ETHICAL USE OF CUSTOMER DATA IN A DIGITAL ECONOMY

March 2019

UK FINANCE

KPMG

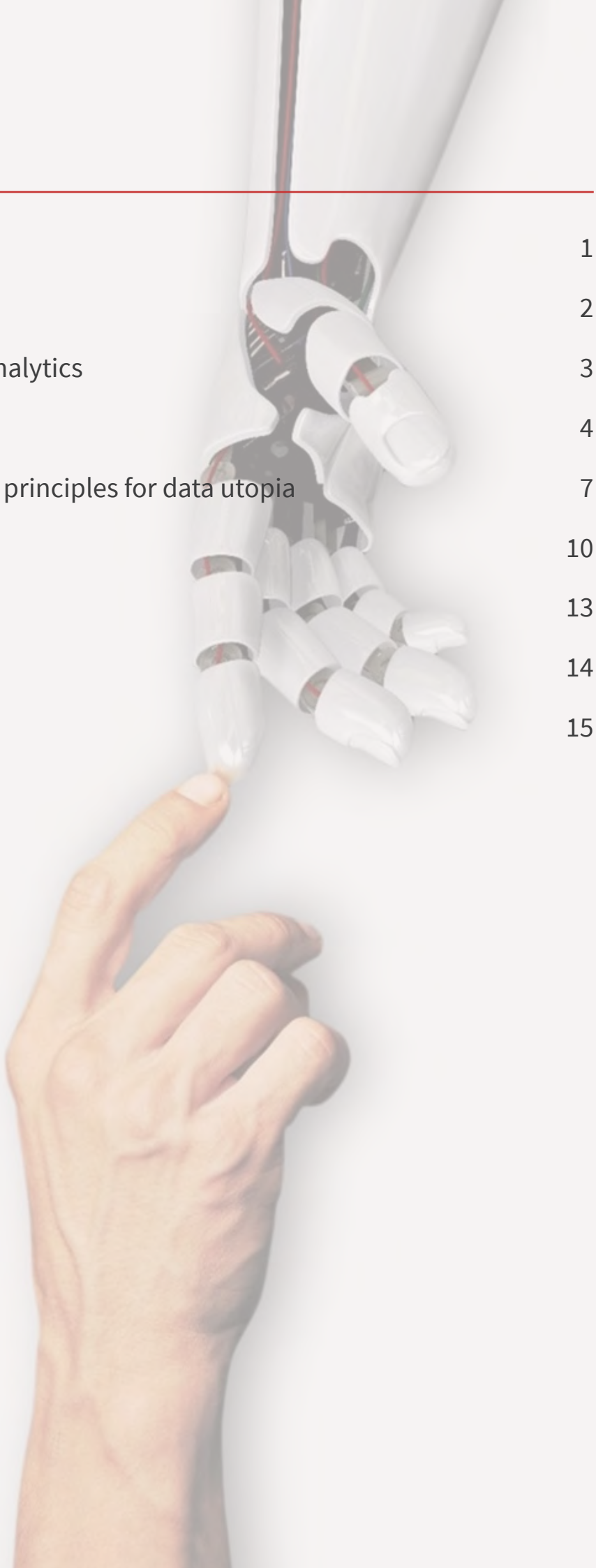
UK Finance is the collective voice for the banking and finance industry.

Representing more than 250 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry. We offer research, policy expertise, thought leadership and advocacy in support of our work. We provide a single voice for a diverse and competitive industry. Our operational activity enhances members' own services in situations where collective industry action adds value.

KPMG LLP, a UK limited liability partnership, operates from 22 offices across the UK with approximately 16,300 partners and staff. The UK firm recorded a revenue of £2.338 billion in the year ended 30 September 2018. KPMG is a global network of professional services firms providing Audit, Tax and Advisory services. We operate in 153 countries and territories and have 207,000 people working in member firms around the world. The independent member firms of the KPMG network are affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. Each KPMG firm is a legally distinct and separate entity and describes itself as such.

Contents



Foreword

The ethical use of data, and the extensive use of AI in day-to-day customer interactions have been an area of increased focus for politicians and regulators globally, as well as for news and media channels, over the last couple of years. New centres of research, such as the UK Centre for Data Ethics and Innovation, have been established and sit alongside the research developed by 'big tech' companies across the world.

If financial institutions lose their status as trusted custodians of customer data, they may well lose their licence to operate. In mainstream financial services, all forms of institutions are increasingly coming to understand the liabilities associated with data ownership and the use of autonomous technologies. While the amount of coverage in these areas has increased recently, for financial institutions the reality is that the ethical use of customer data has been a focus for some time. A good example is the 'Principles of Reciprocity' which were developed as a basis for sharing customer data with third-party providers in order to better undertake credit checks.

The use of data for such purposes requires firms to be diligent in their application of laws and regulations, including confidentiality, broader privacy rules and data protection. However, it's clear the industry needs to evolve from here.

The pressure to invest further in the automation of customer processes has never been greater, driven by the desire to reduce operating costs and improve return on equity. This path from automation, through machine learning to AI, is one that all forms of institution are pursuing in some way.

Equally though, the decisions taken by regulated institutions such as banks must conform to the rules of the relevant authorities: fair to the customer, transparent and defensible in terms of outcome. Therefore, the further convergence of data, technology and industry regulation is inevitable.

This goes beyond just a list of things that cannot be done with customers' data. Firms should be actively considering how they can use data to drive outcomes in customers' interests. The opportunity for better use of data to drive improved outcomes for vulnerable customers and around financial inclusion issues is significant.

Following the debate on 'fake news' in social media, customer awareness of the issues has increased dramatically. This paper is all about framing this debate and puts the customer, their data and outcomes at its heart.

We don't claim to answer all the questions. Time, technology and the views of society generally will all have an influence, and indeed we may never have all the answers. However, we can define some principles for this convergence as 'guard rails' for customers and institutions alike. In turn, these principles help the financial services industry to be more to the fore in this important area.

This is a White Paper focusing on what is currently an ambiguous area for customers and institutions. We appreciate your interest, attention and your feedback.

Stephen Jones, CEO, UK Finance

Karim Haji, UK Head of Banking and Capital Markets, KPMG

Introduction

Data analytics, including intelligent and autonomous systems, have become part of our everyday lives - and ubiquitous in all sectors of society, including financial services. However, if these increasingly public-facing and high-profile systems are to continue to serve our human values and the public interest, we now need ethical principles, policies and guidelines to govern and ensure their transparent and fair development.

Recent regulation of data protection constitutes a good start, but a holistic view of data ethics covers more than just compliance. Regulation will not always keep pace with rapid technological development, so a robust ethical approach that goes beyond direct compliance is needed to ensure fair and trustworthy outcomes are maintained. It should encompass how all customer data is generated, reported, stored and used in a trustworthy way.

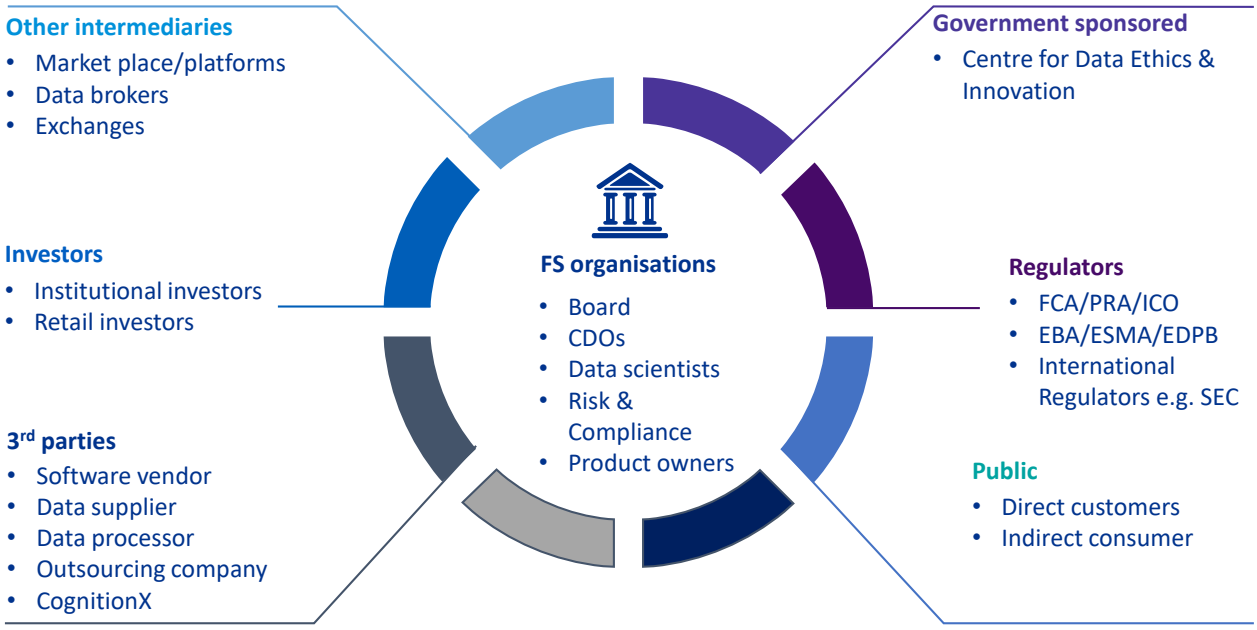
This paper seeks to build on existing international and cross-sector work, focusing in more depth on the specific customer impact risks and challenges that financial institutions face. Rather than create an entirely new set of ethical principles, our aim is to move the debate forward with foundational financial services-focused actions.

This paper therefore sets out to discuss the key ethical challenges facing financial institutions today, propose a set of principles for the ethical handling of customer data and set out some 'next steps' to help firms start embedding these into their operations.

Our objective is to help financial services firms to mitigate the risks these evolving technologies entail, while prioritising and protecting the human rights of the customer and delivering positive outcomes for them. Earlier industrial revolutions brought great advantages for society but the impact on labour forces was not regulated, creating challenges such as social unrest and taking a long time before sustainable frameworks were embedded.

Above all, we want to ensure the fourth industrial revolution and advanced analytics can be a force for good for all stakeholders, including customers, financial institutions themselves and broader society. To do this requires a number of stakeholders to consider their role in the data value chain.

FIGURE 1: DATA ETHICS STAKEHOLDER ECOSYSTEM



The rise and rise of data analytics

"With 2.5 quintillion bytes of data created every day, people are being defined by how they travel, surf the internet, eat and live their lives [1]."

The data revolution is creating a world that is more collaborative, interconnected and frictionless. And thanks to digital advances such as the Internet of Things (IoT), the boundaries between the physical and the digital worlds are blurring. In short, data is everywhere.

However, in the aftermath of the financial crisis of 2007 banks focused their efforts on reactive data strategies driven by regulation. They created data governance and management strategies and appointed Chief Data Officers (CDOs) in the context of the Basel Committee's reforms. More recently, they have hired Data Protection Officers (DPOs) to support compliance with the General Data Protection Regulation (GDPR).

The focus of the past few years has been on achieving compliance with regulations. Now, however, organisations are starting to use regulation as a driver for transformational change and forging ahead on strategic actions to embed data management and privacy into the culture of their businesses.

This will need to accelerate. With the rise of fintech and digital banks, customer appetites for new products and services, and faster and more seamless digital connections, are growing quickly. Banks must rethink their operating models to deliver far greater customer centricity. This will mean shifting to proactive data strategies that drive profitability and transform customer satisfaction for the better.

"Companies that invest in analytics have grown three times more quickly than those which are less analytically driven."

If the industry gets this right, the opportunities are enormous. In fields ranging from cancer research to smart cities, the use of data analytics tools to interrogate vast data sets has already delivered invaluable new insights that are changing people's lives. From a commercial perspective, companies that invest in analytics have grown three times more quickly than those which are less analytically driven[2]. Smarter use of data can also generate other tangible benefits – the pooling of data can, for example, be a crucial tool in the battle against cyber-crime and financial crime[3].

Many financial services businesses are already applying intelligent, automated technologies to large data sets to enhance customer experience, improve the agility of their services and to boost sales. One bank's mobile app, for example, provides 'predictive banking' that analyses a customer's account in order to offer personalised insights and guidance. We know of another firm with aspirations to use artificial intelligence for automatic loan approval and management, reducing processing time from three weeks to instantaneous outcomes[4].

However, while these advances are delivering valuable customer benefits, they are also driving a significant increase in certain risks that must be addressed. We have already witnessed a painful backlash following revelations about the misuse of data. Public trust has been undermined by scandals such as unauthorised data sharing by social media platforms, the resale of customer information by data brokers, and the bias of certain algorithms.

Such cases underline the importance of a crucial question: does the fact we can now do certain things mean that we should? This problem goes to the core of the data ethics debate.

1 It's Time to Talk About Data Ethics – March 2018 - https://www.datascience.com/blog/data-ethics-for-data-scientists
2 Smarter Analytics for Banks – September 2018 – https://www.mckinsey.com/industries/financial-services/our-insights/smarter-analytics-for-banks#0
3 Staying Ahead of Cyber Crime, UK Finance/KPMG, April 2018 – https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/staying-ahead-cyber-crime
4 How banks and their customers can benefit from artificial intelligence – https://www.atmmarketplace.com/articles/how-banks-and-their-customers-can-benefit-from-artificial-intelligence/

The dangers of data

Data analytics provides an opportunity to generate enormously positive outcomes, but also to create significant liabilities. The first step in developing a more ethical approach to data is therefore to identify the threats that data analytics could pose; this insight is the starting point for managing such liabilities.

We have become used to data being described as a valuable commodity – the new gold or the new oil. Certainly, like any commodity, data can be bought and sold, with more than 4,000 data brokers already worldwide[5]. In other respects, however, the idea of data (particularly personal data) as a commodity is at an early stage: the rules around how it is stored, processed, shared and exploited are still being written, as the regulatory environment and public perception catch up with technological advances.

Financial services institutions cannot afford to wait for consensus or certainty. The scale of the potential liability for organisations that do not act now to mitigate risk is simply too great, spanning regulatory failure, contractual dispute and the loss of customer trust.

The liabilities can manifest themselves through Legal and Regulatory, Operational or Reputational issues and risks, some of which we have outlined below.

LEGAL & REGULATORY RISK | OPERATIONAL RISK | REPUTATION RISK

Managing risk and liability

Financial institutions understand the need to "follow the road that maximises the benefits…while minimising its risks"[6]; but traditional approaches to risk management will need to be tailored in the face of these evolving challenges.

There will be new questions about issues such as liability and accountability – for example, who within the bank has primary responsibility for ethics and determining a framework to measure it against? Banks will require a robust governance framework to place the ethical use of data at the top of the agenda[7].

Risk of constraining individual choice

Banks' data contains valuable insights into their customers, potentially unlocking a better understanding of their behaviours and preferences and allowing the bank to focus its marketing efforts accordingly – with personalised products, for example. Choice architecture, nudges and other tools from behavioural economics can help individuals to make good, well-informed decisions.

These techniques should be managed carefully to minimise the risk of restricting the information customers have access to, which in turn can prevent them from making informed and independent decisions in their own best interests.

5 https://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers/

6 European Commission's High-Level Expert Group on Artificial Intelligence, https://www.euractiv.com/wp-content/uploads/sites/2/2018/12/AIHLEGDraftAIEthicsGuidelinespdf.pdf

7 AI in Control, KPMG – https://home.kpmg/xx/en/home/insights/2018/12/kpmg-artificial-intelligence-in-control.html

Introducing unfair bias

Intelligent and autonomous systems requiring little or no human intervention can greatly boost the efficiency and effectiveness of organisations, for example by improving fraud detection and supporting cost reduction. But while such systems help the bank to 'work smarter', they might not automatically optimise fair outcomes. Financial institutions may struggle to identify the limitations of these systems at an early stage and to ensure their outputs are free from unfair bias and prejudice, whether conscious or unconscious.

For example, one element of a disparate dataset may unfairly prevent a group of customers accessing a product or service. In one extreme example in the US, race prevented prison inmates being considered for parole. Financial institutions must ensure they are measuring the fairness of their predictive models in order to achieve high standards. The reality is that "ethics and innovation have to come together"[8].

"In a KPMG client survey across 120 internal auditors, 35% said AI was already being used in their organisation, with 62% saying that AI was being planned for[9]."

Data limitations

Where the data set has known limitations, it may be challenging to accurately validate outcomes. For example, how do banks ensure there is no gender bias when processing credit checks if gender is not directly captured as part of the data set?

Processing a certain data set could inadvertently cause discrimination or bias, even when 'protected characteristics'[10] such as gender and race are not collected. In practice, firms might choose not to gather such information in order to minimise their data collection. Firms will need to consider the balance between collecting and generating more data to identify and avoid unfair bias, and collecting less data in an effort to maximise customer privacy.

"Of the companies that took part in KPMG Guardians of Trust report, 92% question the trustworthiness of data analytics and are worried about the impact on reputation as a result[11]."

Interconnected systems

Transparency is crucial if a firm is to measure fairness and improve trust, but many systems are interconnected and can be complex. Where their logic is complex and layered, isolating data and decisions is difficult. It therefore becomes hard to check integrity and validate the outcomes of the decisions.

Similarly, the more we automate processes, the greater the potential to lose the expertise to explain why a decision was made. It is imperative to ensure outcomes are sufficiently transparent, explainable and auditable to allow for evaluation and challenge to decisions by the customer or a third party where appropriate.

8 Tabitha Goldstaub, CognitionX – https://blogs.thomsonreuters.com/answerson/uks-ai-council-chair-humanizing-the-business-of-artificial-intelligence/

9 Trust In Artificial Intelligence, KPMG - https://home.kpmg.com/uk/en/home/insights/2018/06/trust-in-artificial-intelligence.html

10 Equality Act 2010, section 4

11 Guardians of Trust: Who is responsible for trusted analytics in the digital age? KPMG – - https://home.kpmg/xx/en/home/insights/2018/02/in-digital-world-do-you-trust-the-data.html

Related concepts:

- Transparency: regulators and customers demand clarity on the purpose, data used, structure and underlying actions the algorithm performs to make decisions. Transparency is about being able to describe, inspect and reproduce the mechanisms through which the AI system makes decisions, and the governance of the data used.
- Explainability: this is about explaining the rules the algorithm uses, without reference to the decision outcome, in a way that can be easily understood by humans. This is driven through the concept of a 'glass box', as opposed to a 'black box' which cannot be explained. (Full explainability cannot be expected for 'deep learning' AI where the complexity may not be easily explained. Trust in these systems needs to be driven through rigorous testing).
- Auditability: this is the ability for an outside entity (eg: a regulator) to review how an organisation developed its algorithm—without compromising that organisation's intellectual property. This could in particular be to check that the technology does not discriminate against a protected class of people. Such an audit might prevent future risk on AI litigation.

Skills shortages

Sometimes it is the application of the technologies, rather than the technologies themselves, that requires oversight[12]. Those involved in the use or processing of data – whether as part of an internal development team or a third party – need a strong ethical grounding as they strive for fair data use and model outcomes.

These individuals and teams need to be well-educated on the ethical use of data and how to mitigate risks associated with bias and misuse. Those responsible for validating the outcomes will also need new skills and insights as we move away from traditional auditing capabilities.

External security

Even firms with the best intentions on ethics are at risk of damaging outcomes and impacts if their data is not secure. Firms will need to ensure that high standards are maintained throughout their supply chain. And while portability and interoperability of data is a risk for most organisations, the introduction of "Open Banking" raises the stakes.

The requirement to share data with regulated third-party providers at the request of the customer will become a real issue for financial institutions. Even with a legal obligation to share data with regulated third-party providers, and a regulatory framework in place around them, there could be reputational risks for financial institutions if something goes wrong. It must be a priority to address how to safely and securely make data available.

12 Centre for data Ethics and Innovation: Government response to consultation - https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation/centre-for-data-ethics-and-innovation-government-response-to-consultation

Managing the danger: five principles for data utopia

The prize for those financial institutions that can tackle the dangers listed above is a valuable one: getting data ethics right will both mitigate potential liability and secure priceless customer trust.

Indeed, "trust" is cited as the single most important factor by consumers reporting what they think about when asked to share personal data (94 per cent)[13]. In fact, banks are relatively well trusted compared to other organisations - 57 per cent of consumers trust their banks[14] – but it is crucial to maintain and improve this standing. Data ethics will become the guide to achieving these goals.

It is important to remember that the benefits of greater trust will be widely shared. Where banks improve ethical data practices and increase customers' data literacy, the latter will find it easier, for example, to make informed decisions and identify money-saving opportunities; for their part, banks will see improved customer experience, smarter innovation, and an enhanced suite of services and products.

How can these gains be realised? GDPR prompted banks to re-evaluate and enhance their data protection policies, moving in the right direction for greater trust through clarity over what personal data is captured, stored and processed and for what purpose. But this is only a start; from this point the key is to refocus risk and data management frameworks to embed data ethics in the culture of the organisation – to establish trust as a key point of differentiation.

This work is now underway, with negotiations about global standards, roles, rights and responsibilities. While this conversation will continue, key foundational principles are beginning to emerge from a range of sources that will help banks move towards data utopia. Crucially, these interconnected principles encompass both process and outcome – and they build on the minimum legal and regulatory requirements to establish much higher ethical standards.

Whilst each organisation clearly must start by thinking carefully about what their issues mean for their specific business model, we have identified five core, common, principles. As technology and business models evolve, these principles will no doubt evolve with them. Given the broad scope of applications of analytics and AI, these need to be applied with a degree of flexibility. Firms should consider proportionality in assessing the risks associated with the use of data and the algorithms and weigh these against the perceived benefits of such an algorithm. In particular, where they are being used to pursue a public interest objective, a careful balance will be required. For example, the application of these principles to personalised products and marketing will be different to where they are used to detect and prevent fraud.

13 Open data Institute – https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/

14 Open data Institute – https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/

RESPECT HUMAN AGENCY | SAFEGUARD EQUALITY AND FAIRNESS | DELIVER TRANSPARENCY

SPONSOR ORGANISATION-WIDE APPROACH | ESTABLISH ACCOUNTABILITY

Principle 1: Respect human agency

Financial institutions should respect human beings' ability to make their own free choices:

- This means financial institutions must not mislead or manipulate customers to act against their own interests, or unduly constrain customers' access to information.
- Unless there is an overriding public interest not to do so, customers should be able to tell or check when they are engaging with artificial intelligence or automated decisions, and there should be an appropriate level of human control over these systems, including an appropriate avenue for customers to challenge important automated decisions.

Principle 2: Safeguard equality and fairness

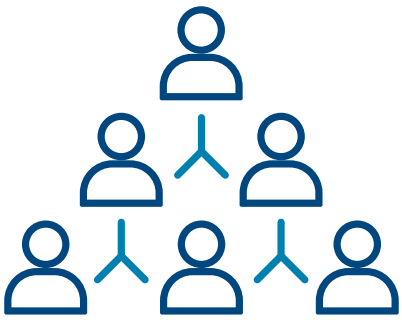
Financial institutions should treat their customers fairly and respect their basic rights:

- Identify potential negative impacts of processing on customers and carefully weigh these against the anticipated benefits to ensure proportionality. This includes material impacts such as financial loss and also less tangible impacts on basic rights, such as privacy.
- Identify and evaluate risks of unfair bias and discrimination that can occur through the data itself or through the human bias within the workforce programming the AI algorithm. Minimising risks include removal of any personal characteristics that cannot be objectively justified for use, with particular care over protected characteristics such as gender or race.

Principle 3: Deliver transparency

Financial institutions should process data outcomes within the boundaries of a 'glass box':

- Transparency will support the intelligibility, explicability and verifiability of the data and any actions taken on the basis of the data. Firms need to be able to understand the decisions they are taking and be able to explain these decisions to customers, auditors and regulators in an appropriate manner.
- Where it is difficult to explain exactly how a decision has been reached, firms should seek to minimise the risk of unfair or unexpected outcomes. Rigorous and extensive testing, making sure the algorithm works as it is supposed to, can form the basis for trust.
- Transparency with the customer will help boost data literacy and aid in the creation of a culture of trust.



Principle 4: Sponsor organisation-wide approach

Financial institutions should drive data ethics from the top and ensure it is adopted across business functions by building it into their existing governance frameworks under the financial services conduct regime:

- Establish appropriate senior sponsor-driven enterprise governance frameworks to provide the necessary transparency, communications, culture and defined business and data ownership.
- Senior leaders need to be evangelical in their support for ethical data use, but they must also ensure robust day-to-day behaviours.

Principle 5: Establish accountability

Financial institutions need to establish a chain of command on data ethics, with clear principles of accountability:

- Define accountability and ensure it is understood and agreed by all parties across the supply chain. This will help resolve any ambiguities, including around liability, if any issues or ethical breaches should arise. The same principles, governance and accountability should be applied to third parties as are applied internally.
- Develop processes and frameworks to test, monitor and govern the potential liability around the ethical use of data. Employees should understand the limitations of AI and algorithms.

How to embed data ethics

Banks need a way of embedding data ethics, and one way of doing that is through a framework – both for the challenges they face today and those that will emerge tomorrow. As we have seen, these challenges will span operations, reputation, regulatory compliance and more.

They will constitute the battleground on which financial institutions will battle for customer trust.

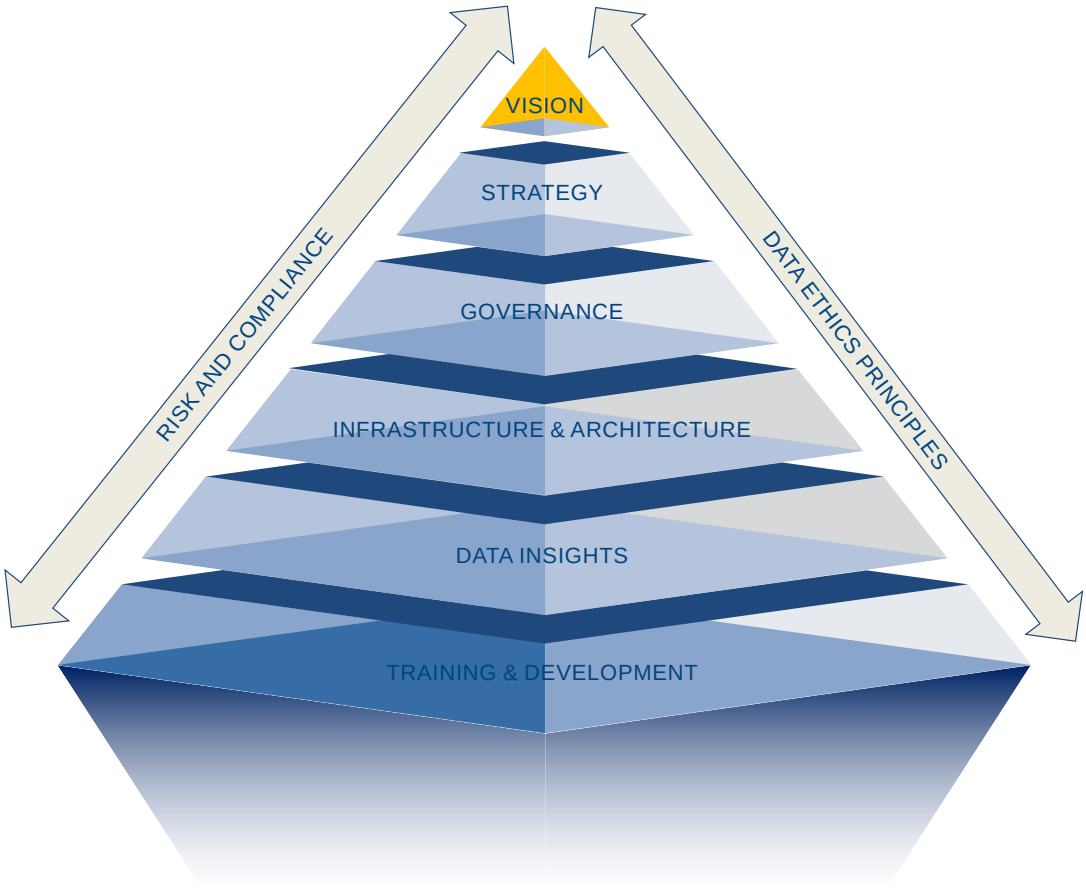
Such a framework will inevitably be far-reaching, going beyond the standard data strategy and understanding data both as an asset and a liability. For many financial institutions, it will help to think in terms of structures that address the whole lifecycle of data within their organisations:

- Data management – how data is collected, shared, stored and governed
- Data analytics – how data is analysed, including the design and use of algorithms
- Data outcomes – how organisations act on the insight generated by their data

This perspective provides financial institutions with a clear view of the value and potential risks associated with their data. As a result, they can begin to embed data ethics through every part of their organisation, at each stage of the data value chain. It offers a new lens through which to view, assess, and improve existing business-as-usual safeguards and controls, as well to consider new challenges, including those currently unknown.

This does not mean reinventing the wheel: in practice, a data ethics framework will build on existing frameworks within financial institutions using a combination of technical and non-technical approaches.

Consider six key areas:



VISION

Address the question 'What does the "ethical" use of data look like for your financial institution? What outcome are we trying to achieve?'

INFRASTRUCTURE AND ARCHITECTURE

Establish appropriate infrastructure and architecture to manage data across the enterprise, supporting transparency and the implementation of data integrity, controls, access and security. This infrastructure must be fit for purpose, agile, scalable and robust.

STRATEGY

Set strategic goals to achieve this vision, addressing the far-reaching nature of the current challenges and ensuring data ethics are enforceable, embedded in the organisational culture, continuously applied and improved.

DATA INSIGHTS

Use insights to support explicable and accurate data outcomes and identify data limitations, using tools such as dashboards to track and monitor model trends, and to sound an early warning where ethical challenges may arise.

GOVERNANCE

Drive a robust governance framework with strong senior sponsorship. Embed ethical principles in the organisation's policies, procedures, business processes and ownership models.

TRAINING AND DEVELOPMENT

Put in place training and education on the ethical issues surrounding the use (and misuse) of data, including design and development of measurable testing and evaluation outcomes for analytics and autonomous systems. Those involved in the handling of the data and development of models need the right level of skills and experience.

Framework component	Practical example
Strategy	Strategic goal: establish an ethical data culture that drives innovation
Governance	KPIs to measure ethical use of data, which are tracked and monitored by second line of defence
Infrastructure and Architecture	Documented data lineage across the architectural landscape for critical automated outcomes
Data Insights	Quality controls implemented on critical data to validate outcomes
Training and Development	Clear organisation definition of 'ethics' and people and skill requirements to support ethical framework e.g. audit capabilities

Next steps

With such a data ethics framework in place, banks can begin to integrate these key principles into existing enterprise-wide risk management practices. Financial institutions will need to reconsider questions such as existing access to – and use of – data within their organisation.

Do you know where customer data is used as part of intelligent autonomous solutions, whether you have mechanisms to manage relevant risks, and how you would assess any potential impact resulting from liability? Across the principles outlined in this paper, possible actions include:

Principle 1: Respect human agency

- Nudges are identified and appropriate.
- An appropriate degree of control to override profiles and nudges is provided.
- Customer journeys allow customers to access an appropriate description of how they are engaging with AI or other automated systems.

Principle 2: Safeguard equality and fairness

- New tools and products are reviewed to identify costs and benefits to different parties, and weigh up these impacts.
- Procedures exist to identify and review risks of unfair bias in datasets and algorithms and address any that cannot be objectively justified.
- Training data is reviewed for unfair bias.

Principle 3: Deliver transparency

- Customer journeys are reviewed to ensure customers can access an explanation that is helpful in context, while avoiding information overload.
- An appropriate level of explanation of 'default settings' is provided to customers.

Principle 4: Sponsor an organisation-wide approach

- Roles and responsibilities are clearly defined and understood for the data owner, system owner, model owner and development teams.
- Robust processes and procedures are in place to ensure models are documented and maintained.
- R&D teams and data scientists have contractual requirements to adhere to an ethical code of conduct, and third parties have ethical standards imposed by contract.
- If you operate internationally, take stock of relevant regional differences in ethical expectations.

Principle 5: Establish accountability

- Data ethics is clearly and consistently defined and is consistently tracked and monitored by second line of defence
- Building explainability into the AI system (as far as possible).
- Determining individuals or groups who are most responsible for the impact of the algorithms or AI.
- Risk appetite measures and monitors data ethics just as closely as the quality of the relevant data.
- Change management functions are engaged to ensure that information is up to date.

Conclusion

It is logical that the use of customer data combined with the autonomous Machine Learning and AI systems must be subject to challenge and be open to legal and regulatory scrutiny in order to establish much higher ethical standards.

This is a very significant debate and for data analytics to be a force for good, it will require a coordinated effort from both industry and regulators to help avoid repeating the mistakes of the industrial revolution.

Many national and international bodies have begun to address this issue, but given the principles vary greatly across many domains, not least within countries and cultures, more work is required to reach consensus.

Now is the time for all stakeholders to build on the existing international and cross-sector work, focusing in more depth on the specific customer impact risks and challenges. Rather than create an entirely new set of ethical principles, our aim is to move the debate forward with foundational actions.

Contributors - UK Finance

Dan Crisp, Director, Digital, Technology and Cyber, UK Finance

Dan is Director for Digital, Technology and Cyber at UK Finance, overseeing policy initiatives including fintech, cloud computing and data protection. Dan is also focused on projects to operationalise industry utilities for technology risk and E-ID.

Prior to joining UK Finance, Dan was Chief Operations Officer for Barclays Global Information Security, primarily responsible for the technical integration of global acquisitions. Dan has also held various senior risk and compliance roles at JP Morgan and Citigroup. Most recently, Dan served as Chief Technology Risk Officer for BNY Mellon where he led the innovation, development and deployment of global technology risk regulatory controls.

Dan is a board member for the Internet Security Alliance, a non-executive director for Huntswood and a charter member of the Cloud Security Alliance metrics group. He is also a mentor at Level 39, Europe's largest fintech accelerator and incubator. Dan holds qualifications from the University of Memphis (USA) and Stanford University (USA). He has also completed the Strategic Management Program at Cambridge University (UK).

Jonathan Middleton – Manager, Digital and Technology Policy, UK Finance

Jonathan Middleton joined UK Finance in 2018 as Manager for Digital and Technology Policy. He oversees work on a range of topics including innovation, fintech, disruption, regtech and AI.

Prior to joining UK Finance, Jonathan was Head of Technology Policy at the Government Digital Service. Jonathan is a graduate of Oxford University and the University of London. He is also a Fellow of the Royal Asiatic Society.

Walter McCahon – Manager, Data Policy, UK Finance

Walter McCahon oversees policy work on privacy and data protection issues at UK Finance, particularly the General Data Protection Regulation and Data Protection Act.

Before coming to UK Finance, he worked for the BBA in various policy areas, including privacy, data protection and Open Banking. He previously worked for the New Zealand Banker's Association and New Zealand Ministry of Economic Development on financial sector regulatory reforms.

Contributors - KPMG

Chris Steele – Director, Banking Regulatory, KPMG

Chris is a Director in KPMG's Risk and Regulatory team. He has 18 years of experience in financial services and leads the Retail Conduct group. He is a member of KPMG's RegTech and Open Banking working groups and KPMG's interim Principal delegate to the Institute of International Finance covering a broad range of regulatory matters. He assists clients with their conduct, regulatory change, governance and digital agendas.

Dr Leanne Allen – Director, FS Tech-Data, KPMG

Leanne Allen is a Director in KPMG's FS Tech Consulting Practice and leads KPMG's Data capability. Her background includes a PhD in mathematics and she started her career as an actuary before moving into Tech-Data consulting. She brings 15 years' experience in Data Architecture, Data Management & Governance, and Reporting & Analytics.

In addition to helping her clients navigate complex issues and drive data-driven transformational change, Leanne is a thought leader in Tech-Data, developing, leading and thinking ahead.

Ashley Watkins – Senior Manager, FS Tech-Data, KPMG

Ashley Watkins is a Senior Manager in KPMG's FS Tech Consulting Practice, with particular focus on Data and Regulatory driven projects. She has ten years' experience in Data Management, Change Management and Data Architecture across the retail and investment banking industry.