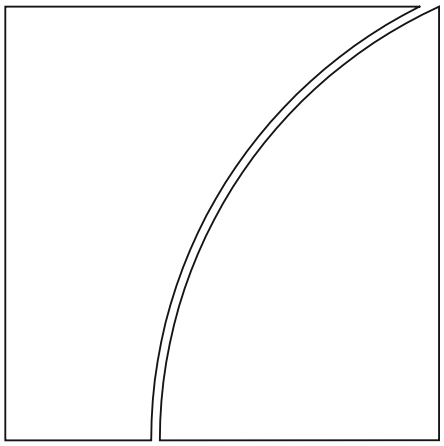
Financial Stability Institute | BIS

FSI Insights on policy implementation
No 73



In data we trust? Emerging policy and supervisory approaches to AI data use in financial services

by Juan Carlos Crisanto, Adrien Currat, Johannes Ehrentraud, Wenguang Wu

March 2026

JEL classification: C60, G29, G38, O30

Keywords: artificial intelligence, machine learning, corporate governance, data governance, risk management, risk modelling

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in these publications are those of the authors and do not necessarily reflect the views of the BIS, its member central banks or the Basel-based standard-setting bodies.

Authorised by the Chair of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Global Media and Public Relations team, please email media@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-249X (online)
ISBN 978-92-9259-943-0 (online)

Contents

In data we trust? Emerging policy and supervisory approaches to AI data use in financial services[1]

Executive summary

Artificial intelligence (AI) is transforming the financial sector while further amplifying the critical role of data within it. Advanced forms of AI, such as generative (gen) AI, depend on vast and diverse amounts of data across all stages of their life cycle. Data are essential for training gen AI models, assessing performance, identifying biases and refining outputs, and therefore shape their capabilities, limitations and evolution. As these systems become more embedded in core financial institutions' activities, such as deposit-taking, credit and insurance underwriting, and payments, sound data management becomes essential not only for ensuring reliable and trustworthy AI applications but also for preserving trust and confidence in the financial system.

Although data management challenges are not new, the financial sector consistently identifies them as significant barriers to the broader adoption of gen AI. A long-standing issue is the incompatibility of the sector's numerous data sources, which often contain rich but fragmented information. This has historically resulted in inconsistent data quality, hindering analytics and automation efforts. The scaling of gen AI amplifies these weaknesses while introducing new challenges, including those related to the growing use of synthetic and alternative data. Among the most pressing concerns are those relating to data privacy, quality and security, all of which are exacerbated by third-party dependencies. Taken together, these shortcomings can heighten consumer protection risks as well as micro- and macroprudential vulnerabilities. If left unaddressed, they have the potential to erode the anticipated benefits of gen AI in the financial sector.

Data protection has received considerable attention, even before the advent of AI, including at the international level. Although data protection is widely regulated across jurisdictions, its scope varies, and applying data protection principles to AI remains a challenge as their interplay continues to evolve. In response, some data protection authorities have started issuing cross-sectoral guidance on how data requirements apply to AI practices. This guidance, combined with cross-sectoral data protection frameworks, forms the foundation for addressing AI-related data risks in the financial sector.

Data protection frameworks place particular emphasis on data privacy, understood as individuals' ability to control their personal data. However, advanced AI systems, which rely on extensive volumes of personal data, can undermine individuals' ability to determine how their data are collected, processed and shared. Upholding core data privacy principles – such as lawful basis, meaningful consent, purpose limitation, data minimisation and retention limitation – becomes particularly challenging in the context of AI. Other principles, including fairness and transparency, also present complexities in AI.

Data quality is equally central. Data protection frameworks emphasise data accuracy, completeness and representativeness to prevent the spread of false information and reduce the likelihood of decisions based on inaccurate data. Similarly, AI frameworks attach critical importance to this area as poor data quality can lead to biased or harmful outputs. While both frameworks align in their emphasis

[1] Juan Carlos Crisanto (Juan-Carlos.Crisanto@bis.org), Johannes Ehrentraud (Johannes.Ehrentraud@bis.org), Adrien Currat (Adrien.Currat@bis.org), Bank for International Settlements; and Wenguang Wu (wwenguang@pbc.gov.cn), People's Bank of China. The authors are grateful to Elisabeth Noble, Jermy Prenio, Jeffery Yong, Jon Frost, Alain Otaegui, Timothy Shakesby, Musa Parmakisz, Joe Perry, Shunsuke Tani, Giuseppe Bianco and Lucia Russo. Charlotte Gardini provided valuable administrative support.

on data quality, they differ in approach: statistical accuracy in AI is based on likelihoods and predictions, whereas accuracy in data protection requires personal data to be correct and complete.

Data security – encompassing confidentiality, integrity and availability – is another core aspect of data protection frameworks. Organisations are required to implement robust security measures to safeguard data within information and communication technology (ICT) systems, which is especially important in AI settings given the scale and potential sensitivity of the data processed. Data breaches in such contexts can result in financial losses, reputational damage and legal repercussions. Furthermore, strong data security measures are essential for maintaining operational resilience.

Sound data governance forms the backbone of managing the complexities of data in AI, providing a strong foundation to support data quality, privacy and security. It establishes clear roles, responsibilities, processes and policies necessary to manage data effectively while ensuring compliance with regulatory requirements. A key aspect of data governance is accountability, a fundamental principle that requires organisations to take responsibility for how data are sourced, processed and used.

While relying on cross-sectoral data protection frameworks, financial authorities address AI data risks through a combination of approaches, often using established and largely non-prescriptive guidance. In addition to AI-related legislation and industry standards, international standards such as the Basel Committee on Banking Supervision's (BCBS) Principles for effective risk data aggregation and risk reporting (BCBS 239) serve as a key reference for robust data management. Building on these, authorities commonly rely on established supervisory and regulatory guidance for general data management, model risk management (MRM) and operational resilience, which includes cyber security, outsourcing and third-party risk management. They also frequently employ non-prescriptive approaches, such as thematic reviews and information papers, to highlight emerging good practices for managing data in AI. While specific supervisory expectations for AI data usage are not yet fully consistent, early signs of convergence are emerging in key areas, including data privacy, quality, security and governance.

Nonetheless, important challenges remain within the current policy framework for addressing AI data risks. Tensions persist between technological capabilities and existing data protection requirements, in particular in their practical application across different stages of the AI life cycle. Although data protection authorities are providing guidance, some requirements place demands that current AI technologies are not yet fully equipped to meet. Existing regulatory and supervisory frameworks designed for traditional data-related uses or earlier forms of AI might not fully capture the complexity of gen AI ecosystems. Third-party dependencies further complicate oversight due to limited data visibility across the AI supply chain, often compounded by market concentration among key providers.

To address AI data-related challenges, financial authorities could issue tailored guidance on data governance, quality, security and third-party dependencies. This may involve clarifying supervisory expectations for robust data governance frameworks and the application of data protection principles throughout the AI life cycle. Guidance on data quality could focus on strong data management processes, continuous quality assurance and clear standards for key data quality dimensions such as accuracy and completeness. Data security measures might emphasise the importance of effective incident response plans and integration of cyber security with data protection controls in AI environments. Supervisors could also strengthen expectations regarding third-party dependencies in AI ecosystems, including enhanced transparency on data lineage and monitoring of third-party providers. Additionally, authorities could foster industry understanding through thematic reviews and best practices. Over time, developing a comprehensive policy framework tailored to AI data issues would be particularly beneficial.

Enhanced collaboration between financial authorities and data protection authorities is vital given the cross-cutting and rapidly evolving nature of AI data challenges. Structured cooperation can promote regulatory consistency, reduce uncertainty and help mitigate the risk of cross-border fragmentation. Continued dialogue with industry stakeholders will also be key. The overall objective is to ensure that AI adoption in financial services supports innovation while reinforcing trust, resilience and financial stability.

Section 1 – Introduction

1. **Artificial Intelligence (AI) is reshaping the financial sector while further amplifying the critical role that data play.** As a key enabler of economic activity, the financial sector relies on its ability to collect, analyse and utilise data effectively to facilitate the flow of information and resources across the economy and to manage risks. Recent advances in AI, and in generative (gen) AI in particular, are transforming these processes by offering financial institutions diverse applications to improve productivity and efficiency, as well as to support risk management and regulatory compliance.[2]

2. **Gen AI relies on vast amounts of data.** Large volumes of diverse data are required at each stage of the gen AI life cycle. During development, data are used to train models, and during operation, they power deployed models. Data are also crucial for assessing model performance, identifying biases and refining algorithms. As such, data serve as a core factor that influences the capabilities, limitations and ongoing development of gen AI models.

3. **An important consideration in this context is the quality of data.** Poor data quality can result in inaccurate model outputs, which in turn can pose significant risks, in particular in high-stakes applications such as credit underwriting. While data quality is crucial for training machine learning (ML) models, it becomes even more critical as AI use cases grow in scope, complexity, scale and autonomy. Gen AI systems rely on large and heterogeneous data sets and are therefore particularly sensitive to deficiencies in accuracy, completeness and representativeness.

4. **At the same time, data used in AI systems include personal or sensitive information that is subject to legal, regulatory and ethical constraints.** Frameworks for data protection, privacy and security govern how such information may be collected, processed, stored and shared, imposing obligations that extend across organisational boundaries and throughout the AI life cycle. For financial institutions, ensuring compliance with these requirements, for gen AI applications in particular, has become both more challenging and more consequential as shortcomings can undermine consumer trust and damage their reputation, invite regulatory enforcement and erode their competitive advantage.

5. **The financial industry consistently identifies data-related challenges as major barriers to further AI adoption.** According to IIF-EY (2025), the top two challenges in deploying AI are data quality and data availability. Similarly, the 2024 report *Artificial intelligence in UK financial services* notes that four of the top five perceived risks are data-related: data privacy and protection, data quality, data security, and data bias and representativeness.[3] In South Africa, the banking and investment industry shares data-related concerns similar to those identified in the UK report, while in Europe, data governance risks associated with the use of gen AI in the banking sector, such as limitations on quality, reliability and privacy, have been highlighted as key concerns.[4]

6. **Several factors contribute to data-related challenges.** Over time, data protection[5] obligations have taken on an increasingly prominent role in the financial sector. Interpretation of these obligations in the context of AI has proven difficult and often lacks clear guidance. While some data protection authorities have begun issuing cross-sectoral guidance, these are typically domestic in scope, with only a few exceptions. This creates challenges for AI models, which often operate on a global scale, potentially

[2] See Crisanto et al (2024).

[3] See BoE-FCA (2024).

[4] See Hlophe and Mabetha (2025) and EBA (2024).

[5] For the purposes of this paper, "data protection" refers to the legal and institutional framework that governs the processing of personal data, aiming to protect individuals from unjustified interference in their private life. "Data privacy", on the other hand, is the underlying fundamental human right or value that individuals should have control over their personal data, a right that data protection frameworks are designed to uphold. As such, data protection has a broader scope, encompassing the entire life cycle of personal data along with aspects such as data quality, security and governance.

adding further complexity to compliance efforts.[6] Additionally, the cross-cutting nature of AI poses challenges for supervisory coordination and effective information-sharing between financial and non-financial authorities, in particular data protection authorities.[7]

7. **As financial institutions continue to explore AI use cases, supervisors are challenged to keep pace with AI and data-related developments**. Financial authorities are not only facing new challenges associated with the use of AI by their supervised institutions; they are also confronted more and more with data-related issues such as data protection and governance. While these issues typically fall under the remit of data protection authorities, they are relevant to financial authorities within the context of their mandates. For instance, AI-driven decisions in areas such as credit underwriting and customer onboarding that rely on poor-quality data may produce inaccurate outputs, potentially resulting in financial losses or consumer harm. Additionally, data breaches or other violations of data privacy in activities such as deposit-taking and payment processing could undermine customer trust. If widespread, such incidents could erode confidence in the financial system, ultimately posing risks to financial stability.

8. **This paper aims to enhance understanding of the role of data, its associated challenges and authorities' supervisory expectations regarding AI-related data usage, in the context of gen AI in particular.** It identifies the key emerging requirements and expectations for data use in AI within financial services, focusing on developments in China, the European Union (EU), Singapore, the United Kingdom and the United States. The remainder of the paper is structured as follows: Section 2 provides an overview of the role of data in AI within the financial sector, Section 3 highlights common themes in cross-sectoral data-specific obligations and emerging policy expectations for data use in AI, Section 4 reviews the guidance provided by financial authorities on the use of data in AI and Section 5 concludes.

Section 2 – The role of data in AI and the financial sector

Background

9. **Financial services are a data-driven industry.** Data underpin virtually all aspects of financial activity, from customer onboarding to credit assessment and insurance underwriting, fraud detection and anti-money laundering (AML) surveillance, and prudential risk management. As part of these activities, financial institutions routinely collect, process and analyse vast amounts of data from consumers. This includes personal and financial information; transaction records; and increasingly alternative data such as digital footprints, geospatial data or information acquired through third parties (eg e-commerce platforms, vendors) through partnerships, application programming interfaces (APIs) or mergers.[8] These data are essential to bridge information gaps, offer tailored products and services to customers, support decision-making, manage risks and facilitate the efficient allocation of credit.[9]

10. **Data used by financial institutions come in various forms.** They include structured data such as financial records, personal identity information or balance sheet figures; semi-structured data like XML files or event/incident logs; and, less frequently, unstructured data, which lack a pre-defined format, such as emails and social media posts. Data can be proprietary to the financial institution, publicly available or

[6] However, this is not always the case. Some models follow a "gold standard" principle, while others are customised for local use cases without necessarily introducing significant complexities.

[7] See for example OECD (2026).

[8] See Jeng et al (2025).

[9] See Haksar et al (2021).

privately held by individuals or organisations.[10] They may be collected directly, sourced from third parties or, less frequently, generated as synthetic data, mimicking the statistical properties of "real-world" data (Box 1).[11]

11. **A specific category of data is personal data.** Data relating to natural persons are often subject to data protection requirements for their collection, storage and use, aimed at safeguarding individuals' right to privacy.[12] These requirements may be stricter for the processing of particularly sensitive personal data, such as health or biometric information.[13] In contrast, non-personal data are not subject to these restrictions, albeit some jurisdictions regulate their handling.[14] However, the distinction between personal and non-personal data is not always clear. This ambiguity arises because some data (eg geolocation data) are not inherently personal, but they become personal when processed for a specific purpose or in a specific way.[15] Moreover, questions persist as to whether inferred data (eg default risk attributed to a potential borrower by an AI model) should be considered new personal data, distinct from the data from which they have been inferred.[16]

12. **To enable the use of personal data in advanced AI models, measures to mitigate privacy risks are increasingly used, but they are not a silver bullet.** For instance, well known privacy-enhancing and privacy-preserving technologies (PETs/PPTs) include anonymisation (removal of individuals' identifiers), pseudonymisation (substituting individuals' identifiers with codes), differential privacy (introducing statistical protections to outputs so individuals' information cannot be reverse-engineered) and homomorphic encryption (techniques that allow computation on encrypted data). While foundational PETs/PPTs are increasingly used in financial institutions, more sophisticated methods remain unevenly adopted, often limited to pilots or niche applications. At this stage, PETs/PPTs have proven effective in reducing baseline privacy risks, but they involve trade-offs in accuracy, complexity and cost. For example, anonymisation can disconnect data from individuals, but it reduces data utility for certain applications,[17] giving rise to a quality-privacy trade-off[18] while carrying the risk of re-identification due to advancements in AI.[19]

[10] For the purposes of this paper, "organisations" refers to entities – such as companies, institutions, firms or other legal bodies – that are involved in the collection, use, storage or processing of data.

[11] EDPB (2024b) differentiates between "first-party data" (personal data which the controller has collected from the data subjects) and "third-party data" (personal data that controllers have obtained from a third party, for example from a data broker or collected via web scraping). For more information on the use of synthetic data for models in financial services, see FCA (2025).

[12] For example, under the EU's General Data Protection Regulation (GDPR), personal data consist of any information relating to an identified or identifiable natural person.

[13] Data protection laws typically impose stricter requirements on the processing of sensitive data, often requiring specific consent. For instance, in the EU, the GDPR prohibits the processing of certain categories of data – such as those related to health, race or sexual orientation – unless specific conditions are met, eg obtaining explicit consent from the individual. Additionally, any use of AI to process such data must rely on one of the specific derogations outlined in Article 9 of the GDPR. For elements included in sensitive data definitions, see United Nations Conference on Trade and Development, *G20 members' regulations of cross-border data flows*, March 2023, Table 1.

[14] For example, the EU regulates non-personal data, inter alia, through the Data Act and the Data Governance Act. Additionally, the European Data Union Strategy includes a legislative proposal to update and consolidate EU data rules.

[15] See Rupp and von Grafenstein (2024).

[16] In the EU, the view that inferred data constitute personal data was endorsed by the Article 29 Working Party (WP), predecessor to the European Data Protection Board (EDPB). See Article 29 Datra Protection Working Party, *Opinion 4/2007 on the concept of personal data*, June 2007.

[17] Anonymisation can affect the usefulness of data, decreasing the quality of AI results. See Patchipala (2023).

[18] See Perlov (2024).

[19] The EU GDPR acknowledges the risk of re-identification, highlighting that anonymised data must be treated as personal data if they become identifiable due to technological advancements. Even before AI, Sweeney (2002) showed that linking four shared attributes (ie date of birth, gender, zip code) contained in two separate databases makes it possible to re-identify individuals.

Box 1

Alternative and synthetic data

As large-scale internet-based data become increasingly saturated, attention is shifting from accessibility to alternative data sources. Two developments are shaping this shift. First, gen AI models are rapidly consuming web-based data, and second, websites are increasingly introducing limitations to data scraping.① These trends have a significant impact on gen AI model performance by limiting access to new data sets and reducing data diversity, which could hinder their progress and scalability.

In response, gen AI developers are entering into data licensing deals, purchasing data from a variety of companies.② However, access to curated and domain-specific data sets might not fully satisfy the growing demand for continuous gen AI model training. Compounding the issue, many companies and governments face difficulties in making their data usable for gen AI purposes, as they often remain siloed, unstructured, unlabelled and not machine-readable.

Similarly, gen AI is increasingly relying on synthetic data, ie artificially generated data that mimic real-world data while preserving their statistical properties. Gen AI developers and deployers continue to improve techniques aiming at using AI-generated synthetic data as a supplement to or replacement of real data.③ This approach offers several advantages. It helps address data limitations, enhances privacy, reduces biases and supports model training, testing and validation in areas where real data are scarce or pose privacy and compliance risks. However, research highlights potential challenges with this approach, pointing out that "indiscriminate use of model-generated content […] causes irreversible defects in the resulting models" by reducing gen AI's ability to accurately predict low-probability events.④

To overcome challenges related to the use of alternative data sources and synthetic data in gen AI, institutional initiatives are being explored. In Europe, several initiatives are under way to improve access to financial data for a broader audience, such as the European single access point (ESAP) and the EU Data Hub.⑤ While the ESAP, led by the European Securities and Markets Authority (ESMA), will provide centralised access to aggregate financial and sustainability-related information from companies across the EU, the Data Hub will enable market participants to access supervisory data upon request, eg for gen AI model testing. To ensure compliance with confidentiality requirements, the European Commission (EC) has decided to build the Data Hub using synthetic data generated from the original confidential data held by national competent authorities.⑥

In the financial sector, several authorities have begun to set expectations for the governance of alternative and synthetic data used in gen AI models. In the United States, financial regulators issued an inter-agency statement on the use of alternative data in credit underwriting, noting that a well designed compliance management programme provides for a thorough analysis of relevant consumer protection laws and regulations to ensure firms understand the opportunities, risks and compliance requirements before using alternative data.⑦ In the United Kingdom, the Financial Conduct Authority's (FCA) report on synthetic data for models in financial services highlights the absence of a dedicated governance framework and encourages practitioners to build on existing model risk management and data and AI ethics frameworks. The report outlines three key governance considerations: establishing robust frameworks, controls and processes; assigning clear roles and accountability; and maintaining comprehensive and transparent documentation throughout the synthetic data life cycle.⑧

① See Reuel (2025). ② See Posnett (2025). ③ See EC (2025a). For example, a technique used in connection with synthetic data is data set condensation. Broadly speaking, this technique generates a small synthetic training set from a large one. An advantage of condensation is that the confidentiality of original data is preserved because synthetic data are generated as output. Nonetheless, condensation is extremely challenging in terms of computation, limiting its applicability at present when it comes to very large data sets. ④ Shumailov et al (2024). ⑤ See ESMA et al (2025) and EC, "Data Hub", *EU Digital Finance Platform*, digital-finance-platform.ec.europa.eu/data-hub. ⑥ A useful point of reference in this context are the FAIR Guiding Principles for scientific data management and stewardship, which aim to improve the findability, accessibility, interoperability and reuse of digital assets. See GO FAIR, *FAIR Principles*. ⑦ See FRB et al (2019). ⑧ The FCA created the Synthetic Data Expert Group (SDEG) in March 2023, bringing together 20 experts from across financial services, the public sector, data and technology vendors, and consumer groups to explore synthetic data use in financial markets. For more information, see FCA (2025).

Use of data in AI systems

13. **Data form the foundation of AI models, serving as the raw material for their development and refinement.**[20] Traditional AI, such as classical ML models (eg decision trees), uses structured data – generally proprietary business data – to detect patterns, make predictions or classify information based on statistical relationships. In contrast, advanced forms of AI, such as gen AI, rely on massive and diverse data sets, often including public, unstructured and multimodal data (combining text, images, audio, video), to train models through a series of complex, multi-step processes.[21] These models can generate new content or insights and handle a broader range of tasks with greater flexibility and autonomy.

14. **The financial services industry has been using traditional AI for decades.** Early applications, such as credit scoring models and algorithmic trading, relied on structured data and traditional AI to automate decision-making and improve efficiency.[22] Over time, AI use expanded to areas like customer service, AML/CFT and fraud detection. Beyond these applications, in the EU, banks also use AI to profile and cluster clients based on their behaviour, preferences or transaction/credit history, as well as to detect anomalies in transaction patterns that may indicate operational errors.[23] As of September 2025, around 92% of EU banks – based on a sample of 85 institutions – deploy AI, primarily using traditional AI.[24]

15. **Gen AI is transforming financial services, with growing potential beyond internal applications.** The current use of gen AI in financial services is primarily focused on internal use cases, such as improving staff productivity and detecting suspicious transactions. However, while traditional AI continues to underpin many financial operations, financial institutions are increasingly investing in gen AI to expand its external applications, including core business and revenue-generating activities.

16. **Advances in gen AI have been driven by a combination of significant growth in computing power, substantive progress in model architecture and access to extensive and diverse data sets**. These developments have been supported by the expansion of key technological infrastructure such as cloud computing. This has allowed financial institutions to better leverage their data resources so that gen AI models can be refined for financial use cases.[25] The ability to take greater advantage of data resources has also benefited from substantive improvements in data curation techniques, including:

- more efficient **data storage** to organise large amounts of data such that AI models can easily and efficiently access and process them during training;
- improved **data cleaning** processes to help remove errors, duplicates, and inconsistencies or irrelevant information from data sets;
- more systematic **data labelling** practices to ensure data sets are correctly tagged or annotated so that the AI model can understand the meaning or context behind the data and therefore learn meaningful patterns and produce outputs that reflect the intended task;
- improved **metadata management** to document and organise information about the data such as their location, format and structure, ownership, access rights, and creation and update dates; and

[20] See EC (2025a).

[21] See McKinsey & Company (2025).

[22] For a description of the evolution from traditional statistical models to deep learning, see Liu (2025). For an assessment of how gen AI will affect finance, see Aldasoro et al (2025).

[23] See EBA (2024).

[24] See EBA (2025).

[25] See IIF (2024).

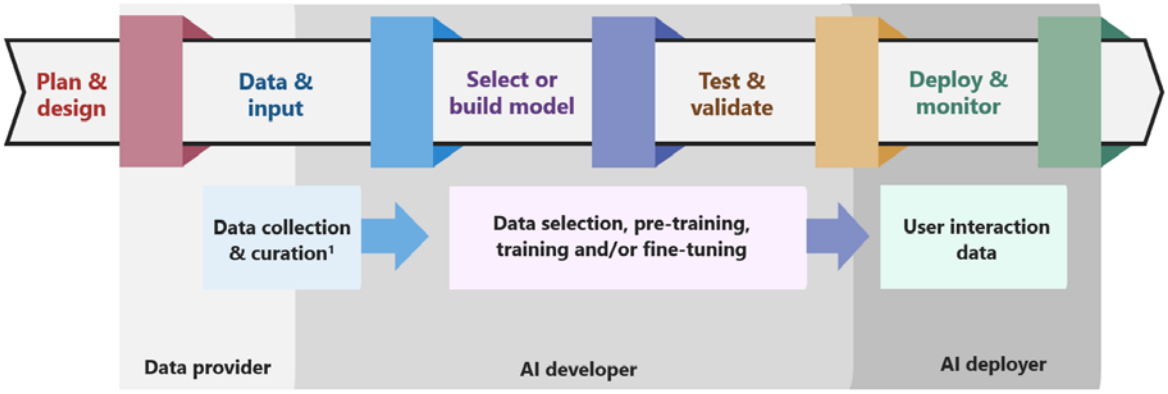
- enhanced **data provenance or lineage** tracking, building upon metadata, to provide transparency on where data come from, how they have been processed and how they flow through the AI system.

17. **Data play a key role at every stage of the gen AI life cycle, from model training to deployment and use.** During training and testing, large volumes of structured and unstructured data enable models to identify complex relationships and patterns. In the fine-tuning and deployment phases, domain-specific data (eg financial transactions or customer interactions) may be used to adapt the model to particular use cases. Moreover, data generated during the use of the model can be used to help improve the accuracy and performance of the model.

18. **Several key stakeholders play a critical role in sourcing and managing data throughout the gen AI life cycle**. These include the following:

- **Data providers** are responsible for supplying data sets that underpin model development and fine-tuning, including ensuring their relevance, quality and legality**.** These can include external vendors providing market data, credit bureau information or fraud indicators; public sector agencies; and institutions that provide access to their proprietary data sets. In the financial sector context, data providers can also include internal business units such as retail and corporate banking, payments, risk and compliance functions.
- **Model developers/providers** (referred to as developers throughout this paper) are generally third-party technological providers such as OpenAI, Anthropic, Google and DeepSeek. They are primarily responsible for the initial stages of the gen AI life cycle, in particular for the selection, pre-processing and curation of data for training and fine-tuning purposes. Model developers are typically accountable for how data choices influence model behaviour, bias and performance.
- **Model deployers** (referred to as deployers throughout this paper) are typically financial institutions themselves, which embed gen AI models in internal productivity applications, customer service tools and compliance monitoring frameworks where additional data may be generated through user interactions, feedback loops and monitoring processes. Model deployers assume responsibility for how AI models use and generate data in practice, and therefore address data shortcomings or misuse through ongoing monitoring of model outputs.

The role of data across different stages of the gen AI life cycle — Graph 1



[1] Includes storage, classification, cleaning, labelling, metadata and provenance.

Source: FSI staff.

Data challenges in AI systems

19. **A long-standing challenge for financial institutions lies in the fragmentation of their many data sources.** For instance, core banking systems often operate on legacy mainframes with rigid batch-based data structures, while front-office digital channels (eg mobile apps and online banking platforms) generate event-based data with every customer interaction. Similarly, insurance firms rely on multiple data sources, including policy administration systems, claims handling systems and customer relationship management platforms, which often fail to integrate seamlessly. This lack of cohesion stems from fragmented technology stacks, reliance on legacy systems that store data in silos, inconsistent data entry practices, the absence of standardised definitions and taxonomies, and shortcomings in data accountability frameworks.[26] Digital-native banks and insurers, however, may have an advantage in managing and leveraging data effectively, thanks to their legacy-free, often cloud-based infrastructure.

20. **With the increasing use of gen AI in the financial industry, long-standing data-related challenges are amplified and new ones are introduced.** Persistent data-related challenges in the financial industry have long resulted in inconsistent data quality and hindered analytics and automation efforts. With the scaling and integration of gen AI into financial services, these challenges are becoming increasingly pronounced. According to IIF-EY (2025), 79% of financial institutions identify data quality as a key barrier to launching AI solutions in production and, within data quality, issues such as "noisy, untimely, inaccurate and inadaptable data" were selected by 96% of firms as the primary obstacle, followed by the lack of labelled data (94%). Moreover, gen AI's reliance on large-scale data sets and its unique life cycle exacerbate existing governance issues, and the growing importance of alternative and synthetic data also comes with a range of new challenges (Box 1).

21. **The most pressing AI data-related risks arising from the increasing integration and scaling of gen AI in financial services are data quality, privacy and security risks.**

- **Data quality risks:** The quality of training data is an essential factor in the development and deployment of reliable and trustworthy gen AI. The accuracy, completeness and representativeness of both training and operational data sets have a large impact on the performance, reliability and fairness of gen AI systems. Even the most advanced algorithms can deliver poor results if the training data fail to meet these requirements. However, assessing data quality is often difficult as training data sources may be opaque or completely unavailable, which is often the case for pre-trained models. AI models also risk degradation if their training data sets no longer represent current realities (data drift) or contain excessive amounts of AI-generated content. Moreover, poor data quality can lead to unintended bias or, more generally, the reinforcement of harmful stereotypes due to different preferences around data-sharing. For example, it appears women are much more reluctant than men, and older people much more reluctant than younger people, to share personal data in exchange for better offers on financial services, which can result in data sets that are biased against women and older consumers.
- **Privacy risks:** The processing of personal data at different stages of the gen AI life cycle generates unique risks that require careful management and oversight. Personal data may be collected, processed, exposed or transformed in different ways depending on the stage of the gen AI life cycle, giving rise to significant privacy, ethical and compliance concerns. During model training, personal data may be inadvertently captured or retained within data sets, creating potential breaches of privacy or data protection laws. In the deployment/use phase, the use of real-time personal information to generate outputs can result in unethical or unlawful profiling, discrimination or unintended disclosure. Moreover, stored or derived personal data may be repurposed in ways that are inconsistent with original consent. These risks are magnified in gen AI, where models can reproduce or infer sensitive information from training data.

[26] See Mittal (2025).

- **Security risks:** Financial institutions' growing reliance on AI increases their exposure to cyber attacks and exploitation by malicious actors, underscoring potential security risks. Malicious actors may exploit vulnerabilities through data poisoning (introducing harmful material into training data sets to degrade model performance or disseminate misinformation) or through indirect prompt injection attacks (embedding hidden commands that deceive AI models into disclosing unauthorised information such as confidential data). While attacks during the training and development phases of gen AI models are complex and less likely, the risks become more pronounced post-deployment.[27] Moreover, risks can arise from the external hosting and storage of data. While such data are typically stored securely, for example in cloud facilities, inadequate safeguards can lead to breaches, exposing proprietary, confidential or sensitive client information. Such breaches can result in intellectual property loss, legal repercussions, regulatory fines and diminished customer trust.

22. **Third-party dependencies exacerbate AI data-related risks.** The reliance on third parties for the development and deployment of gen AI systems amplifies challenges in managing data-related risks. As these systems increasingly depend on training data sourced or managed by third parties, the potential for quality deficiencies, security breaches and privacy violations grows. External data providers may apply inconsistent standards for data curation, validation or protection, resulting in unreliable or biased inputs that undermine model performance and trustworthiness. Moreover, limited transparency around data provenance and handling practices makes it difficult for financial firms to verify the accuracy of tools; ensure compliance with privacy, data governance, data quality and cyber security requirements; and maintain explainability and human oversight. For instance, bias often originates during the training of foundation models, restricting the deployer's ability to address it. Intellectual property risks also emerge from undisclosed training data, further compounding these challenges.[28]

23. **The concentration of AI and data services among a few large providers, including big techs and cloud service providers, complicates the management of third-party dependencies.** Third-party service providers already hold dominant positions in the market, and there is growing potential for non-horizontal mergers to result in firms consolidating data on the same or similar consumers from vastly different domains, such as payments, health data, geolocation, social media and search history.[29] The widespread use of a small number of cloud service providers introduces additional challenges, in particular when data are transmitted across jurisdictions with differing legal and regulatory safeguards.

24. **The intersection of open finance frameworks and gen AI systems presents opportunities for data availability while raising important considerations around data quality, privacy and security.** By enabling customer-authorised financial data-sharing across institutions through APIs, open finance enhances data portability and interoperability and potentially increases the volume and granularity of data available for gen AI models. At the same time, it can introduce new data quality challenges through, for instance, inconsistent data standards and differences in data completeness across institutions. Moreover, the wider circulation of sensitive financial information across interconnected platforms may amplify privacy and security risks, especially when open finance data are combined with external or unstructured sources in gen AI systems. Therefore, as open finance frameworks expand and increasingly intersect with advanced AI systems, these dynamics may have broader implications for the integrity, confidentiality and reliability of the data underpinning such systems.

25. **Challenges connected with copyrighted information and localisation, as well as the limited availability of relevant skills, further amplify AI data-related risks.** The training of gen AI systems has thus far relied predominantly on publicly available data drawn from the internet. While this approach has

[27] For example, malicious actors may manipulate gen AI tools that learn from user interactions, influencing them to spread misinformation or produce harmful outputs.

[28] See eg Heikkilä (2026).

[29] See Jeng et al (2025).

enabled rapid progress in model development by providing scale and diversity, it has introduced significant challenges since these data often contain copyrighted information, exposing AI developers to potential legal liabilities.[30] In addition, data localisation policies, which restrict where data can be stored and processed, may limit cross-border data flows and constrain the diversity and scalability of gen AI systems.[31] Another key challenge relates to the availability of appropriately skilled staff to deploy and oversee AI systems, which remains a major challenge for the financial industry.[32] In particular, many firms report difficulties in filling the roles of AI ethics specialists, AI data scientists and data architects.[33] While these challenges are significant, they are not examined further in this paper as they largely fall outside the direct influence of financial authorities.

26. **Taken together, data-related shortcomings can erode the potential benefits of gen AI in the financial sector by exacerbating consumer protection risks as well as micro- and macroprudential risks**. As argued above, the quality of data used to train and use AI models affects their performance, integrity and fairness. Relevant shortcomings in this domain can lead to biased or inaccurate outputs, amplifying consumer protection risks through discriminatory decisions or inaccurate advice.[34] Poor data quality or lack of data integrity may also undermine prudential soundness by weakening MRM.[35] Data security vulnerabilities can expose institutions to cyber and other operational risks. Traditional AI data governance frameworks are not typically designed to oversee the additional layers of complexity and exposure generated by the use of large and diverse public and private data sets in advanced AI systems.[36] Also, an important human factor consideration is that overreliance on gen AI outputs may obscure accountability and impede effective oversight. At a system-wide level, heavy reliance on similar data sources (and models) may increase herding behaviour and concentration, with implications for financial stability.

Section 3 – Key themes in cross-sectoral guidance on use of data in AI

27. **The critical role that data play in AI has attracted the attention of policymakers.** This role raises questions about how to ensure compliance with data regulations and meet the expectations of data protection authorities when building and implementing AI systems. There is also a growing recognition that obligations under these regulations may need to be interpreted and applied differently in different phases of the AI life cycle.[37] Against this background, data protection authorities have started providing guidance on how to apply their requirements in the context of AI.

28. **Data protection has been an area of policy attention since well before the advent of AI, with a key role played by the OECD in fostering international cooperation.** The OECD has been instrumental in establishing global principles for both data protection and AI. Its Privacy Guidelines, first

30 In this regard, Reuel (2025) featured research conducted on 1,800 text data sets widely used for training foundation models. This research found that more than 70% of data sets on popular data set hosting sites such as GitHub and Hugging Face lacked adequate licence information, while 50% of the licences were miscategorised.

31 See IRSG (2026) and BoE (2026).

32 According to IIF-EY (2025), availability of skilled staff ranks very high among the challenges for the financial industry in deploying AI, especially for global systemically important banks and insurance companies.

33 See Singla et al (2025).

34 See EBA (2025).

35 The probabilistic nature of gen AI models introduces reproducibility challenges that sit in tension with existing MRM and validation expectations.

36 See McKinsey & Company (2025).

37 See CIPL (2024b).

adopted in 1980 and revised in 2013, provide a framework for safeguarding personal data while promoting their free flow across borders.[38] In 2019, the OECD adopted the OECD AI Principles (updated in 2024), the first intergovernmental standard on AI, to promote the use of trustworthy AI that respects human rights and democratic values.[39] In 2024, the OECD and the Global Partnership on Artificial Intelligence (GPAI) joined forces under the GPAI brand to create an integrated partnership. Bringing together 44 countries, the GPAI facilitates collaboration between policymakers and AI experts, bridging the gap between theory and practice in AI policy.[40] An Expert Group on AI, Data and Privacy brings together leading experts from data protection authorities, policymakers, industry, civil society and academia to provide insights into potential synergies in these domains.

29. **International forums of data protection authorities stress that data protection principles remain applicable to AI products and services even as jurisdictions develop AI-specific policies.** Over the years, the Global Privacy Assembly (GPA), a global forum for data protection authorities, has adopted numerous resolutions addressing emerging challenges in AI (Box 2). These resolutions consistently emphasise the importance of upholding data protection and privacy principles in the development and use of AI systems.[41] Additionally, the resolutions affirm that data protection authorities have jurisdiction over AI systems when the processing of personal data is involved.[42] In other words, whenever an AI system uses personal data, all of the standard provisions of the relevant data protection framework apply, with oversight provided by national data protection authorities.[43]

Box 2

International cooperation on data protection and privacy in AI

Established in 1979 as the International Conference of Data Protection and Privacy Commissioners, the Global Privacy Assembly (GPA), an international forum comprising over 130 accredited member authorities, serves as a platform for collaboration and knowledge-sharing among global data protection authorities. The GPA's primary objectives include promoting consistent, high-level data protection standards, fostering enforcement cooperation and enhancing members' capacities to safeguard data subjects in an era of rapid digitalisation and advancing technologies.

In its 2018 *Declaration on ethics and data protection in artificial intelligence*, the GPA held that respect for the rights to privacy and data protection are increasingly challenged by the development of AI and that these challenges reinforce the need for the adoption of an international approach and standards in order to ensure the promotion and protection of human rights in all digital developments at the international level.① It also called on data protection and privacy enforcement authorities to coordinate their efforts to influence the development and implementation of global data protection and privacy measures and to take appropriate actions when necessary.

38 The OECD Privacy Guidelines have inspired data protection frameworks around the globe. The OECD also promotes cooperation on privacy and data governance across its member countries and beyond, addressing challenges such as cross-border data transfers, enforcement, and cross-border and cross-sectoral cooperation. For more information, see OECD (2023).

39 See OECD (2019). To advance these principles, the OECD has advanced research, analytical work and knowledge-sharing, including through a network of experts and the OECD.AI Policy Observatory.

40 See OECD (2024a).

41 The GPA often addresses "data protection" and "data privacy" together and sometimes uses the terms interchangeably or in overlapping ways in its resolutions. This likely reflects the distinct but interconnected nature of these concepts. While data protection focuses on the legal and institutional frameworks for managing personal data, privacy refers to the fundamental human right to control personal information and protecting individuals from undue intrusion. By including both terms, the GPA may aim to emphasise its commitment to addressing both the regulatory and rights-based dimensions of personal data management. For simplicity, this paper uses the term "data protection" even when the GPA refers to "data protection and privacy", except in Box 2.

42 See GPA (2024).

43 See CIPL (2020).

To promote understanding and adherence to the principles outlined in the 2018 resolution, the GPA established the Permanent Working Group on Ethics and Data Protection in Artificial Intelligence in 2018.② Responding to the increasing use of data for AI, the GPA adopted and published a series of resolutions on AI, including on gen AI systems and the collection, use and disclosure of personal data.③

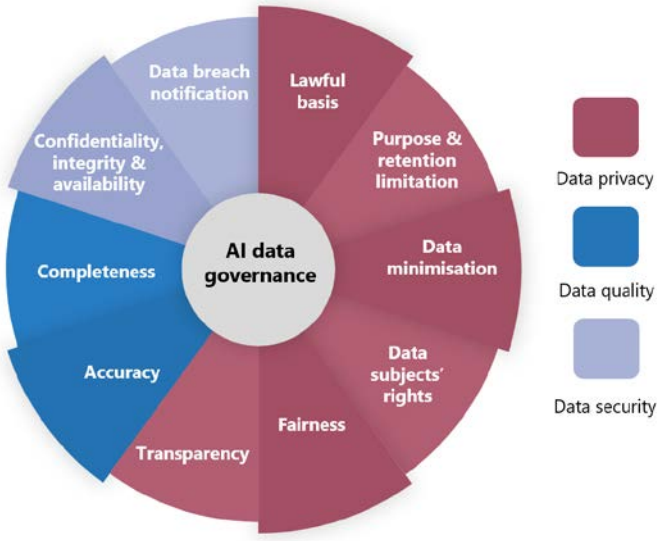
In addition to participating in the GPA, data protection authorities have launched collaborative initiatives to address shared challenges in personal data protection and privacy in AI. In October 2024, the G7 Data Protection and Privacy Authorities (G7 DPAs) adopted an Action Plan, emphasising the need for joint efforts to strengthen data protection and privacy in key technological domains like AI.④ By June 2025, they had highlighted the importance of embedding privacy considerations from the earliest stages, in particular in the design, development and deployment of new technologies.⑤

① See GPA (2018). ② The mandate of this working group includes promoting understanding of and adherence to the principles outlined in the 2018 resolution among all stakeholders in AI development. For its latest report, see GPA (2025a). ③ Key resolutions in the context of AI include: GPA (2020), GPA (2023), GPA (2025b) and GPA (2025c). See adopted resolutions of the GPA. ④ See G7 DPAs (2024). ⑤ See G7 DPAs (2025). For other initiatives, see OAIC (2025).

30. **Data protection is widely regulated across jurisdictions, though the scope of these frameworks varies**. According to the International Association of Privacy Professionals (IAPP), as of January 2025, 144 countries have enacted national data privacy laws, covering about 82% of the world's population (IAPP (2025)). This includes four of the five jurisdictions in the scope of this paper (ie China, the EU, Singapore and the United Kingdom), where legislation establishes wide-ranging frameworks for the protection of data. In the United States, given the absence of a comprehensive federal data protection law, data protection is governed primarily by state-level regulations.[44] This is complemented by sectoral federal laws that regulate the circumstances under which financial personal information can be processed and shared.

31. **Against this background, data protection authorities have issued cross-sectoral guidance to address the intersection of data requirements and AI.** This guidance aims to clarify how data principles apply in the context of AI, the challenges AI poses for compliant data management and governance, and ways to resolve potential conflicts between data requirements and AI practices. Key themes identified include data privacy, quality, security and governance (Graph 2).

Main themes in cross-sectoral data guidance — Graph 2



Source: FSI staff.

[44] Nineteen states have passed data privacy laws. For details, see IAPP, *US state privacy legislation tracker 2025*, November 2025.

Data privacy

32. **Data privacy refers to the principle that individuals should have control over their personal data.** It includes the ability to determine how data are collected, stored, processed and shared. As such, data privacy embodies the ethical management of data, ensuring transparency about why data are collected, how they are used and the measures taken to protect them from misuse. At its core, data privacy is rooted in societal values. As such, the interpretation and implementation of data privacy principles can vary across jurisdictions, reflecting cultural norms and legal frameworks.[45]

Lawful basis

33. **Organisations are generally required to establish a lawful basis for processing personal data, typically by obtaining the consent of the individuals concerned.** Personal data may only be collected, used or disclosed with the consent of the individual concerned, unless they have been effectively anonymised, in which case they can be processed without consent. Alternatively, organisations may also rely on other lawful bases for processing, depending on the applicable data protection framework.[46] In the United States, while there is no national privacy law, various other laws impose requirements that restrict the processing of personal data.[47]

34. **When developing or deploying AI systems, organisations also need to identify an appropriate legal basis for their data processing activities even if data are publicly available.** The GPA emphasises that the collection of personal data for the pre-training, training and fine-tuning of AI models must be lawful, even if the data are publicly accessible. It further stresses that the public availability of personal data does not automatically constitute a lawful basis for processing, which must always be assessed in the light of the data subject's reasonable expectations of privacy.[48] In the EU, the European Data Protection Board (EDPB) clarified that AI models trained on personal data cannot, in all cases, be considered anonymous, and their anonymity must be assessed on a case by case basis.[49]

35. **The same principles apply to gen AI.** According to the GPA, developers and deployers of gen AI systems must identify the legal basis for processing personal data at the outset if a model is not deemed anonymous. This includes the processing of data related to (i) the collection of data used to develop gen AI systems; (ii) training, validation and testing data sets used to develop or improve these systems; (iii) individuals' interactions with gen AI systems; and (iv) content generated by gen AI systems.[50] In China, providers of gen AI services are required to use "legitimate data sources" for training activities such as pre-training and optimisation. When personal information is involved, they are required to obtain the individual's consent or otherwise comply with applicable laws and regulations.[51]

[45] For example, some jurisdictions may prioritise individual consent and control, while others may emphasise welfare gains resulting from efficient use of data.

[46] See "Principle (a): Lawfulness, fairness and transparency" in ICO (2023c).

[47] While no federal data protection framework exists in the United States, the processing of financial personal data may be subject to sector-specific laws. For instance, the Gramm-Leach-Bliley Act (GLBA) governs financial institutions by regulating the collection, use, protection and disclosure of non-public personal information. Similarly, the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA) require companies to implement programmes to mitigate identity theft risks and prevent unauthorised access to consumer reports.

[48] See GPA (2025b).

[49] The EDPB also provided guidance on the implications of unlawfully processing personal data during the development phase of an AI model and how it may affect the lawfulness of the model's subsequent operations (EDPB (2024b)).

[50] See GPA (2023).

[51] See Article 7(1) of Cyberspace Administration of China et al (2023). The term "legitimate data sources" refers to data obtained in compliance with the requirements of various applicable laws, including the Data Security Law (2021), in particular Articles 32 and 33, and the Personal Information Protection Law (PIPL) (2021).

36. **AI developers often rely on "legitimate interest" as the legal basis for processing personal data, especially when other lawful bases are unavailable.** AI developers frequently use publicly accessible sources, such as web-scraped data, for training purposes. This often makes it challenging to meet the conditions required for other legal bases. However, relying on legitimate interest requires data-collecting organisations to balance the necessity of processing personal data against the rights and interests of individuals.[52] Under the EU General Data Protection Regulation (GDPR), this involves meeting three cumulative conditions: identifying the legitimate interest, assessing whether processing is necessary for that purpose and determining whether the individual's interests override it or not.[53] The proposed Digital Omnibus Regulation, once enacted, would explicitly clarify that processing personal data for the development and operation of AI systems may rely on legitimate interest as a lawful basis.[54]

Purpose limitation, data minimisation and retention limitation

37. **Purpose limitation, data minimisation and retention limitation are closely interconnected principles that ensure responsible handling of personal data.** The principle of purpose limitation requires organisations to collect, use or disclose personal data only for specified and explicit purposes, ensuring data are not processed in ways incompatible with those purposes. This principle aims to provide individuals with clarity on how their data are used and to ensure that data processing aligns with their expectations. The principle of data minimisation requires organisations to limit their data collection to what is strictly necessary to fulfil the intended purpose.[55] Lastly, the principle of retention limitation reinforces these principles by requiring that personal data be retained only for as long as necessary to achieve the intended purpose, after which they must be deleted or anonymised.

38. **Although gen AI models typically require substantial amounts of data, the data minimisation and retention limitation principles restrict them to what is strictly necessary.** These principles oblige AI developers and deployers to limit the collection, processing and retention of personal data to what is strictly necessary to achieve the intended purpose.[56] As emphasised by the GPA, the collection and use of personal data must be limited to only what is reasonably necessary to fulfil a legitimate, specific and explicit purpose, and data must only be used or disclosed for the purpose(s) for which they were originally collected. Any further use or disclosure must be compatible with the initial purpose, authorised by the data subject through consent or permitted by law, while also aligning with the individual's reasonable expectations and having a lawful basis (GPA (2025b)).

39. **The intended purpose and risks of using personal data to develop gen AI models may vary and may be assessed at every stage of their life cycle.** The GPA advises that personal data should not be collected or processed indiscriminately. They can be used as training data only if required to achieve the gen AI model's intended purpose and following a comprehensive data protection and privacy impact assessment to identify, assess and address the risks posed by these systems at every stage of their life cycle.[57] In the United Kingdom, the Information Commissioner's Office (ICO) advises organisations to define sufficiently specific and explicit purposes for the data for each stage of the AI life cycle (Graph 3).

[52] "Legitimate interest" differs from other lawful bases as it is not linked to a specific purpose, such as fulfilling a contract, safeguarding vital interests or performing a public task. Unlike consent, it does not depend on the individual's explicit agreement. See ICO (2023b) and EDPB (2024a).

[53] EDBP (2024b) offers guidance for data authorities on assessing the use of legitimate interest as a legal basis for data processing in AI development and deployment.

[54] In November 2025, the EC introduced the Digital Omnibus package, which clarifies that processing personal data in developing and operating AI systems may rely on legitimate interest as a lawful basis under Article 6(1)(f) of the GDPR, provided appropriate safeguards are in place and without overriding consent requirements under EU or national law. See EC (2025c).

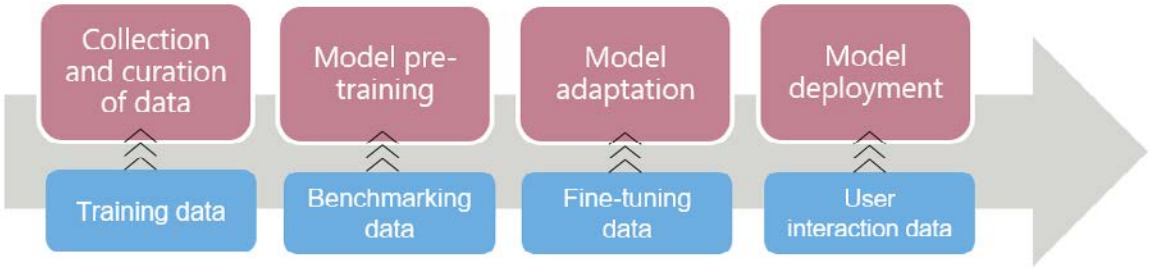
[55] In China, Article 6 of PIPL requires that the "collection of personal information shall be limited to the minimum scope necessary to achieve the purposes of processing, and excessive collection of personal information is prohibited".

[56] See EDPB (2024b) and Barberà (2025).

[57] See GPA (2023).

In addition, given that a single gen AI model can give rise to different applications, organisations are advised to distinguish between developing the model, creating an application based on it and identifying what types of data are used and how they are processed at each stage.[58]

Purpose limitation in gen AI: Data types and purposes across different stages — Graph 3



Source: Authors' conceptualisation. Adapted from ICO (2024a,b,c).

Data subjects' rights

40. **Individuals have a range of rights under data protection laws, aimed at giving them control over their personal data.** These rights include the right to be informed, right of access, right to rectification, right to erasure, right to restrict processing, right to object and rights related to automated decision-making and profiling.[59] Organisations are required to ensure mechanisms are in place to facilitate the exercise of these rights where provided by law at all stages of data processing, including where personal data have been used in the pre-training, training and fine-tuning of an AI model.[60] These rights apply not only to data used during training but also to data generated after deployment.[61]

41. **The right to be informed requires organisations to provide individuals with information about the collection and use of their personal data, whether collected directly or from other sources.** It requires organisations to inform individuals about any use of their personal data, including the purposes of using data for AI, and, where AI is used to make automated decisions, the likely impact on individuals.[62] However, exceptions to this right exist, such as when providing privacy information to each individual would be impossible or involve disproportionate effort, as may be the case with web-scraped data sets.[63]

42. **The right of access gives individuals the right to obtain a copy of their personal data held by an organisation.** This may include the right to receive additional information such as how their data have been used or disclosed. In the EU, this is known as a subject access request, which allows individuals to receive their data and verify that they are being processed lawfully. This right also extends to AI models, requiring developers to respond to individuals' requests for access to their personal information. In the United Kingdom, the ICO expects gen AI developers to have methods in place to facilitate and respond to

[58] See ICO (2024b).

[59] Another right is data portability, though this is not covered in this paper.

[60] See GPA (2025b).

[61] See ICO (2024c).

[62] Gen AI developers may process personal data provided by clients, such as customer data supplied by a bank to fine-tune a model for financial services. In this case, the bank would be responsible for providing information to the individuals (ICO (2024c)).

[63] According to GPA (2023), developers, providers and deployers of gen AI systems must ensure individuals are informed about the collection and use of their personal data. According to ICO (2023a), those relying on exceptions must still safeguard individuals' rights by publicly providing privacy information and offering mechanisms to exercise these rights.

these requests, regardless of whether they relate to data used in training, fine-tuning or deployment (ICO (2024c)).

43. **The rights to rectification, erasure and objection are closely interconnected.** The right to rectification allows individuals to have inaccurate personal data corrected or completed, and organisations may need to share the corrected data with any third parties to whom they were disclosed. The right to erasure enables individuals to request the deletion of their personal data, such as when they withdraw consent, the data are no longer needed for their original purpose or they have been processed unlawfully.[64] Similarly, the right to object allows individuals to request the restriction or suppression of their personal data, potentially requiring organisations to erase the data unless they are needed for other legitimate purposes.

44. **However, these rights pose significant challenges in the context of AI, in particular with gen AI models**. AI models can sometimes reproduce portions of their training data – including personal data – verbatim, through a process known as memorisation, while offering no practical way to correct or erase such data.[65] This issue becomes even more complex when personal data are used to train LLMs, as it is often difficult to determine what the model has truly retained. In such cases, it is virtually impossible to exercise these rights effectively, as organisations such as financial institutions often lack access to the training data sets. Furthermore, it is frequently unclear what data have been used by model developers (ie often big tech companies) to train these models, adding another layer of difficulty.

45. **Rights related to automated decision-making protect individuals from being subjected to decisions made solely by automated processes.**[66] Data protection frameworks may establish the right for individuals not to be subject to fully automated decision-making and require organisations to ensure that individuals can request human intervention, receive meaningful information about the logic behind the decision-making process, obtain an explanation of the decision and challenge it. In 2025, the GPA highlighted the benefits of meaningful human oversight in automated decision-making and underscored the importance of enabling individuals to request a timely human review of automated decisions that may significantly affect their fundamental rights and freedoms.[67]

Fairness and transparency

46. **Fairness is a common principle in data protection regimes.** It requires organisations to process personal data in a fair manner, taking into account the potential impact of such processing and avoiding any unjustified negative effects or outcomes. This involves handling personal data in ways individuals would reasonably expect while preventing harm.[68] However, the fairness principle is often vaguely defined and open to interpretation, influenced by social, cultural and other factors.[69]

47. **In the context of AI, fairness centres on addressing biases and preventing unlawful discrimination.** In 2018, the International Conference of Data Protection and Privacy Commissioners, the

[64] This right may not apply if the processing is necessary for purposes such as scientific research, historical research or statistical analysis. See "Right to erasure" in ICO (2023a).

[65] See A Reisner, "The flaw that could ruin generative AI", *The Atlantic*, 11 January 2024. In this context, the ICO has sought feedback on methods to suppress or remove personal data from trained gen AI models (ICO (2024c)). Addressing these challenges, some scholars propose reinterpreting data subjects' rights for AI. For example, Mo (2025) suggests redefining the right to erasure to include "logical erasure", focusing on achieving the effect of erasure rather than complete physical deletion, especially for LLMs.

[66] Automated decision-making involves decisions made solely by machines, such as determining eligibility for a loan or insurance through algorithms. Profiling, which is often used in automated decision-making, involves analysing data from various sources to predict individual behaviour or traits based on patterns observed in others with similar characteristics. See ICO (2022).

[67] See GPA (2025c), which follows GPA (2023).

[68] See "Principle (a): Lawfulness, fairness and transparency" in ICO (2023b).

[69] See CIPL (2024a).

predecessor of the GPA, stated that AI models should uphold the fairness principle by meeting individuals' reasonable expectations and ensuring data are used in ways compatible with the original purpose of their collection. Building on this, in 2023, the GPA stressed that developers and deployers of gen AI systems must avoid creating or implementing systems that risk causing unfair, unethical or discriminatory outcomes. This was reinforced in 2025, when the GPA highlighted the importance of ensuring that both processing and outcomes are fair, emphasising that data sets must be accurate, complete, representative of the processing purpose and carefully assessed to prevent the inadvertent inclusion of unwanted bias.[70]

48. **Fairness in data collection and usage within gen AI is a fundamental principle emphasised by various jurisdictions.** China, for instance, highlights the importance of promoting fairness and justice in AI data development and deployment, as outlined in Ministry of Science and Technology of the People's Republic of China (2021). Moreover, for gen AI, Cyberspace Administration of China et al (2023) requires measures during training data selection as well as other processes to prevent discrimination based on factors such as ethnicity, belief, country, region, gender, age, occupation and health. Similarly, in Singapore, the Personal Data Protection Commission (PDPC) emphasised that AI algorithms and models embedded in decision-making systems should incorporate fairness at their core (PDPC (2018)).

49. **The principle of transparency requires organisations to explain how they handle personal data.** This involves providing easily understandable information. Data protection frameworks often outline the specific details that must be disclosed, such as the types of data being processed, the purposes for processing and any use of automated decision-making.[71] In addition, individuals may need to be informed about their rights and how to exercise them.

50. **Transparency is a fundamental responsibility of both AI developers and deployers.**[72] According to the GPA, they are expected to implement adequate notice and transparency measures, including by providing clear, concise and easily accessible information about the collection and use of personal data. AI developers are also expected to inform organisations deploying these systems about potential data protection and privacy risks and explain how such risks have been addressed. Deployers, in turn, are responsible for disclosing how, when and why personal data are collected and used during training of gen AI systems.

51. **These expectations are mirrored at the national level.** For instance, in Singapore, organisations using any AI system need to be transparent and include relevant practices and safeguards in their written policies to ensure that they act fairly and in a way that a reasonable person would consider appropriate under the circumstances (PDPC (2024a)). In China, both developers and deployers of gen AI services must implement measures tailored to the characteristics of their services to enhance transparency as well as the accuracy and reliability of generated content.[73] In the United Kingdom, developers of gen AI systems are expected to assess their compliance with data protection principles, including whether the purpose for processing personal data has been explained to the individuals concerned.

52. **Fairness and transparency in gen AI present significant challenges, as advanced AI models are often difficult to understand.** The limited explainability of these models complicates efforts to ensure proper human oversight and provide clarity on how they arrive at specific outcomes, and detecting and addressing bias is equally challenging.[74] Furthermore, although higher-risk use cases call for greater transparency, developers may hesitate to disclose details about the specific sources and types of data used

[70] See GPA (2018, 2025b).

[71] In the EU, Articles 13 and 14 of the GDPR specify the types of information that need to be provided.

[72] See GPA (2023, 2025b).

[73] See Article 4(5) of Cyberspace Administration of China et al (2023).

[74] See Pérez-Cruz et al (2025). See also Article 10 of the EU AI Act, which aims to address these risks.

to train their models due to proprietary concerns, as such information forms part of their intellectual property and could expose their models to replication or misuse.[75]

Data quality

53. **Data quality refers to the degree to which data meet the standards necessary to serve their intended purpose effectively and reliably**. It encompasses key attributes such as accuracy and completeness, as well as consistency, timeliness and relevance. The effective management of data quality involves robust quality assurance practices. These practices centre on a structured approach that ensures data remain "fit for purpose" and support the data needs of various business needs.

54. **Data quality is a fundamental element of data protection frameworks, with the principles of accuracy and completeness playing a key role**. The accuracy principle in data protection aims to ensure that personal data are reasonably accurate, preventing the dissemination of false information and avoiding decisions based on incorrect data.[76] A related aspect is the completeness of data, which aims to ensure that personal data are sufficient and comprehensive for their intended purpose, as incomplete or missing data can lead to flawed decision-making, unfair treatment or inaccurate conclusions. While some jurisdictions explicitly require data completeness, others include it implicitly within the broader definition of accuracy.[77]

55. **Robust data quality expectations apply throughout the development and deployment of AI systems, as poor data quality can undermine output reliability.** According to the GPA, in order to avoid discriminatory or unlawful impacts, developers and deployers of AI models are responsible for ensuring data are accurate, reliable and representative. This responsibility is heightened in fully automated systems, where outputs can significantly affect individuals. To address these risks, the GPA expects AI developers to take reasonable steps to ensure accuracy throughout pre-training, training and fine-tuning processes.

56. **These expectations are reinforced by clarifications and measures taken at the national level.** In the United Kingdom, the ICO has stated that if inaccurate training data lead to inaccurate outputs that affect individuals, both the developer and the deployer are likely to be in breach of the accuracy principle.[78] In China, Ministry of Science and Technology of the People's Republic of China (2021) emphasises the importance of data quality throughout all phases of the research and development process, while the Cyberspace Administration of China et al (2023) requires providers of gen AI services to adopt effective measures to enhance the quality of training data, ensuring their authenticity, accuracy, objectivity and diversity during activities such as pre-training and optimisation training.[79] Finally, the EU

[75] One way to address these issues is (i) for gen AI developers to publish explanatory documents, such as model or system cards and technical reports, to enhance transparency and accountability (CIPL (2024a,b)); and (ii) for deployers to ensure that AI reasoning processes are sufficiently visible to enable effective oversight and remediation (Hsu (2025)).

[76] In the EU, under the accuracy principle, organisations are required to ensure that the personal data they process are "accurate and, where necessary, kept up to date", taking "every reasonable step […] to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay". The AI Act builds upon this principle by requiring high-risk AI systems to use high-quality and unbiased data to prevent discriminatory outcomes. Article 10 of the AI Act has data quality requirements for high-risk AI systems.

[77] For example, in China, "the quality of personal information shall be guaranteed to avoid adverse effects on personal rights and interests caused by inaccurate and incomplete personal information" (Article 8 of PIPL). In Singapore, an organisation must make a reasonable effort to ensure that personal data collected by or on behalf of an organisation are accurate and complete, if the personal data (a) are likely to be used by the organisation to make a decision that affects the individual to whom the personal data relate; or (b) are likely to be disclosed by the organisation to another organisation (Article 23 of the Personal Data Protection Act).

[78] The ICO has asked for feedback on how to assess, measure and document the relationship between inaccurate training data and inaccurate model outputs. See ICO (2024c).

[79] See Articles 7 and 8 of Cyberspace Administration of China et al (2023).

AI Act stipulates that training, validation and testing data sets shall be relevant, sufficiently representative and, to the best extent possible, free of errors and complete in view of the intended purpose and that the levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.[80]

57. **The concept of accuracy in data protection differs from statistical accuracy in AI systems.**[81] Data protection accuracy requires personal data to be correct and complete, whereas statistical accuracy measures how often an AI system correctly predicts outcomes against labelled test data.[82] Importantly, compliance with the accuracy principle does not necessitate 100% statistical accuracy, and the required degree of accuracy depends on the context.[83] Nevertheless, when using AI to make inferences about individuals, it is crucial to ensure that the system is statistically accurate for its intended purpose.

58. **In order to uphold the accuracy principle in data protection, it is essential to clarify the responsibilities of developers and deployers of gen AI systems.**[84] Developers are expected to understand the accuracy of their training data and assess how their accuracy affects outputs. They are also expected to ensure that the statistical accuracy of outputs aligns with the model's purpose and data protection requirements and communicate these findings transparently to deployers and end users. Deployers, in turn, are responsible for mitigating risks from inaccurate data or outputs and providing clear information on the application's statistical accuracy and intended use, monitoring its usage and refining safeguards as needed to protect individuals.[85]

59. **Developers and deployers have various tools and strategies at their disposal to uphold the accuracy principles.** These include curating training data to ensure they meet the requirements for accuracy for the intended purpose, excluding false or misleading information, and avoiding unsupported claims about system accuracy. Robust data governance practices, such as documenting the sources of training data sets, play a critical role in maintaining data quality. In addition, technical safeguards like input-output filters and query restrictions can help mitigate risks associated with inaccurate outputs.

Data security

60. **A key element of data protection frameworks is the security of the data held within ICT systems.** Data security involves safeguarding information from unauthorised access, corruption, theft, loss or alteration while supporting its availability. It relies on a range of measures to protect data from both internal and external threats throughout the life cycle.

Confidentiality, integrity and availability

61. **The principles of confidentiality, integrity and availability form the foundation of data security within data protection frameworks**. These principles are often referred to as the CIA triad. Confidentiality ensures that data is accessible only to authorised individuals or systems and prevents

80 See Articles 10(3) and 15(3) of the EU AI Ac.

81 See ICO (2024c).

82 For AI, there are performance measures beyond statistical accuracy, such as precision and recall.

83 Achieving 100% statistical accuracy in AI models is generally not desirable, as it often indicates overfitting, reducing the ability to generalise and perform effectively on unseen data. Furthermore, even with high-quality, representative training data, gen AI systems will produce inaccurate or false information, often referred to as "hallucinations". See GPA (2023).

84 See GPA (2023, 2025b) and ICO (2024c).

85 Additionally, both developers and deployers must address the issue of model drift, where a model's performance deteriorates over time due to changing data patterns. When this occurs, retraining the model becomes essential to maintain its accuracy and reliability.

unauthorised access, disclosure or exposure of sensitive information. Integrity ensures that data are not improperly changed or destroyed and guarantees that they are genuine and trustworthy. Availability ensures that information is accessible to authorised users in a timely and reliable manner.[86]

62. **To uphold the CIA triad, organisations are expected to implement robust security measures.** These measures should cover different aspects of data processing, including IT and cyber security, physical safeguards (eg access to premises) and organisational controls (eg implementing an information security policy), and be proportionate to the risks involved. For instance, the UK ICO expects organisations to establish processes to assess security risks, mitigate them and regularly monitor and test the effectiveness of their measures.[87]

63. **Effective security measures are particularly important in the context of AI.** The GPA expects developers and deployers of gen AI systems to implement effective security measures, especially when the system accesses external data sources. This includes integrating traditional cyber security controls with those tailored to gen AI vulnerabilities (eg indirect prompt injection attacks), preventing model inversion attacks that could extract personal data from training data sets and ensuring that safeguards are in place to foster compliance with data protection obligations. Organisations are also expected to assess and mitigate risks of misuse of AI systems, such as the creation of deepfakes or generation of phishing content.[88]

Data breach notification

64. **Data breaches can have severe consequences, causing harm, losses and a decline in consumer trust in organisations.** Under Article 4(12) of the EU GDPR, a personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data". These breaches can target a wide range of information and take various forms (eg cyber attacks, insider threats or accidental data exposure).[89] For example, in Singapore, unauthorised access is one of the most common types of data breach, often due to weak passwords, while vulnerabilities in software development and system configurations (ie coding issues) have also been identified as a significant cause of several incidents in recent years.[90]

65. **Personal data breaches must typically be reported to the relevant data protection authority and, in certain cases, to the individuals affected**. In China, organisations must notify the relevant authorities responsible for personal information protection and the individuals concerned in the event of a data breach. However, if effective measures are implemented to prevent harm caused by the breach, organisations may not be obligated to notify individuals (Article 57 of the Personal Information Protection Law (PIPL)). In Singapore, organisations must assess whether notification of a data breach is required. If a breach is likely to cause significant harm to individuals or is of significant scale, they are required to notify the PDPC and affected individuals as soon as practicable.[91]

66. **Effectively managing data breaches is critical, and data protection authorities play a key role in providing guidance and support to affected organisations**. Data protection authorities often publish guidelines on managing and notifying data breaches.[92] They have also established procedures for

[86] See NIST (2020).

[87] See ICO (2023d).

[88] See GPA (2023).

[89] See EC-Council University, "Understanding data breaches: what you need to know", 7 November 2023.

[90] See PDPC (2024b).

[91] Notification is mandatory when prescribed personal data, such as non-public financial information (eg creditworthiness, outstanding debt, assets or payments), that are deemed to result in significant harm are disclosed. See PDPC (2022).

[92] In the EU, *Guidelines 01/2021 on examples regarding personal data breach notification* and (2023); in the United Kingdom, the ICO guide on personal data breaches; in Singapore, PDPC (2021).

reporting, along with online forms to facilitate breach notifications.[93] Additionally, organisations may be encouraged to develop a data breach management plan to respond to breaches more effectively. For example, Singapore's PDPC published a guide to help organisations identify, prepare for and manage data breaches (PDPC (2021)). In the EU, organisations must also maintain a register of data breaches, documenting details such as the nature of the breach, its impact and the remedial actions taken.[94]

Data governance

67. **Data governance is the foundation for managing data effectively and in compliance with data protection principles.** It provides an overarching framework that defines the roles, responsibilities, processes and policies required to manage data effectively while ensuring compliance with regulatory requirements. Data governance supports foundational data protection principles such as data security, privacy and quality by creating a unified framework for managing data, including by defining rules, decision rights and accountability structures to guide the collection, use and overall handling of data.[95]

68. **Accountability is a fundamental principle under data protection frameworks.** The GPA defines accountability as the "compliance and demonstration of compliance with personal data protection and privacy regulations, in particular through the adoption and implementation of appropriate, practicable, systematic and effective measures", requiring organisations to take responsibility for how they handle personal data and ensure compliance with data protection regulations, in particular through the adoption and implementation of suitable measures.[96] These include, for example, establishing governance structures, developing management policies and good practices for handling personal data, implementing organisational processes to operationalise them and using monitoring mechanisms and controls to ensure that policies and processes are effectively implemented.[97]

69. **Practical measures to demonstrate accountability include assigning responsibility, conducting risk assessments and promoting transparency**. Organisations may designate a Data Protection Officer (DPO) to oversee compliance with data protection requirements. They may also conduct risk assessments, such as the data protection impact assessment required under the EU GDPR, to identify and mitigate risks to individuals' personal data, in particular in high-risk processing activities.[98]

70. **The principle of accountability applies to both developers and deployers of AI systems.** According to GPA (2020), organisations are expected to embed data protection in AI systems by design and by default and implement a broad range of accountability measures to ensure compliance. For gen AI, this includes providing technical documentation throughout the AI system's life cycle, detailing model functionality, training data, and potential data protection and privacy impacts before deployment. Additionally, organisations should facilitate external audits to independently evaluate model functionality, test outputs for inaccuracies and biases, and recommend measures to mitigate potential risks effectively.[99]

71. **The principle of accountability goes beyond organisational measures to encompass meaningful human oversight of AI systems.** The GPA underscores the importance of human oversight as a vital tool for ensuring compliance with data protection principles, mitigating risks and building trust in AI systems, especially in decision-making processes that could have a significant impact on individuals'

93 For the EU, see EDPB, *How to notify a data breach to your DPA?*

94 See EDPB (2023).

95 See eg J Holdsworth and M Kosinski, "What is data governance?", *IBM Think*.

96 See GPA (2020).

97 See PDPC, *Accountability within an organisation*.

98 See Article 35 of the GDPR.

99 See GPA (2023).

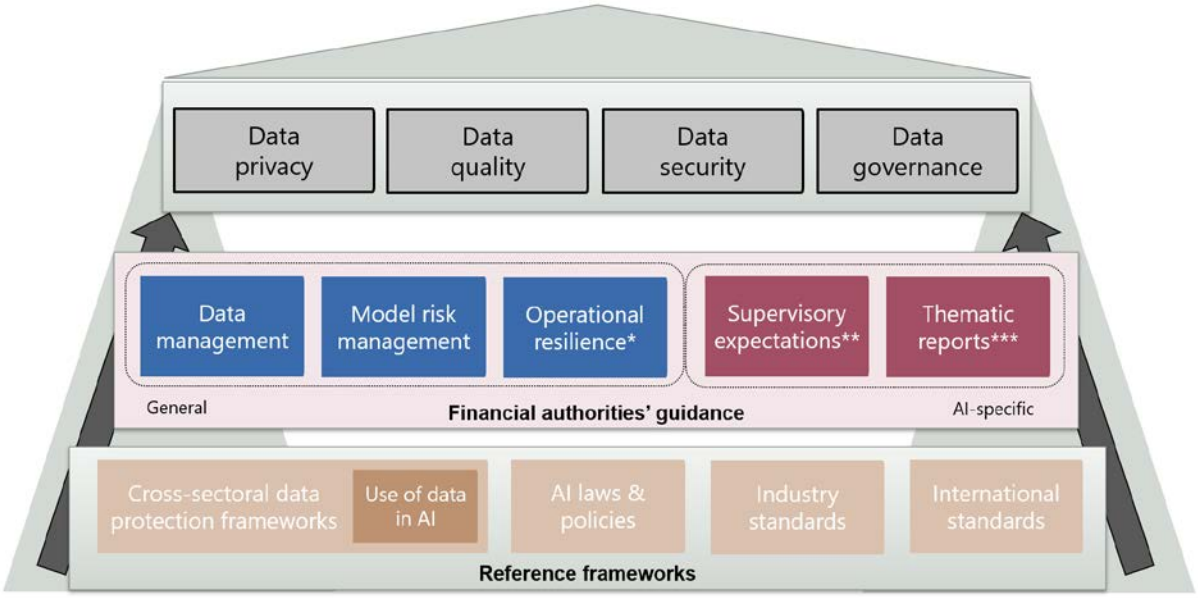
rights and freedoms. Effective human oversight requires not only monitoring AI decisions but also ensuring that overseers have the necessary expertise, resources and independence to evaluate decisions and intervene when needed. While organisations rely on overseers to diligently assess and monitor AI-driven decisions, ultimate accountability for decisions made by AI systems rests with the organisation (GPA (2025c)).

Section 4 – Financial sector-specific guidance on the use of data in AI systems

72. **Financial authorities have taken steps to address risks associated with data use in AI.** As discussed in previous sections, shortcomings in data usage throughout the AI life cycle can exacerbate prudential concerns by introducing deficiencies in MRM and increasing cyber security exposure. They can also give rise to consumer protection risks if AI training data are inaccurate, incomplete or biased, and increase financial stability vulnerabilities in case of excessive reliance on a limited number of third-party AI service providers.

73. **To address these risks, financial authorities' policy approach combines microprudential and consumer protection objectives with financial stability considerations.** This approach often leverages established regulatory and supervisory guidance for general data management, MRM and operational resilience, including cyber security, outsourcing and third-party risk management. Authorities also frequently employ non-prescriptive supervisory guidance, thematic reviews and information papers to highlight emerging good practices for managing data in AI. Their approach is underpinned by a range of frameworks and standards, such as data protection frameworks, cross-sectoral guidance, AI-specific legislation and policies, industry standards and international standards (Graph 4).

Financial authorities' policy approach to AI data — Graph 4



* Including cyber security, third-party risk management and outsourcing frameworks. ** At this stage, supervisory guidance is commonly non-prescriptive. *** Also includes informative reports.

Source: Authors' conceptualisation.

Reference frameworks for financial authorities

74. **Cross-sectoral data protection frameworks, including guidance on the use of data in AI, serve as the foundation for financial institutions' management and safeguarding of data**. As outlined in Section 3, financial institutions must adhere to their respective domestic data protection frameworks regardless of whether the data are used for AI applications or other purposes. To support this, various data protection authorities have issued guidance on the use of data in AI, which financial authorities expect supervised institutions to incorporate into their practices. Recognising the cross-cutting nature of AI data management, financial and data protection authorities have begun collaborating to align perspectives and foster consistent regulatory approaches. For example, the United Kingdom's Digital Regulation Cooperation Forum (DRCF) brings together four regulators, including the ICO and the Financial Conduct Authority (FCA), to ensure greater cooperation on online regulatory matters.

75. **Cross-sectoral AI legislation and policies are another cornerstone.** Several jurisdictions have begun designing and implementing AI legislation. China has adopted multiple rules and guidelines governing the use of AI.[100] Similarly, the EU introduced its landmark AI Act, which seeks to ensure that AI systems are safe, trustworthy and aligned with fundamental rights and values. Singapore and the United States have opted not to enact AI-specific laws.[101] Instead, they have developed voluntary governance frameworks that organisations can choose to adopt. The United Kingdom published an AI Opportunities Action Plan[102] but is yet to establish a statutory framework for AI governance.[103] These cross-sectoral developments form the basis for financial institutions' use of AI and guide financial authorities' approaches.

76. **Several industry standards have also emerged to support financial institutions in operationalising sound data practices for AI systems**. In the United States, the National Institute of Standards and Technology (NIST) published the Artificial Intelligence Risk Management Framework, a voluntary, non-sector-specific framework designed to help institutions incorporate trustworthiness into AI design and deployment.[104] NIST later introduced the Generative AI Profile, which identifies risks specific to gen AI and suggests actions to address them.[105] In Europe, the European Telecommunications Standard Institute (ETSI) issued a standard on baseline cyber security requirements for AI models and systems, while the European Commission (EC) requested that the European Committee for Standardization and European Committee for Electrotechnical Standardization develop standards on several aspects covered under the EU AI Act.[106] In Singapore, the Monetary Authority of Singapore (MAS) co-developed the Fairness, Ethics, Accountability and Transparency (FEAT) Principles with the financial industry to promote the responsible use of AI and data analytics.[107] To aid implementation, the MAS launched the Veritas Initiative, which has since released methodologies, a technical toolkit and case studies to guide the assessment of fairness and

100 The Algorithm Recommendation Management Provisions, the Deep Synthesis Management Provisions and Cyberspace Administration of China et al (2023), which collectively aim to regulate the development and use of AI technologies.

101 In the United States, while there is no federal bill to regulate AI, several laws have been passed at the state level. For example, the Colorado AI Act requires a developer of a high-risk AI system to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination in the high-risk system.

102 See UK Government (2025).

103 The Artificial Intelligence (Regulation) Bill, originally tabled in the House of Lords during the 2023–24 parliamentary session, aimed to introduce AI-specific legislation. Although it did not progress into law before Parliament's dissolution ahead of the general election, the bill was reintroduced on 4 March 2025 and is currently under review in the House of Lords.

104 The characteristics of trustworthy AI systems highlighted in the framework include valid and reliable, safe, secure and resilient, accountable and transparent, interpretable, privacy-enhanced and fair with harmful bias managed. See NIST (2023).

105 Among the risks identified, two directly relate to the use of data in gen AI systems: harmful bias from non-representative training data and data leakage through unintended disclosure. See NIST (2024).

106 Expected to be delivered by end-2027. See ETSI (2025) and EC (2025b).

107 See MAS (2018).

data governance in AI models. In addition, the MindForge Consortium released *AI risk management: executive handbook* to provide considerations and implementation practices for governing AI.[108] This will be followed by a detailed operationalisation handbook with implementation examples from the industry.

77. **In the financial sector, international standards guide the sound use of data in AI models.** For instance, the BCBS 239 Principles are a key reference point for banking supervisors regarding data management and governance. These principles have been implemented for global and domestic systemically important banks by several authorities worldwide (Box 3).[109] For the insurance sector, the International Association of Insurance Supervisors (IAIS) *Application Paper on the supervision of artificial intelligence* provides guidance on sound practices for the use of AI systems in insurance, including on data management in the context of fairness and the use of third-party AI systems and data.

Box 3

Status of the implementation of BCBS 239 Principles

Following the Great Financial Crisis, the BCBS published BCBS 239, *Principles for effective risk data aggregation and risk reporting*, in January 2013. BCBS 239 outlines 14 principles covering governance and infrastructure, risk data aggregation capabilities, risk reporting practices and supervisory review.

The principles were expected to be fully implemented by global systemically important banks (G-SIBs) by early 2016. National supervisors were encouraged to apply the principles to domestic systemically important banks (D-SIBs), and in several jurisdictions authorities decided to extend their scope to other banks as well.①

Since the publication of BCBS 239, the BCBS has been monitoring banks' adoption of the principles and published seven progress reports. The most recent progress report (2023) shows uneven implementation, calling for additional work at all banks to attain and/or sustain full compliance.② It noted that progress in implementation has been slower than anticipated, primarily due to persistent challenges such as fragmented IT landscapes, legacy systems and reliance on manual processes that are not fit for purpose. Other challenges include (i) incomplete data provenance/lineage and lack of a common taxonomy, which further complicates banks' ability to harmonise systems and detect data defects; (ii) lack of awareness and attention to data issues by boards and senior management, and therefore inadequate budget, resources and accountability for risk data aggregation and reporting initiatives; and (iii) lack of quality data, creating limitations for banks in implementing digitalisation projects.

At the national level, supervisory authorities have emphasised the importance of full compliance with BCBS 239. For example, in Singapore, D-SIBs – consisting of three local banks and four foreign banks – are required to comply with these principles.③ In Europe, the European Central Bank (ECB) has repeatedly highlighted the slow progress and has committed to intensifying its efforts to ensure that supervised institutions meet supervisory expectations.④ In 2024, the ECB published a guide outlining supervisory expectations to help institutions enhance their risk data aggregation and reporting capabilities.⑤ Additionally, the ECB's Supervisory Board approved a system-wide strategy to monitor banks' compliance with supervisory expectations and follow up on remediation efforts across all supervised institutions.⑥

A BCBS newsletter published in early 2026 highlighted that BCBS 239 has become a foundational framework for data and risk management practices in the banking sector. Both supervisors and industry participants view alignment with the principles as an ongoing process that requires continuous reassessment and effort due to the complexities of implementation and the ever-evolving nature of operational and business transformations. The newsletter also noted that emerging technologies, such as AI and automation, hold significant promise for enhancing risk data aggregation capabilities. However, it cautioned that the effectiveness of AI-driven outputs relies heavily on high-quality data, making robust data management increasingly critical for successful implementation.⑦

① For example, in Singapore, D-SIBs are required to comply with BCBS 239. See MAS (2024a). ② While the majority of the 31 assessed G-SIBs achieved "largely compliant" or "fully compliant" ratings across principles, only two banks were "fully compliant" with all the principles.

[108] Project MindForge examines the risks and opportunities of gen AI technology for financial services. See MAS (2025b).

[109] The BCBS's 2020 implementation progress report noted that many banks have extended the scope of these principles beyond risk data, applying them to other, if not all, data sets used by banks. See BCBS (2020).

Furthermore, no single principle has been fully implemented across all banks. See BCBS (2023). ③ See MAS (2024a). ④ In 2019, the ECB sent a letter to significant institutions urging substantial and timely improvements. ⑤ The guide states prerequisites for effective risk data aggregation and reporting capabilities, focusing on seven key areas including the responsibility of a bank's management body, key roles and responsibilities for data governance, implementation of a group-wide integrated data architecture and the effectiveness of data quality controls. See ECB (2024). ⑥ See ECB, *Supervisory priorities 2026–28*, January 2026. ⑦ See BCBS (2026).

Approaches adopted by financial authorities

78. **To address AI data-related risks, authorities largely rely on established regulatory and supervisory guidance related to general data management and MRM**. While in some jurisdictions this guidance is binding or prescriptive, most adopt a non-prescriptive and principles-based policy approach. This guidance is complemented by established regulatory and supervisory expectations on cyber and operational resilience, governance and consumer protection, as well as outsourcing and third-party risk management.

79. **Supervisory expectations on outsourcing and third-party risk management are particularly relevant for the use of data in AI models**. In line with well established supervisory practice, financial institutions are responsible for addressing risks from outsourcing,[110] including from outsourced AI solutions.[111] As gen AI models often use data provided by external parties, authorities expect financial institutions to implement robust third-party risk management and due diligence practices.[112] More specifically, financial institutions are expected to establish contractual safeguards and ensure transparency regarding data ownership, suitability, quality and bias controls. Furthermore, given the financial stability implications connected with the high degree of third-party AI data dependencies, the emerging frameworks for critical service providers can be particularly relevant.[113]

80. **Beyond established regulatory and supervisory guidance, authorities commonly rely on non-prescriptive policy approaches, reflecting an evolving framework that prioritises flexibility over rigid requirements**. Authorities commonly use non-prescriptive supervisory guidance and reports, such as thematic reviews and information papers, to outline emerging good practices on the use of data in AI. These publications cover data in areas like MRM, data governance and management, operational resilience (including outsourcing and third-party oversight) and AI.[114] They support sound practices and guide supervisory expectations, enabling adaptation to a rapidly changing environment. Table 1 gives an overview of guidelines issued by various jurisdictions.

81. **While specific supervisory expectations for the use of data in AI are not yet fully consistent, early signs of convergence are emerging in key areas such as data privacy, quality, security and governance**. Financial authorities continue to adopt varied approaches.[115] However, existing guidance

[110] For example, FRB et al (2023) stresses that outsourcing does not reduce a bank's responsibility for safe and sound operations or compliance with applicable regulations.

[111] See BCBS (2025).

[112] In China, for example, Article 26 of NFRA (2024) requires banking and insurance institutions to establish an approval and governance framework for external data sourcing, incorporating it into their outsourcing risk management framework. Key requirements include verifying the authenticity and legality of data sources as well as evaluating the security safeguards and data risk profiles of providers.

[113] For instance, in the EU, under the Digital Operational Resilience Act (DORA) regime, 19 entities, including Amazon, Google and Microsoft, have been designated as critical ICT third-party providers.

[114] For example, in Singapore, the MAS has published expectations and good practices on data governance, data management and AI MRM, drawing insights from thematic reviews of financial institutions. In , the MAS states that the good practices highlighted in MAS (2024a) would also apply to data used for AI.

[115] See Lin (2026) for a discussion on the approach taken in China.

collectively reveals a growing alignment on these critical areas, which are increasingly recognised as essential pillars for the safe and effective use of data in AI systems within financial services.

Guidelines issued by financial authorities Table 1

	China[2]	EU	Singapore	UK	US
Data governance and management	✓	✓	✓		
General MRM		✓		✓	✓[1]
AI MRM	✓		✓		
AI guidelines	✓		✓		

[1] FRB-OCC (2011) is the foundational document for MRM in the United States, and the Federal Deposit Insurance Corporation (FDIC) adopted the guidance in 2017. The OCC adopted its own MRM handbook to assist and educate examiners in their examination and supervision of banks. See OCC (2021). [2] In December 2025, the National Financial Regulatory Administration (NFRA) introduced a plan to promote high-quality development of digital finance in the banking and insurance sectors. Key provisions include accelerating the growth of "AI + finance", improving the safe application of AI technologies, managing risks associated with algorithmic models and enhancing data security protection. See NFRA (2025).

Source: FSI staff.

Data privacy

82. **Financial authorities stress the critical importance of supervised institutions adhering to data protection frameworks**. For example, in Germany, the Federal Financial Supervisory Authority (BaFin) highlights that, when using personal data in AI systems, financial institutions must comply with data protection requirements.[116] Similarly, the European Banking Authority (EBA) and European Insurance and Occupational Pensions Authority (EIOPA) emphasise the necessity of meeting all data governance obligations outlined in the GDPR.[117] To support these efforts, financial authorities may collaborate with data protection authorities, as in the MAS and PDPC's joint development of the FEAT Principles.[118]

83. **Authorities often emphasise the principles of fairness, transparency and the rights of individuals in AI-related data processing**. Recognising the strong link between data privacy and consumer protection, financial institutions are expected to ensure fair treatment of clients and transparency in AI-driven decisions and provide accessible channels for customers to seek explanations or challenge outcomes influenced by AI models. In addition, authorities expect financial institutions to carefully consider the data used in AI decisions and ensure transparency with clients. This includes being open about the use of AI and whether human review was involved and providing clarity on what data informed the decision and how they shaped the outcome. For example:

- **China.** The National Financial Regulatory Administration (NFRA) requires banks and insurers to implement effective measures to protect the legitimate rights and interests of financial consumers, highlighting that the use of personal information for automated decision-making should ensure transparency, fairness and impartial outcomes.[119]
- **Europe.** Luxembourg's Commission de Surveillance du Secteur Financier (CSSF) advises financial institutions to conduct a data protection impact analysis for AI/ML projects and ensure that users are adequately informed about data processing activities. Furthermore, if decisions are made

[116] See BaFin (2021).

[117] See EBA (2020) and EIOPA (2021).

[118] See MAS (2018).

[119] See NFRA (2024).

through AI/ML models, institutions must provide valid explanations of how these decisions were reached and ensure that individuals can rectify or erase incorrect personal data.[120]

- **Singapore.** For regulated activities with significant impact on customer outcomes, the MAS advises financial institutions to carefully assess the features of data used as inputs, justify their use, enable users to identify key drivers of AI outputs and inform customers about the use of AI-driven decisions, their consequences and available channels for redress.[121]
- **United States.** US regulators stress the importance of transparency and fairness in AI-driven lending decisions. For instance, depending on the types and objectives of banks' models, the OCC requires institutions to document model choices with supporting rationale, including key assumptions, data inputs and data exclusions, as well as to include standards to help ensure models do not cause or promote discrimination.[122] Relatedly, the Consumer Financial Protection Bureau (CFPB) mandates that creditors relying on complex or AI-based algorithms disclose the specific reasons for adverse credit decisions, including the data used by the model.[123]

84. **Authorities expect financial institutions to regularly review and validate data sets to avoid unintended bias or unfair outcomes**. Validation of AI data and models refers to the process of verifying that the data used to train, test and operate an AI model are accurate, representative and free of bias, and that the model's behaviour does not lead to discriminatory or unfair outcomes for particular groups. In Singapore, the MAS's FEAT Principles highlight the importance of reviewing and validating AI data and models for accuracy and relevance, with an emphasis on minimising unintentional bias.[124] Similarly, the EBA recommends implementing controls during data preparation and feature engineering phases to detect and prevent bias,[125] as well as applying statistical techniques to ensure equal representation across target population groups.[126]

Data quality

85. **Authorities consistently consider sound data quality to be fundamental to the safe and effective use of AI in finance.** The reliability of advanced AI models heavily depends on the scope and quality of their training data sets. Incomplete, inaccurate or unrepresentative data can erode model robustness, entrench algorithmic bias and undermine strategic decision-making by boards and senior management. In the context of finance, the use of historically limited data sets in some regions has resulted in inaccurate credit self-assessments and contributed to elevated credit risk.

86. **To address data quality risks, authorities emphasise the need for financial institutions to build on existing MRM frameworks.** For example:

- **The MAS guidelines on AI risk management highlight the importance of sound data management controls, including on data quality**. Institutions are expected to assess the adequacy of the quality of data used in an AI use case, system or model, including data relevance,

120 See CSSF (2018).

121 The MAS published a consultation paper to introduce guidelines on AI risk management with the aim of establishing a set of expectations that are generally applicable across the financial sector. See MAS (2025a).

122 See OCC (2021).

123 See CFPB (2023).

124 See Principle 3 of MAS (2018): "Data and models used for AIDA-driven decisions are regularly reviewed and validated for accuracy and relevance, and to minimise unintentional bias". On fairness, the principles highlight that unless justified, individuals or groups of individuals should not be systematically disadvantaged through AI-driven decisions.

125 Feature engineering is the process of transforming raw input data into meaningful features that best represent the underlying problem for prediction.

126 See EBA (2020).

accuracy, completeness and recency, as well as carry out regular monitoring of data quality and checks for anomalies, drifts and potential bias.[127]

- **The Prudential Regulation Authority's (PRA) MRM highlights that the added complexity and uncertainty of interconnected and alternative data should be reflected in the model's classification.** This ensures that models are subjected to appropriate levels of validation and scrutiny.[128]
- **The ECB guide to internal models clarifies that financial institutions are expected to establish and implement an effective data quality management framework as part of their internal models for credit risk measurement.** This should include (i) sound governance principles that clearly define roles and responsibilities for managing data quality; (ii) comprehensive data quality standards addressing all relevant data quality dimensions (ie completeness, accuracy, consistency, timeliness, uniqueness, validity, availability, traceability); (iii) controls and metrics to assess compliance with data quality standards; and (iv) procedures for the continuous assessment and enhancement of data quality.[129]

87. **Authorities expect financial institutions to have a thorough understanding of the quality of their data sources.** This is partly because authorities often associate data quality with fairness, as unrepresentative or biased data sets are a significant cause of discriminatory or unequal outcomes in AI models. In addition, regulators highlight the importance of sound data management practices to maintain and enhance data quality.

- **In the United States, the inter-agency MRM guidance discusses the critical importance of data and the importance of developers demonstrating the suitability of data used in models.** It also discusses the importance of evaluating the relevance of data sources, including when using external data, as well as accuracy and quality assessments performed during model development and validation.[130]
- **In Europe, EIOPA advises institutions to select suitable data sources, perform data exploration analysis to understand the characteristics of the data, address data quality issues through cleaning and document significant changes to data to ensure traceability.** It also highlights the importance of evaluating AI outcomes from a data quality perspective in order to reduce potential biases in trained models.[131] Similarly, the EBA expects issues of data quality to be taken into account throughout the big data and advanced analytics life cycle in order to gain trust in the data processed, and warns that quality of input data is one of the key challenges in the increasing adoption of gen AI in the EU banking and payments sectors.[132]
- **The United Kingdom's AI Public-Private Forum, launched in 2020 by the BoE and FCA, highlights the difficulties of adapting existing data quality frameworks to the complexity and scale of AI applications.** It also underscores the need for financial institutions to be aware of the challenges associated with using alternative or synthetic data, including potential biases or errors. To address these challenges, the Forum advises firms to create internal standards and systems, such as data lineage templates, to provide a clear history of where and how data were produced and how they move through an organisation.

127 See MAS (2025a).

128 See BoE-PRA (2023).

129 See ECB (2025).

130 See FRB-OCC (2011) and FDIC (2017).

131 See EIOPA (2021).

132 See EBA (2020, 2025).

Data security

88. **Most authorities address AI-related data security risk through existing cross-sectoral and financial risk frameworks.** As discussed in Section 2, AI systems trained on large data sets and often dependent on external providers are exposed to risks such as data poisoning, model manipulation and prompt injection. At the same time, gen AI tools can be misused for malicious purposes, amplifying the scale and sophistication of cyber attacks, scams and misinformation campaigns. To address these risks, authorities rely on a combination of data protection guidance; model and data management requirements; and specific guidance on IT systems, cyber and operational resilience, and third-party risk management.

89. **Policy expectations emphasise prevention, detection and response to data-related incidents.** Financial institutions are expected to establish comprehensive data loss prevention measures, report significant data incidents to authorities and maintain business continuity plans to manage disruptions that could materially affect their operations or customer services. For example, the EBA urges management bodies to establish strategies and procedures to monitor, detect and respond to security incidents involving big data and advanced analytics systems, their data sources and third-party technology providers.[133] In the United States, the *Interagency guidelines establishing information security standards* mandate that institutions maintain incident response programmes to notify affected customers and regulators "as soon as possible" following data breaches.[134] The New York State Department of Financial Services (NYDFS) requires financial institutions to notify the regulator within 72 hours of a data breach.[135]

90. **Several authorities have begun to prioritise their policy response to cyber threats arising from the misuse of gen AI.** Focus areas for authorities include deepfakes, AI-generated phishing, malware creation, data poisoning[136] and unauthorised information disclosure or data leakages. The MAS published an information paper, *Cyber risks associated with generative artificial intelligence*, outlining practical mitigation measures for financial institutions, including raising employee awareness, conducting simulation exercises and strengthening gen AI usage policies.[137] In particular, the MAS recommends that institutions desensitise data inputs before using public gen AI tools, prohibit confidential information in prompts and adopt gen AI-specific data loss prevention controls and firewalls to detect attempts to extract or exploit data. Due to the ongoing dynamic evolution of these threats, policy expectations highlight the need for continuous adaptation of cyber security frameworks to evolving AI technologies.

91. **Authorities generally expect institutions to implement robust data security governance across the data life cycle, with particular emphasis on access controls and data classification**. EIOPA recommends that data used in AI models be processed and stored securely, while the People's Bank of China (PBC) stipulates security control measures for personal financial information and important data throughout all stages of their life cycle to ensure integrity and authenticity. Additionally, authorities increasingly expect institutions to classify and manage data according to their criticality and sensitivity. In China, both the PBC and the NFRA require institutions to establish and improve systems and operating procedures for the classification and grading of business data. Similarly, the MAS highlights data classification as a key area in data management controls, noting that institutions should implement classification processes to guide appropriate use of data in an AI system, taking into account the criticality and sensitivity of the data used (MAS (2025a)).

133 See EBA (2020).

134 See FRB (2013).

135 See NYDFS (2023).

136 For example, EBA (2020) states that, in poisoning attacks, attackers deliberately influence the training data to manipulate the results of a predictive model. It emphasises the need to maintain a technical watch and to be regularly updated about progress on security attacks and related defence techniques.

137 This paper aims to raise financial institutions' awareness by providing an overview of key cyber and technology threats arising from gen AI, the associated risk implications and some of the mitigation measures to address the risks. See MAS (2024b).

Data governance

92. **Authorities emphasise that sound data governance is essential to ensure accountability and effective oversight of AI data use.** Effective governance ensures that AI data practices align with institutional objectives, regulatory expectations and ethical standards. Therefore, authorities expect financial institutions to implement governance arrangements under data protection frameworks, MRM frameworks and, where applicable, international principles such as BCBS 239. These data governance arrangements encompass the organisational structures, policies, roles and accountability mechanisms that guide how data are collected, processed, stored and used throughout the AI life cycle.[138]

93. **A well defined organisational structure supports sound implementation of AI data management frameworks.** Authorities view it as a key component of an AI data governance framework to have an organisational structure that ensures clearly delineated responsibilities for AI data management across all levels of a financial institution. This includes assigning accountable roles for data ownership, data stewardship and model development. It also provides clarity in terms of escalation and reporting lines to senior management. In the United States, FRB-OCC (2011) proposes a conceptual division of roles in MRM, assigning model owners responsibility for development, implementation and validation; control groups oversight of risk measurement, monitoring and validation; and internal audit independent evaluation of the overall framework's effectiveness and compliance.[139]

94. **Boards and senior management bear ultimate responsibility for AI data governance.** In China, the NFRA underscores that a banking institution's board of directors takes ultimate responsibility for data governance.[140] In the United States and the United Kingdom, while the board retains ultimate responsibility for governance, it generally delegates to senior management the responsibility for executing and maintaining an effective MRM framework.[141] Regular reporting to the board is expected to ensure appropriate challenge and oversight. The MAS's *Consultation paper on guidelines on artificial intelligence risk management* set the expectations for the board and senior management to play a critical role in establishing and overseeing robust frameworks, policies and procedures to support AI risk management across the financial institution, including in AI data management, by defining clear roles and responsibilities.[142]

95. **In line with the above considerations, emerging industry practices increasingly emphasise the need for a robust AI data governance framework.** The advent of gen AI has challenged existing practices created for governance and oversight of traditional AI, prompting financial institutions to reconsider the best governance strategy for their data.[143] Emerging data governance frameworks are built on clearly defined data-related roles and responsibilities across the AI life cycle.[144] Assurance mechanisms (eg regular audits, testing and exercises) help identify unintended outcomes, while continuous monitoring ensures adaptability to evolving technological and regulatory landscapes.[145] Together, these elements form the institutional foundation for responsible, resilient and trustworthy use of data in AI systems.

[138] Examples as stated in MAS (2025a) include creating cross-functional oversight forums; updating policies and controls; defining roles and responsibilities; developing guidelines for the fair, ethical, accountable and transparent use of AI across banks; and building AI capabilities to support both innovation and risk management.

[139] See FRB-OCC (2011).

[140] See NFRA (2018). The guidelines were issued in 2018 by the former CBIRC, the core predecessor of the NFRA.

[141] See OCC (2021) and BoE-PRA (2023).

[142] See MAS (2025a).

[143] See IIF (2024).

[144] See FS-ISAC (2025a,b).

[145] See CMORG AI Taskforce (2025).

Section 5 – Concluding remarks

96. **Data are fundamental to the success of AI.** While advances in computing power and technological infrastructure have attracted much attention, it is data that ultimately determine whether AI systems deliver reliable, safe and trustworthy outcomes. In this sense, the well known saying that "a model is only as good as its data" remains highly relevant. As AI systems become increasingly embedded in core financial institutions' activities, including deposit-taking, credit and insurance underwriting and payment services, robust data governance frameworks, strong safeguards for sensitive information and effective data quality management throughout the AI life cycle become essential not only for the reliability of AI applications but also for maintaining trust and confidence in the financial system.

97. **The use of AI has brought to the fore inherent tensions between technological capabilities and existing data protection requirements**. A key challenge lies in reconciling the data-intensive nature of AI systems with legal and ethical obligations that are grounded in societal values, including the protection of individuals' right to privacy. While this right is safeguarded by data protection requirements, their practical application to different stages of the AI life cycle remains a work in progress. Data protection authorities are working to provide guidance, but this guidance often lags behind the rapid pace of technological advances. Moreover, even with such guidance, data protection requirements can impose demands that current AI technology is not yet capable of fulfilling. For example, the right to erasure, which allows individuals to request the deletion of their personal data, may be very challenging to implement when personal data has been used to train LLMs.

98. **The rapid evolution of AI in the financial sector, coupled with the increasing use of diverse and complex data sets, further amplifies these tensions**. Financial institutions face significant hurdles, including balancing the efficiency gains associated with extensive data use against the constraints imposed by data protection requirements. Adding to this complexity, financial institutions typically rely on AI models developed by big tech providers, which limits their visibility into the data used to train these models. This reduced transparency can constrain their ability to fully implement robust risk mitigation strategies and to demonstrate compliance with applicable data protection requirements. While institutions can take proactive steps to improve their data handling practices, addressing data-related challenges in the use of AI is an ongoing and complex task that requires continuous effort.

99. **Against this backdrop, guidance from financial supervisors can support financial institutions in addressing AI data-related challenges more effectively**. This could involve supervisory action on two levels. First, at the level of reference frameworks, supervisors could provide additional clarification on how they apply to financial institutions. However, an important constraint is that supervisors often lack a direct mandate over data protection matters and therefore may not always have the authority to provide such guidance. Second, within their own regulatory and supervisory frameworks, supervisors could review and update existing guidance on areas such as data management, MRM and operational resilience. This process could help identify gaps and enable the development of more tailored supervisory expectations. Leveraging international standards such as BCBS 239 could further strengthen supervisory approaches to AI-related data risks.

100. **In developing more tailored guidance, supervisors could prioritise key aspects of the use of data in AI systems, including data governance, data quality, data security, third-party dependencies and data privacy**. The following areas could particularly benefit from clearer regulatory/supervisory expectations:

- First, supervisors could clarify their expectations regarding **data governance** frameworks for AI systems. This may include emphasising sound organisational structures, clear allocation of roles and responsibilities, strengthened accountability across the AI data life cycle and robust documentation practices. Supervisors may also encourage financial institutions to establish

governance mechanisms that ensure effective oversight by the board and senior management, supported by internal controls and independent reviews.

- Second, supervisors could provide further direction on **data quality** management in AI systems. This may involve expectations across key data quality dimensions such as accuracy, completeness, timeliness and representativeness, together with main controls or metrics to assess compliance. In this regard, supervisors could encourage financial institutions to implement strong data management processes, in particular with respect to how data are collected, processed and used, while promoting transparency regarding data limitations. Continuous improvement processes would also be important to ensure that data quality remains adequate over time.
- Third, **data security** considerations could receive additional supervisory attention in the context of AI. Given the scale and potential sensitivity of data sets used in AI systems, supervisors may wish to emphasise the importance of effective incident response plans, including policies and processes to monitor, detect and respond to data security incidents. These arrangements could incorporate data breach notification mechanisms to ensure timely action and minimise potential harm. More broadly, expectations could highlight the importance of integrating cyber security and data protection controls into AI development and deployment environments, as well as the need to adapt these controls continuously in response to evolving cyber threats, including those associated with the misuse of gen AI.
- Fourth, supervisors may consider strengthening expectations regarding **third-party dependencies** in AI data ecosystems. Financial institutions increasingly rely on external providers for data, model development and cloud infrastructure, which may limit their visibility into training data sets and processing practices. Supervisory guidance could therefore emphasise enhanced due diligence processes to thoroughly assess third-party providers. It could also highlight the need for contractual safeguards to ensure accountability, greater transparency in data lineage and ongoing monitoring of third parties involved in the AI supply chain.
- Finally, within the constraints of their mandates, supervisors may also wish to provide greater clarity regarding the application of **data privacy** principles in the AI context. As highlighted before, the large-scale use of personal data in AI systems can create tensions with existing data protection requirements, in particular as regards lawful basis, purpose limitation, data minimisation and individuals' rights. Supervisory guidance could help financial institutions better interpret these principles across different stages of the AI life cycle. Such efforts could also encourage the adoption of privacy-enhancing techniques and robust data protection impact assessments.

101. **In addition, authorities could provide further feedback or information to the industry to foster understanding of existing and emerging challenges.** This could involve conducting fact-finding exercises and publishing insights gained in supervisory work as thematic reviews. Such efforts could elaborate on the practicalities of using data in AI applications, supported by case studies that illustrate real-world examples. These publications could also highlight challenges encountered by financial institutions and offer best practices to address them.

102. **More broadly, a more comprehensive approach to AI-related data issues may warrant consideration over time.** Since data issues span multiple domains, they surface across various policy areas and documents issued by financial authorities. In addition, addressing AI-related challenges, in particular gen AI, is an evolving effort as the technology continues to advance. As a result, existing policy responses are often piecemeal, with guidance typically focusing on either MRM or general data management, neither of which is necessarily tailored to AI. Therefore, developing a more coherent policy framework for AI data in the financial sector, covering the main areas of tension between data protection requirements and AI technology, would be particularly helpful.

103. **Enhanced collaboration between financial authorities and data protection authorities is vital given the cross-cutting and rapidly evolving nature of AI data-related challenges**. More structured cooperation and coordination between these authorities can help align perspectives, reduce uncertainty for supervised institutions and promote greater consistency across regulatory and supervisory approaches. At the same time, regular engagement with industry participants and collaborative initiatives can help authorities remain informed about practical implementation challenges. At the international level, such cooperation can help mitigate the risk of fragmentation in AI and data frameworks, a concern that is especially salient for global financial institutions.

104. **Ultimately, the responsible and effective use of data in AI requires close cooperation between financial authorities and supervised institutions.** Financial institutions remain responsible for implementing robust data practices, while authorities play a key role in articulating expectations, identifying emerging risks and fostering consistent approaches across the financial system. Given the rapid pace of AI innovation, increasing reliance on third-party providers and the emergence of new data sources, both institutions and authorities will need to navigate a constantly shifting landscape. In this environment, ongoing dialogue and mutual understanding will be essential to ensure that AI adoption in financial services not only supports innovation, but also reinforces the trust, resilience and soundness of the financial system.

References

Aldasoro, I, L Gambacorta, A Korinek, V Shreeti and M Stein (2025): "Intelligent financial system: How AI is transforming finance", *Journal of Financial Stability,* vol 81, December.

Armantier, O, S Doerr, J Frost, A Fuster and K Shue (2024): "Nothing to hide? Gender and age differences in willingness to share data", *BIS Working Papers,* no 1187, May.

Bank of England (BoE) (2026): "Summary of AI roundtables – February 2026", February.

Bank of England and Financial Conduct Authority (BoE-FCA) (2022): *Artificial Intelligence Public-Private Forum, final report*, February.

——— (2024): *Artificial intelligence in UK financial services – 2024*, November.

Bank of England and Prudential Regulation Authority (BoE-PRA) (2023): "Model risk management principles for banks", *Supervisory Statement,* no SS1/23, May.

Barberà, I (2025): *AI privacy risks & mitigations – Large language models (LLMs)*, March.

Basel Committee on Banking Supervision (BCBS) (2020): *Progress in adopting the Principles for effective risk data aggregation and risk reporting*, April.

——— (2023): *Progress in adopting the Principles for effective risk data aggregation and risk reporting*, November.

——— (2025): *Principles for the sound management of third-party risk,* December.

——— (2026): "Implementation of the Principles for effective risk data aggregation and risk reporting (BCBS 239 Principles)", January.

Board of Governors of the Federal Reserve System (FRB) (2013): *Interagency guidelines establishing information security standards*, August.

Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration and Office of the Comptroller of the Currency (2019): *Interagency statement on the use of alternative data in credit underwriting*.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency (2023): *Interagency guidance on third-party relationships: risk management*, June.

Board of Governors of the Federal Reserve System and Office of the Comptroller of the Currency (FRB-OCC) (2011): *Supervisory guidance on model risk management*, April.

Centre for Information Policy Leadership (CIPL) (2020): *Artificial intelligence and data protection: How the GDPR regulates AI*, March.

——— (2024a): *Building accountable AI programs: mapping emerging best practices to the CIPL Accountability Framework*, February.

——— (2024b): *Applying data protection principles to generative AI: practical approaches for organizations and regulators*, December.

Commission de Surveillance du Secteur Financier (CSSF) (2018): *Artificial intelligence: opportunities, risks and recommendations for the financial sector*, December.

Consumer Financial Protection Bureau (CFPB) (2023): "Adverse action notifications requirements and the proper use of the CFPB's sample forms provided in Regulation B", *Consumer Financial Protection Circular*, no 2023-03, September.

——— (2024): "CFPB finalises personal financial data rights rule to boost competition, protect privacy, and give families more choice in financial services", October.

Crisanto, J, C Leuterio, J Prenio and J Yong (2024): "Regulating AI in the financial sector: recent developments and main challenges", *FSI Insights on policy implementation*, no 63, December.

Cross Market Operational Resilience Group (CMORG) AI Taskforce (2025): *AI baseline guidance review*, January.

Cyberspace Administration of China, National Development and Reform Commission, Ministry of Education, Ministry of Science and Technology, Ministry of Industry and Information Technology, Ministry of Public Security and State Administration of Radio and Television (2023): *Interim measures for the management of generative artificial intelligence services*, July.

European Banking Authority (EBA) (2020): *EBA report on big data and advanced analytics*, January.

——— (2024): *Risk assessment report of the European Banking Authority*, November.

——— (2025): "Rising application of AI in EU banking and payments sector", September.

European Central Bank (ECB) (2024): *Guide on effective risk data aggregation and risk reporting*, May.

——— (2025): *ECB guide to internal models*, July.

European Commission (EC) (2025a): *Generative AI outlook report – Exploring the intersection of technology, society and policy*, Publications Office of the European Union, June.

——— (2025b): *Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards high-risk AI-systems in support of Regulation (EU) 2024/1689 of the European Parliament and of the Council and repealing Implementing Decision C(2023)3215*, June.

——— (2025c) *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)*, November.

European Data Protection Board (EDPB) (2020): *Guidelines 4/2019 on Article 25: Data protection by design and by default*, October.

——— (2023): *Guidelines 9/2022 on personal data breach notification under GDPR*, March.

——— (2024a): *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, October.

——— (2024b): *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, December.

——— (2025): *Personal data breaches: what to do*, March.

European Insurance and Occupational Pensions Authority (EIOPA) (2021): *Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector*, June.

European Securities and Market Authority (ESMA), Institut Louis Bachelier and the Alan Turing Institute (2025): *Leveraging large language models in finance: pathways to responsible adoption*, May.

European Telecommunications Standard Institute (ETSI) (2025): *Securing Artificial Intelligence (SAI); baseline cyber security requirements for AI models and systems*, December.

European Union (EU) (2016): *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, April.

——— (2024): *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, June.

Federal Deposit Insurance Corporation (FDIC) (2017): *Model risk management: core analysis procedures*.

Federal Financial Supervisory Authority (BaFin) (2021): "Big data and artificial intelligence: Principles for the use of algorithms in decision-making processes", June.

Fedyk, A, A Kakhbod, P Li and U Malmendier (2024): "AI and perception biases in investments: an experimental study", April.

Financial Conduct Authority (FCA) (2025): *Generating and using synthetic data for models in financial services: governance considerations*, August.

Financial Services – Information Sharing and Analysis Center (FS-ISAC) (2025a): *More opportunity, less risk – 8 steps to manage financial services data with gen AI*, January.

——— (2025b): *Define the role, limit the risk – The roles and responsibilities of AI usage in financial services*, May.

Financial Stability Board (FSB) (2024): *The financial stability implications of artificial intelligence*, November.

G7 Data Protection and Privacy Authorities (G7 DPAs) (2024): *G7 DPAs' Action Plan*.

——— (2025): "2025 G7 Data Protection and Privacy Authorities roundtable statement", Office of the Privacy Commissioner of Canada, 19 June.

Global Privacy Assembly (GPA) (2018): *Declaration on ethics and data protection in artificial intelligence*, 40th International Conference of Data Protection and Privacy Commissioners, Brussels, 23 October.

——— (2020): *Adopted resolution on accountability in the development and use of artificial intelligence*, 42nd Closed Session of the Global Privacy Assembly, October.

——— (2023): *Resolution on generative artificial intelligence systems*, 45th Closed Session of the Global Privacy Assembly, October.

——— (2024): *Interim report on the work conducted by the AIWG members on generative AI systems*.

——— (2025a): *Working Group on Ethics and Data Protection in Artificial Intelligence*, July.

——— (2025b): *Resolution on the collection, use and disclosure of personal data to pre-train, train and fine-tune AI models*, 47th Closed Session of the Global Privacy Assembly, September.

——— (2025c): *Resolution on meaningful human oversight of decisions involving AI systems*, 47th Closed Session of the Global Privacy Assembly, September.

Haksar, V, Y Carrière-Swallow, A Giddings, E Islam, K Kao, E Kopp and G Quirós-Romero (2021): "Toward a global approach to data in the digital age", *IMF Staff Discussion Note*, no 2021/005, October.

Heikkilä, M (2026): "AI's 'memorisation' problem: the novels it can't forget", *Financial Times*, February.

Hicks, E (2025): "A revamped CFPB rulemaking on personal financial data rights", *DLA Piper Insights*, 29 August.

Hlophe, N and L Mabetha (2025): *Artificial intelligence in the South African financial sector*, Financial Sector Conduct Authority and South African Reserve Bank's Prudential Authority, November.

Hsu, M (2025): "AI actionability over interpretability", September.

Information Commissioner's Office (ICO) (2022): *Automated decision-making and profiling*, October.

——— (2023a): *A guide to individual rights*, May.

——— (2023b): "Legitimate interests", *A guide to lawful basis*, May.

——— (2023c): *A guide to the data protection principles*, May.

——— (2023d): *A guide to data security*, May.

——— (2024a): *Generative AI first call for evidence: the lawful basis for web scraping to train generative AI models*.

——— (2024b): *Generative AI second call for evidence: purpose limitation in the generative AI lifecycle*.

——— (2024c): *Generative AI third call for evidence: accuracy of training data and model outputs*.

——— (2024d): *Generative AI fourth call for evidence: engineering individual rights into generative AI models*.

Institute of International Finance (IIF) (2024): "AI, Data, and the Cloud: Connectivity, innovation and generating value in financial services", *IIF Staff Paper*, May.

Institute of International Finance and EY (IIF-EY)(2025): *IIF-EY annual survey report on AI use in financial services*, October.

International Association of Privacy Professionals (IAPP) (2025): "Data protection and privacy laws now in effect in 144 countries", 28 January.

International Regulatory Strategy Group (IRSG) (2026): *AI in financial services: emerging global norms*, January.

Jeng, L, J Frost, E Noble and C Brummer (2025): "Consumer financial data and non-horizontal mergers", *Fordham Journal of Corporate & Financial Law,* vol 30, no 2, November.

Lin, L (2026): "Artificial intelligence in China's banking sector: promises, perils, and regulation", *European Business Organisation Law Review*, February.

Liu, C (2025): "Artificial intelligence, big data, and financial risk management", *Financial Supervision Research*, no 5, September.

McKinsey & Company (2025): "How financial institutions can improve their governance of gen AI", 27 March.

Ministry of Science and Technology of the People's Republic of China (2021): "The New-Generation Artificial Intelligence Code of Ethics was released", 26 September.

Mittal, A (2025): "Poor data quality is stalling AI adoption", *Insurance Day*, 12 November.

Mo, Y (2025): "The right to erasure of personal information in large language models: challenges and responses", *Tsinghua China Law Review*, vol 17, no 1, January, pp 33–58.

Monetary Authority of Singapore (MAS) (2018): *Principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector*, November.

——— (2024a): "Data governance & management practices – observations and supervisory expectations from thematic inspections", *Information Paper*, May.

——— (2024b): "Cyber risks associated with generative artificial intelligence", *Information Paper*, July.

——— (2024c): "Artificial intelligence model risk management – observations from a thematic review", *Information Paper*, December.

——— (2025a): *Consultation paper on guidelines on artificial intelligence risk management*, November.

——— (2025b): *AI risk management: executive handbook*, November.

National Financial Regulatory Administration (NFRA) (2018): *Guidelines on data governance for banking financial institutions*, May.

——— (2024): *Measures for the management of data security of banking and insurance institutions*, December.

——— (2025): "The National Financial Regulatory Administration issued the 'Implementation Plan for High-Quality Development of Digital Finance in the Banking and Insurance Industry'", December.

National Institute of Standards and Technology (NIST) (2020): "Data integrity: detecting and responding to ransomware and other destructive events", *NIST Special Publication*, no 1800-26A, December.

——— (2023): *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, January.

——— (2024): *Artificial Intelligence Risk Management Framework: Generative artificial intelligence profile*, July.

New York State Department of Financial Services (NYDFS) (2023): *Cybersecurity requirements for financial services companies*, November.

Office of the Australian Information Commissioner (OAIC) (2025): *Joint statement on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI*, February.

Office of the Comptroller of the Currency (OCC) (2021): "Model risk management", *Comptroller's Handbook – Safety and Soundness*, August.

Organisation for Economic Co-operation and Development (OECD) (2019): "Recommendation of the Council on artificial intelligence", *OECD Legal Instruments,* no OECD/LEGAL/0449, May.

——— (2023): "Report on the implementation of the OECD Privacy Guidelines", *OECD Digital Economy Papers*, no 361, November.

——— (2024a): "GPAI and OECD unite to advance coordinated international efforts for trustworthy AI", *Statement*, July.

——— (2024b): "2024 GPAI New Delhi Declaration", July.

——— (2026): "Supervision of artificial intelligence in finance: challenges, policies and practices", *OECD Artificial Intelligence Papers*, no 54, January.

Patchipala, S (2023): "Data anonymization in AI and ML engineering: balancing privacy and model performance using Presidio", *IRE Journals,* vol 6, no 10, April.

Pérez-Cruz, F, J Prenio, F Restoy and J Yong (2025): "Managing explanations: how regulators can address AI explainability", *BIS Occasional Paper*, no 24, September.

Perlov, Y (2024): "AI data governance spotlights privacy and quality", *Dataversity*, 25 November.

Personal Data Protection Commission (PDPC) (2018): *Discussion paper on artificial intelligence (AI) and personal data – fostering responsible development and adoption of AI*, June.

——— (2021): *Guide on managing and notifying data breaches under the Personal Data Protection Act*, March.

——— (2022): *Advisory guidelines on key concepts in the Personal Data Protection Act*, May.

——— (2024a): *Advisory guidelines on use of personal data in AI recommendation and decision systems*, March.

——— (2024b): *Guide to data protection practices for ICT systems*, December.

Posnett, K (2025): "The new markets for AI data", *Financial Times*, May.

Reuel, A (2025): "Chapter 3: Responsible AI", *Artificial Intelligence Index Report 2025*, April.

Rupp, V and M von Grafenstein (2024): "Clarifying 'personal data' and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection", *Computer Law & Security Review*, vol 52, April.

Shumailov, I, Z Shumaylov, Y Zhao, N Papernot, R Anderson and Y Gal (2024): "AI models collapse when trained on recursively generated data", *Nature*, vol 631, pp 755–9, July.

Singla, A, A Sukharevsky, L Yee, M Chui and B Hall (2025): "The state of AI: How organizations are rewiring to capture value", *QuantumBlack, AI by McKinsey*, March.

Sweeney, L (2002): "k-Anonymity: a model for protecting privacy", *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, vol 10, no 5, pp 557–70, May.

UK Government (2025): *AI Opportunities Action Plan*, January.

Wenger, E (2024): "AI produces gibberish when trained on too much AI-generated data", *Nature*, vol 631, pp 742–3, July.