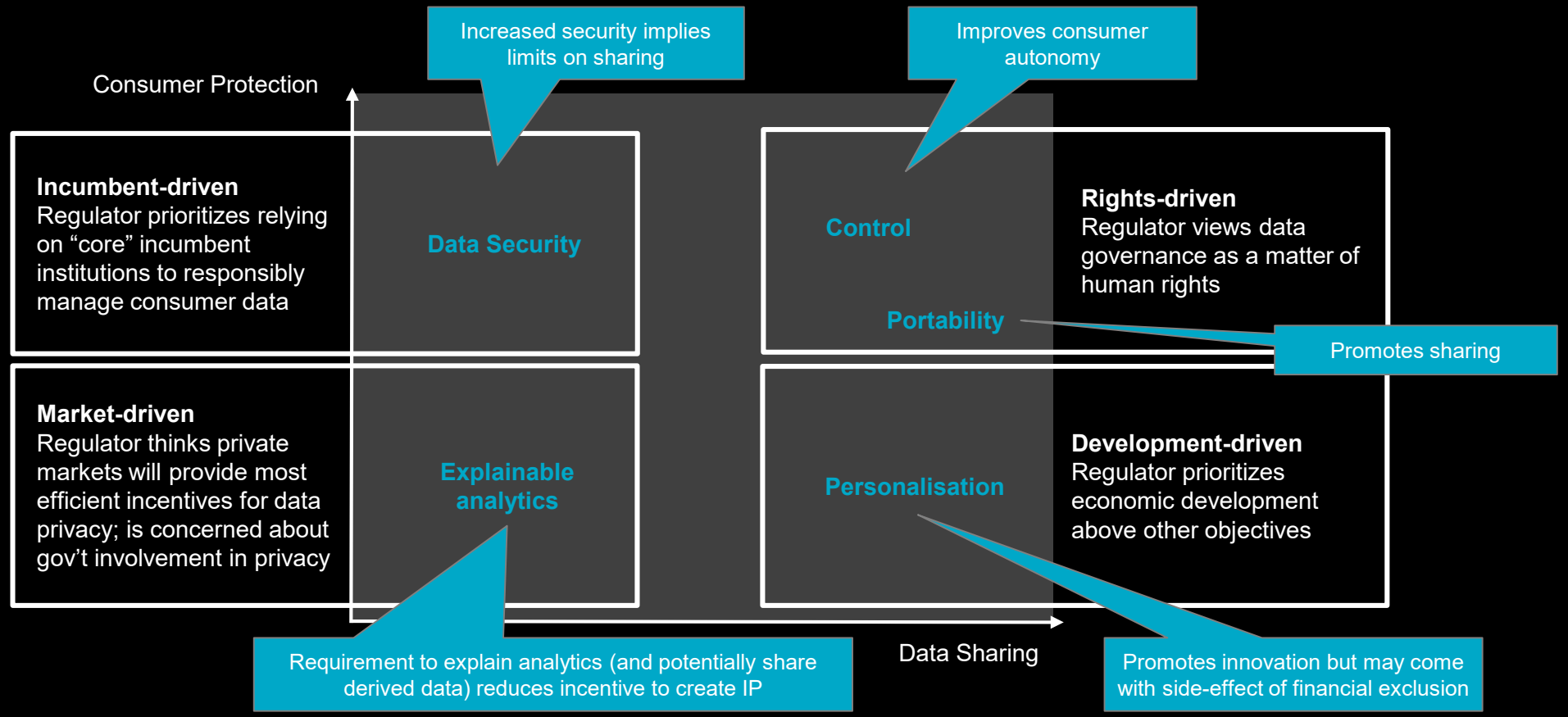
**5 Key Principles of Data Governance**

| | |
|---|---|
| **Control** | ***"Companies should be clear about their use of customer data, attain customer agreement to their customer data policies and, where appropriate, seek consent for specific uses."*** |
| **Security** | ***"Companies should be held responsible and accountable for data security."*** |
| **Personalization** | ***"Companies should be able to create individual customer-level profiles that allow them to provide differentiated customer services."*** |
| **Advanced analytics** | ***"Companies should be able to comprehensively test, validate and explain their use of data analytics and models to customers."*** |
| **Portability** | ***"Companies should, where appropriate, allow customers to access, download, transfer and/or permit third parties to manage data about them."*** |

Simple? Not quite…

# Policymakers are likely to place different importance across these principles

## Simplified framework for mapping policymaker objectives




We can therefore expect significant geographic differences resulting from policymaker priorities

# There also remain important trade-offs within each of the principles

## Control

- **Customer autonomy vs. effective anti-financial crime measures:** E.g. creation of a single client view in an effort to combat financial crime may not be possible due to banking secrecy regulations.
- **Consent requirements vs. customer experience:** Consumer behaviour and preferences do not necessarily match; current consent mechanisms are often time meaningless.
- **Access vs. protection:** Fee-based models might exclude those unable/unwilling to pay for services that companies currently offer for free.

## Security

- **Innovation ability vs. system integrity:** Effective cyber security controls can overburden young start-ups; lax requirements threaten the security of customer data and the integrity of the larger financial system.

## Personalization

- Debate **on limitations for specific data uses** and questions over whether societal checks should be made on outcomes (e.g. requiring basic provision of insurances services for all customers, even those less desirable from a profitability perspective).

## Advanced analytics

- **Appropriate vs. legal:** The topic of data ethics—that what is allowed is not necessarily what one should do, and what one should do is not necessarily allowed—is likely to come to the forefront of forthcoming discussions on the use of data.
- **Explainability vs. model efficacy:** E.g. The notion that a “black-box” algorithm may in some cases deliver more efficient outcomes for customers and companies alike, but that financial institutions then might not be able to explain how a certain outcome was generated.

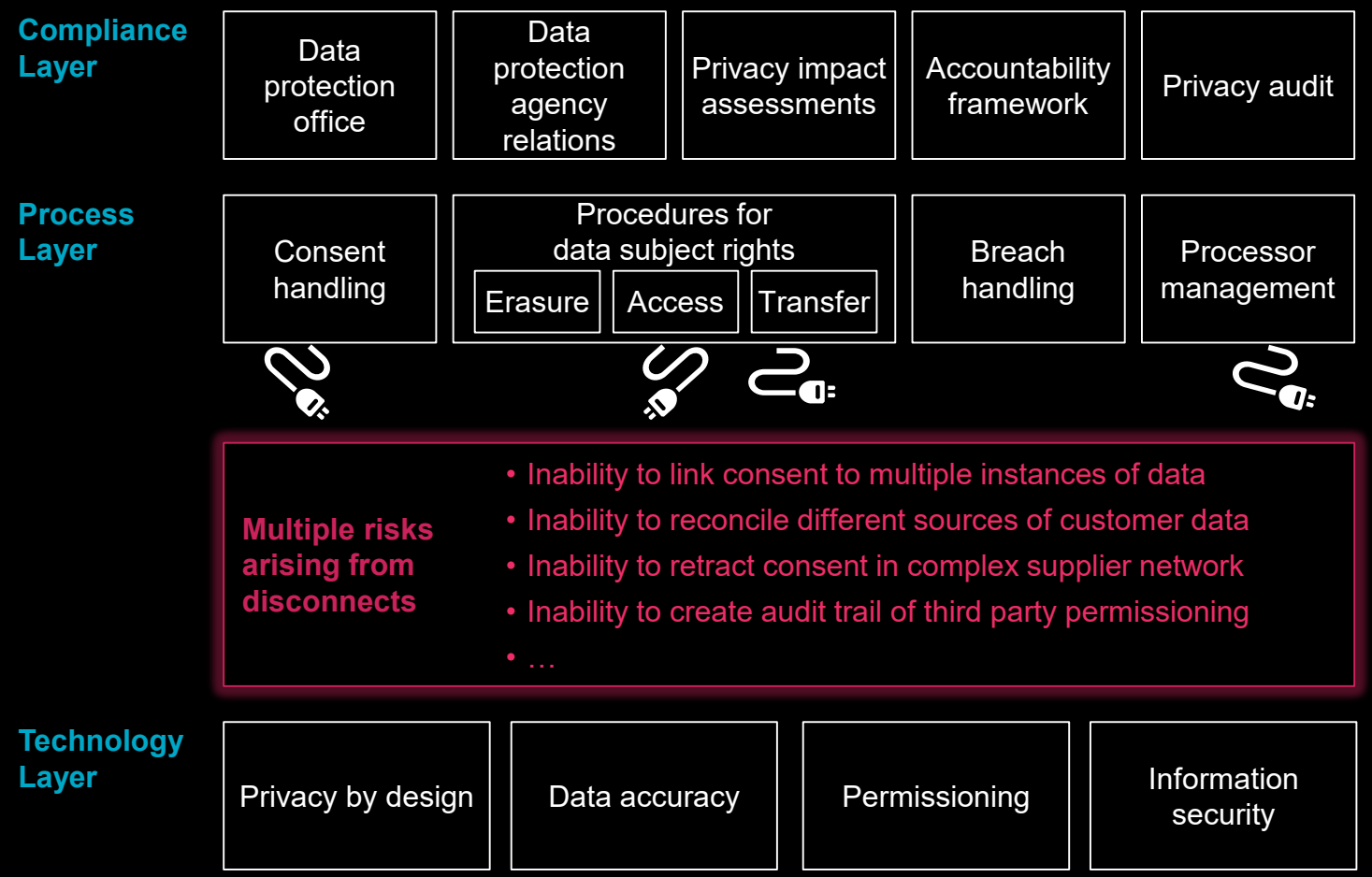
## Portability

- **Customer choice vs. equal treatment:** Regimes enabling customers to freely access, download and share data are assumed to improve efficiency, benefit customer choice and altogether support innovation. However, the effects on established players—the larger incumbent financial institutions—are less appreciated.

# Meanwhile, European banks have been focused on GDPR compliance, which leaves important gaps to be resolved

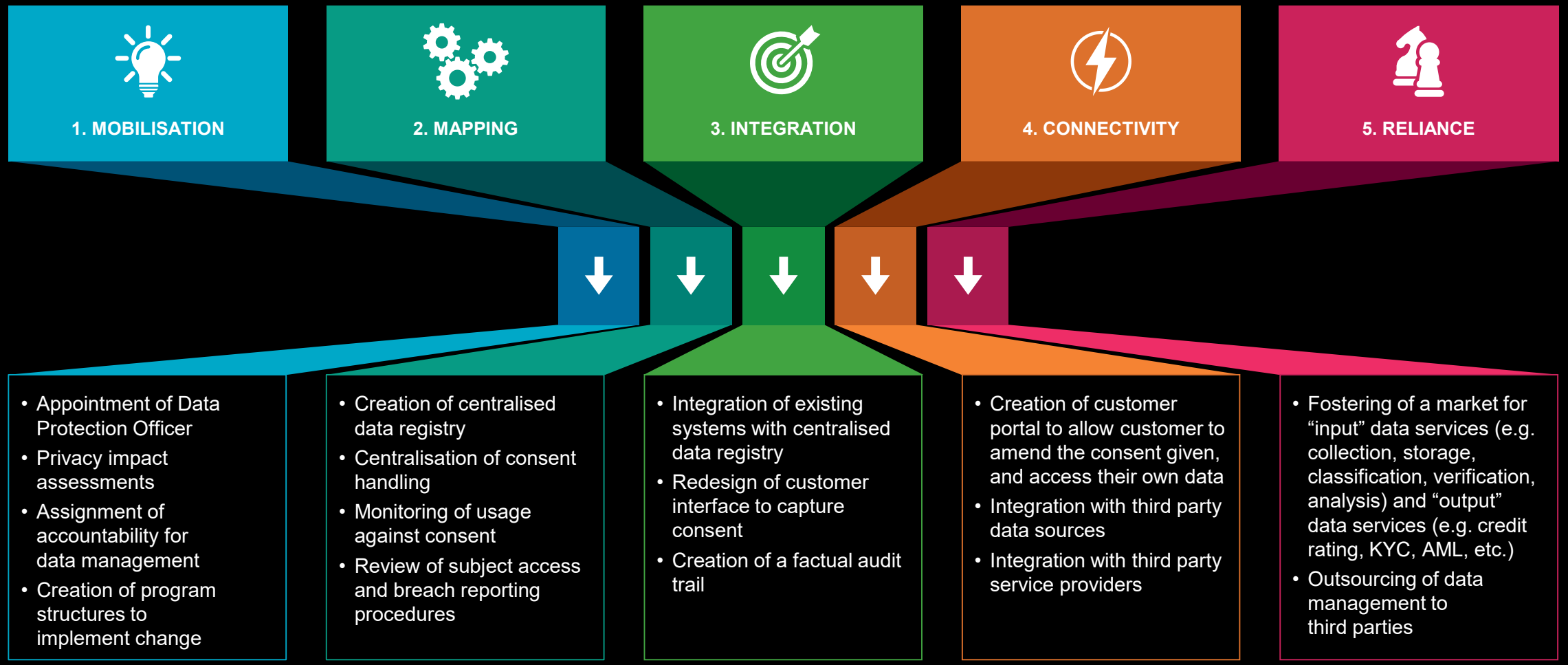
- At many firms, compliance programs have been devised to deliver on the formal elements required by GDPR
  - Policies
  - Data protection officer
  - Committees
  - Privacy impact assessments
- A compliance focussed approach will leave firms with (at best) an ability to highlight and report problems when they occur, but with few tools to make choices about the way that data is being managed
- The continuing trend towards open access (e.g. PSD2) means there will be ever more boundaries and data processors to manage
- Doing this on top of a fragmented data-set without clear management of consent will become ever more difficult

**Loose wires: GDPR programs that focus on basic compliance and are unsupported by technology will not support future privacy efforts**



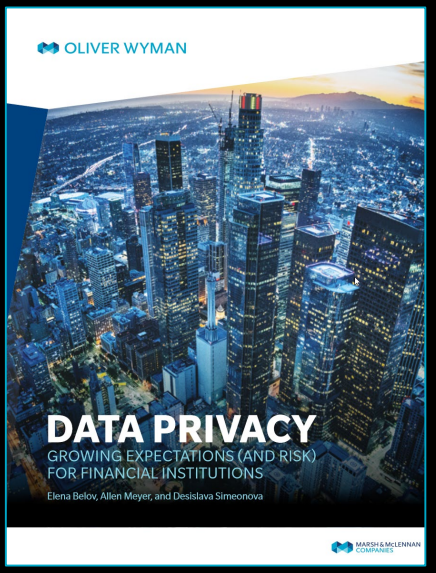
# A roadmap for sustainable privacy management beyond regulatory compliance

## Five steps required for sustainable privacy management



# There are five no-regret moves for firms wishing to advance now

| | | |
|---|---|---|
| 1 | Increase awareness at the senior executive and board levels | • Alignment between strategy and approach to data privacy<br>• Visibility of legislative agenda<br>• Adequacy of resources and infrastructure to handle future requirements |
| 2 | Understand how the organization uses personal information | • Understand what is collected from whom and for what purpose<br>• Understand data management and storage<br>• Develop a view on future requirements e.g. in light of digitisation and disintermediation |
| 3 | Data privacy risk identification | • Establish line-of-sight into the most significant privacy risk scenarios across consent, sharing, aggregation, breaches<br>• Understand the efficacy of protective controls. |
| 4 | Determine the firm's stance on data privacy | Beyond the regulatory minimum:<br>• What do we consider to be personal information?<br>• How do we use and share personal information?<br>• How do we inform consumers about data use?<br>• What rights do we give consumers? |
| 5 | Increase transparency and disclosure for consumers | • Make disclosures more accessible, interactive, and informative<br>• Educate customers on key privacy concepts<br>• Explain steps customers can take to increase their privacy |



# QUALIFICATIONS, ASSUMPTIONS AND LIMITING CONDITIONS

This report is for the exclusive use of the Oliver Wyman client named herein. This report is not intended for general circulation or publication, nor is it to be reproduced, quoted or distributed for any purpose without the prior written permission of Oliver Wyman. There are no third party beneficiaries with respect to this report, and Oliver Wyman does not accept any liability to any third party.

Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been independently verified, unless otherwise expressly indicated. Public information and industry and statistical data are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information. The findings contained in this report may contain predictions based on current data and historical trends. Any such predictions are subject to inherent risks and uncertainties. Oliver Wyman accepts no responsibility for actual results or future events.

The opinions expressed in this report are valid only for the purpose stated herein and as of the date of this report. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

All decisions in connection with the implementation or use of advice or recommendations contained in this report are the sole responsibility of the client. This report does not represent investment advice nor does it provide an opinion regarding the fairness of any transaction to any and all parties.