

Data Privacy:

How can the financial sector
ready itself for an AI-driven
environment?

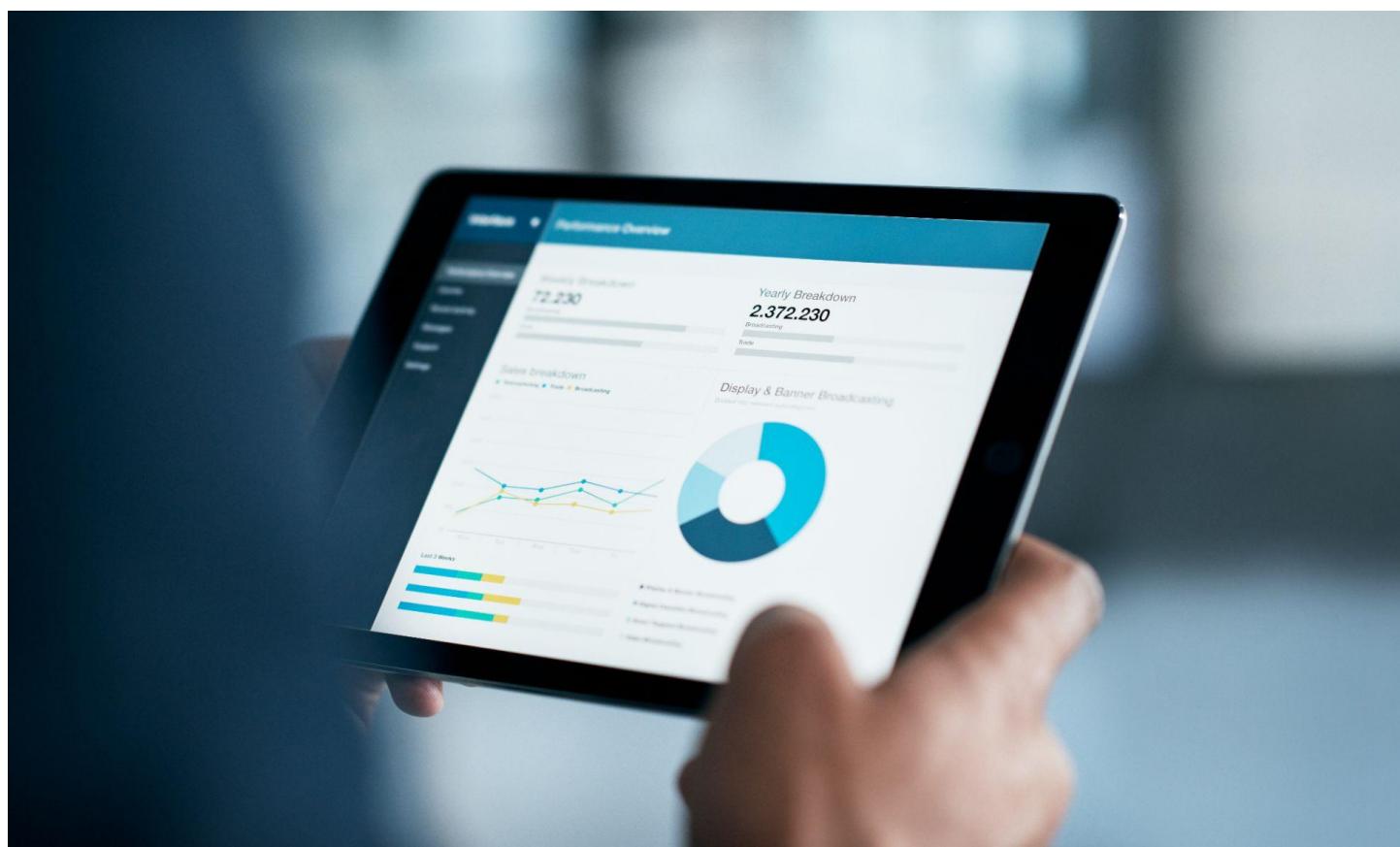
At the recent Dubai Fintech Summit 2023, PwC Middle East chaired a roundtable on Data Privacy that deliberated on how privacy regulations may impact the development and use of automated or semi-automated technology such as AI systems in financial services. It also discussed implications of the recent DIFC legislative consultation on proposed regulations setting out guidelines and the safeguards required for processing personal data when using AI-enabled systems.

Studies show that the volume of data created, captured, copied and consumed worldwide has grown from two zettabytes* in 2010 to 64.2 zettabytes in 2020, and is slated to reach 181 zettabytes by 2025¹. This explosion has led to rapid technological developments, including AI and machine learning that have the ability to learn from data and arrive at intelligent decisions.

While big tech and cloud computing now allows us to store, process, and analyse massive datasets easily, enabling AI systems to analyse, create insights and predict outcomes with high accuracy, the spotlight has turned to privacy concerns. Banks, fintechs and financial services institutions in the region are grappling with complex issues, such as responsible use of data, fairness and accountability and the potential for bias in AI systems.



Today, personal data-powered AI cuts across all industries, and financial services, governments and policy makers around the world are working on regulations and strategies to safeguard personal data. In the UAE, the DIFC Data Protection Commissioner has recently taken steps to develop safeguards via proposed additions to the Data Protection Regulations 2020 that supplement the Data Protection Law, DIFC Law No 5 of 2020, while in the UK, the Department of Science, Innovation and Technology (DSIT) has recently [published an AI white paper](#)² to guide businesses on the use of this revolutionary technology. In June 2023, the European Parliament approved a draft of the proposed [Artificial Intelligence Act](#)³, which promotes a risk-based, tiered approach to regulating AI, including bans on high-risk AI applications. As the number of potential use cases for AI within financial services increases, so too will scrutiny from regulators on how AI is being used and how it processes and reads large amounts of data



1. <https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=The%20 total%20 amount%20of%20data,replicated%20reached%20a%20new%20high> [*One Zettabyte is equal to one billion terabytes]
2. <https://www.gov.uk/government/news/uk-unveils-world-leading-approach-to-innovation-in-first-artificial-intelligence-white-paper-to-turbocharge-growth>
3. <https://www.google.com/url?q=https://iapp.org/news/a/european-parliament-vote-pushes-ai-act-significant-step-forward/&sa=D&source=docs&ust=1689325998768876&usg=AOvVaw3ZEjps9shUThgaFKjnyQK>

This document highlights the key points raised at the roundtable.

Current situation: A regulatory perspective in the region

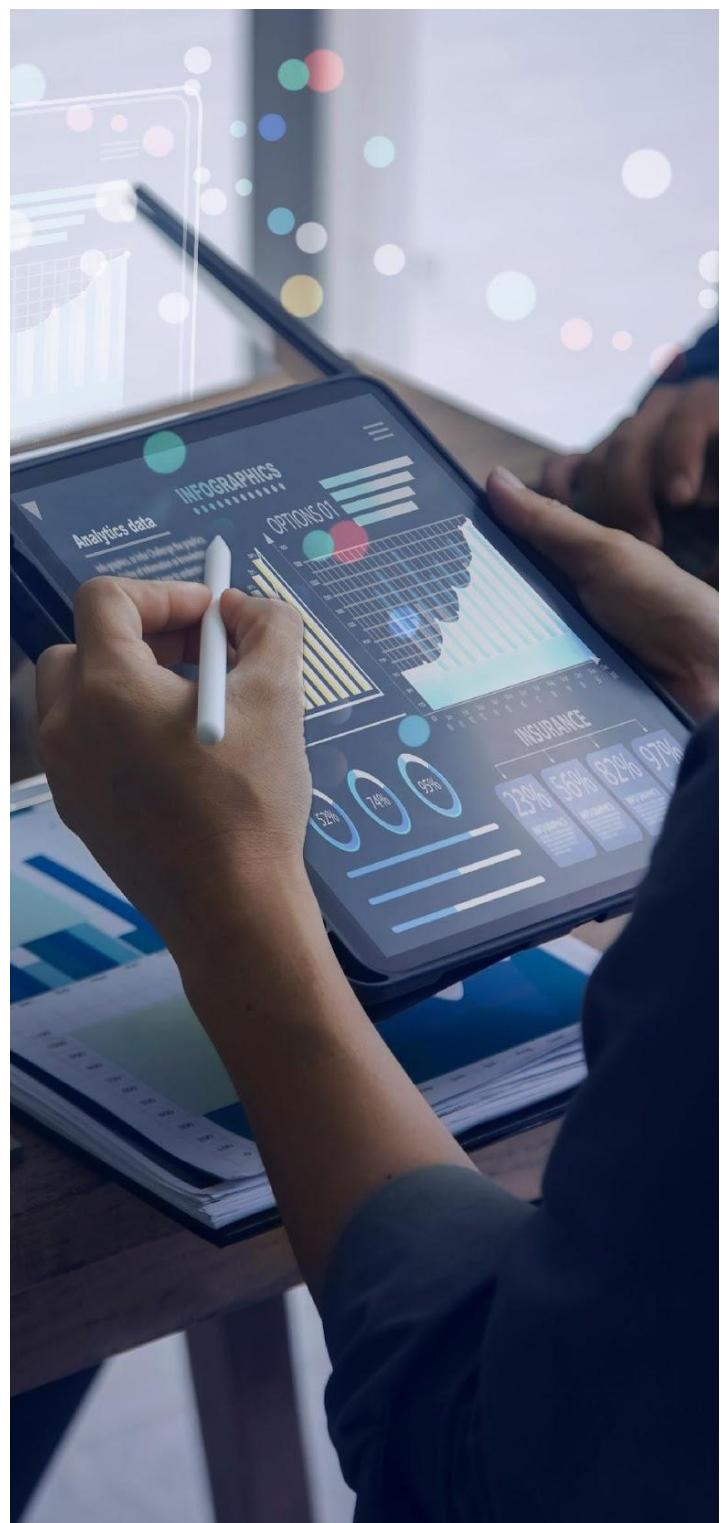
Participants were aware of advanced technology platforms being developed rapidly worldwide and called for a clear need for guidance. They wanted DIFC to rope in best practices from across the globe and agreed that any new regulation(s) around AI should be principles-based in order to express the outcomes to be achieved by regulated businesses rather than detailed prescriptive rules and processes.

DIFC is open to working with organisations to understand and test AI use cases. Regulations could always evolve and be updated, but the need of the hour was for regulators to step in and offer more guidance and practical application materials.

Some participants also pointed out the downside of regulations. For instance, many US-based technology firms are often fined by EU regulators, as a result of complaints submitted by individuals who are concerned about their rights and judicial redress options (or presumed lack thereof) in the United States. The recent developments around data export to the US by way of the EU adequacy decision under the EU-US Data Protection Framework (DPF) may impact this situation for the better, but there will likely be further challenges to the DPF. More privacy-driven regulation may only complicate things.

As implementing AI solutions gains popularity across financial institutions, most organisations are exploring ChatGPT (an AI chatbot developed by OpenAI and released in November 2022), and some are issuing guidelines to govern its use in the workplace. Others are already discouraging employees from unnecessarily sharing personal data.

Most participants agreed that ChatGPT popularised the use of AI, and as a result, we need to learn about the risks involved. Today, most technologies enable unnecessary (and often) unrestricted access to personal data, and AI needs to be controlled in time. Engaging experts and technologists early on will be crucial in designing a handbook for generic AI use (and ChatGPT in particular).



Key points:

Future of regulation

The highlight of the discussion was around framing regulations. DIFC and the roundtable participants agreed that regulation(s) must not be framed in a silo and collaborative regulation and guidance development is the need of the hour. A dual regulatory lens is needed for AI – looking at both opportunities and risks.

Singapore, Hong Kong, and South Korea were cited as examples of best practices around AI guidelines, which can be a great starting point for regulations in the Middle East.

- In August 2021, the Office of the Privacy Commissioner for Personal Data of Hong Kong published its 'Guidance on the ethical development and use of AI'. The aim was to help companies comply with the Personal Data (Privacy) Ordinance requirements as they develop and use AI. The Office also established seven ethical AI principles, including accountability, transparency, and privacy .
- In May 2022, Singapore's Personal Data Protection Commission (PDPC) launched the world's first AI governance and testing framework and toolkit, A.I. Verify. This allows companies to demonstrate responsible AI objectively and verify it while promoting transparency between companies and their stakeholders.
- Major companies across sectors (including AWS, DBS Bank, Google, Meta, Microsoft, and Singapore Airlines) have already tested the toolkit and have provided feedback⁵.
- In February 2023, the Science, ICT, Broadcasting and Communications Committee of the Korean National Assembly passed a proposed legislation to enact the Act on Promotion of AI Industry and Framework for Establishing Trustworthy AI" (the AI Act). If passed into law, the AI Act will be the first statutory foundation comprehensively governing and regulating the country's AI industry. A path breaking feature of this Act allows anyone to develop new AI technology without having to obtain any government pre-approval⁶.

There was consensus around tweaking AI regulation(s) based on sectoral requirements. Regulators highlighted ethics in AI as a significant consideration. Humans should have control over AI and not the other way around. DIFC also cited a growing number of companies and individuals advocating for AI's unregulated existence.

Some areas that participants wanted to be addressed by future regulations, include:

- Companies should explain (possibly, justify) the use of all consumer data
- Safeguarding consumers and not those collecting the data (for instance, a participant cited an example where a financial fraud occurred, and the wallet operator was unable to share information with the complainant because of General Data Protection Regulation (GDPR) compliance)
- 'One size fits all' approach must be avoided and a 'collaborative' model is recommended.

-
4. <https://iapp.org/news/a/hong-kong-privacy-commissioner-publishes-ai-guidance/>
 5. <https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework>
 6. https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=26935#:~:text=The%20AI%20Act%20sets%20forth.businesses%20in%20the%20AI%20industry

AI use cases for the financial sector

Several AI use cases have emerged over recent times, and more are being established as players in the financial sector continue experimenting with this technology. Some of the current use cases include the following:

1. Leveraging AI for credit scoring: AI can easily overcome the limitations of traditional credit scoring models that rely on a limited set of data points (such as payment history and outstanding debt) and often fail for individuals with limited credit history or non-traditional sources of income. AI scoring models can analyse a vast array of data points, including non-traditional data sources, and present a more accurate and comprehensive view on a borrower's credit worthiness.
2. Leveraging AI for Application Data Management (ADM): This is often achieved through metadata analysis and activation, allowing the AI model to detect deviations in data usage (from system design) and correct them. The benefit – financial institutions will spend less time in managing and optimising infrastructure and instead channelise their efforts on building core business value. In January 2023, Google in partnership Aible (a cloud-based AI solution and auto machine learning platform), helped a Fortune 500 company to analyse over seventy-five datasets with over one hundred million rows of data across 150 million variable combinations. The compute cost (at US\$ 80) was much lesser than the cost of traditional methods⁷.
3. Leveraging AI for fraud detection: In 2021 alone, over US\$ 217 billion was spent on AI applications to help prevent fraud and assess risks. AI helps prevent many possible fraudulent activities, such as mail phishing, identity theft, credit card theft, document forgery, and buyer behaviour mimicry. Most banks deploy AI applications to analyse transactions, assign risk scores to these, and segregate consumers into various profiles, among other uses⁸.

Other use cases include leveraging AI for consumer risk management and even law enforcement. For instance, some participants highlighted that contrary to widespread belief, blockchain transactions done through legal routes are completely traceable and this can be fed into AI systems in order to prevent and investigate crime, financial or otherwise. In the UAE, illegal routes supporting blockchain transactions are closed upon discovery.



7. <https://venturebeat.com/data-infrastructure/how-ai-can-ease-data-managementwoes/#:~:text=Businesses%20are%20using%20AI%20to.are%20embedded%20from%20the%20beginning.%E2%80%9D>
8. <https://bfsi.economictimes.indiatimes.com/news/banking/how-banks-are-using-artificial-intelligence-for-fraud-detection/96704604#:~:text=In%20order%20to%20accurately%20detect,a%20number%20of%20different%20profiles>

From a data privacy perspective, how is AI different from technologies of the past?

In the recent past, businesses latched on to the cloud and it witnessed a spiral growth trajectory (Gartner forecasts worldwide public cloud end-user spending to reach US\$600 billion in 2023, registering a 20.7 percent year-on-year growth). Data privacy concerns also grew, and enterprises are still trying to solve them.

Another emerging technology, blockchain, has also presented several use cases, but most companies still need to understand the technology before ultimately leveraging it. Like with the cloud, data privacy concerns exist in this context as well.

With AI gaining popularity, these data privacy conversations tend to be side-lined, as businesses (financial sector and otherwise) focus on exploring their full potential and ramifications. The roundtable participants agreed that both these conversations must be looked at in tandem, and one should not have precedence over the other.

The future of AI

Some participants would like to see AI being used to drive additional value in the financial sector (and even outside it). Another expectation was to have more AI-based start-ups – Japan was mentioned as an example where the most recent start-ups getting unicorn status are those that have successfully leveraged AI in their offerings. A participant mentioned that acquiring AI programmes/codes today is the equivalent of developing real estate in the past.

A word of caution for employees was to jump on the AI bandwagon quickly and equip themselves with new-age skills to avoid any foreseeable redundancies. A scenario discussed involved stock traders becoming redundant in the future as AI applications are expected to predict market movements more accurately. AI applications will be able to analyse even more variables when predicting, including assessing credibility of company founders.

The shortcomings of AI

No discussion on AI is complete without taking a look at its shortcomings. Participants cited that AI is currently unable to identify false or misleading information. For example, in a particular case, AI was leveraged to identify patients that did not need to stay at the hospital to optimise bed space. Analysing the available data, the AI application concluded that patients with both pneumonia and asthma could safely be sent home, which was most likely incorrect. Thankfully, human intelligence prevailed, and the hospital management did not act on AI's recommendations.

This particular shortcoming around reputation building and management is pertinent to the financial sector. The currently in-use AI applications and models are unable to do this. Participants agreed that we have just begun scratching the surface, and more new shortcomings will present themselves as financial institutions continue exploring AI and its use cases.

7. <https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023>

AI and the Middle East region

Our roundtable participants believe that this region could function as a sandbox for the rest of the world. For instance, a regulation was rolled back in KSA following a backlash from affected parties, which is not a usual occurrence elsewhere.

On improving digital literacy, GDPR was mentioned as its driver in Europe. For the Middle East region, participants believe that the catalyst could be the focus on innovation backed by the right regulatory frameworks.

Key takeaways

As the use of AI evolves, it will be important (at an organisational level) to assign key responsibility areas (KRAs) across the organisation. For example, IT and the legal teams are often responsible for safeguarding data privacy, and a clear distinction in their responsibility areas is a must-have.

01

Most participants agreed that third party developers/providers should also be responsible for data privacy.

05

An interesting angle to keep in mind is that cultures and ethnicities also play a role in defining ethical AI – what is right for one populace could be outrageous for another. This circles back to avoiding the ‘one size fits all’ regulation(s) that we highlighted earlier. In the Middle East region in particular, most consumers follow the Western media (and content on OTT platforms, for instance), which are not necessarily sensitised to their local beliefs. This can be solved by giving the due importance to cultural differences in consumer values.

02

Some suggested looking through the financial crime lens when solving data privacy cases as such unlawful elements often have the best understanding of the current legislations and regulations and how to bypass them. Perhaps, ethical criminals could be hired to lend a helping hand in safeguarding data privacy.

06

Current data literacy rates are low across the Middle East region, and most users are sharing unnecessary data (without realising the downside). For instance, a consumer buying from an online platform shares varied data levels with the provider, including his location, payment mechanism(s), and even buying preferences.

04

Participants voiced that all stakeholders should join forces to increase data literacy levels.

- Younger consumers (Gen Z, for instance) have higher digital literacy rates, but there is not enough data to validate this assumption.

It is also important to simplify policies and terms and conditions for consumers. For instance, a consumer signing up for a new credit card has to read dozens of pages, and often gets lost or does not completely understand how the issuing bank will use the data collected. Financial institutions should share this information in a short, succinct manner.

- An interesting twist here is the difference in requirements of regulators and consumers. While the former wants businesses to be as detailed as possible, consumers necessarily do not need to know-it-all. It is a delicate balance, yet essential for financial institutions (or enterprises from other sectors) to maintain.

Contact us



Phil Mennie

Partner

Technology Consulting | Middle East Data Privacy Leader
PwC Middle East
phil.mennie@pwc.com



Richard Chudzynski

Director

Middle East Data Protection and Privacy Legal Leader
PwC Legal Middle East
richard.chudzynski@pwc.com

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Established in the Middle East for 40 years, PwC has 24 offices across 12 countries in the region with over 10,300 people. (www.pwc.com/me). Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.