

Regtech Adoption Practice Guide

Issue #9 - Customer Data and Privacy

May 2023

HONG KONG MONETARY AUTHORITY
香港金融管理局

KPMG

Disclaimer

Regtech Adoption Practice Guide is a publication published by the Hong Kong Monetary Authority (HKMA). It should be noted that the sole purpose of this publication is to provide Authorized Institutions (banks) with information on the latest regulatory technology (Regtech) developments. The industry practices and views described in this adoption practice guide are collected by KPMG. The HKMA does not endorse any use cases, solutions and/or implementation guidance described in this adoption practice guide. If a bank intends to adopt a particular solution or implementation, it should undertake its own due diligence to ensure that the technology or approach is suitable for its circumstances.

Contents

1 Introduction **4**

1.1 Background 4

1.2 Purpose 5

2 Customer data protection and privacy risk management **6**

2.1 Key challenges and developments 6

2.2 How can customer data and privacy Regtech solutions help? 7

2.3 Key considerations when adopting customer data and privacy Regtech solutions 10

3 Implementation guidance **11**

3.1 Establish the right operating model with the right people and capabilities 11

3.2 Identify data being collected and processed 11

3.3 Privacy risk assessment 12

3.4 Determine the suitable deployment model: build vs buy 12

3.5 Provide up-to-date training and education 13

4 Regtech use cases **14**

4.1 Use case #1 - Automating privacy control against evolving regulatory landscape 15

5 Conclusion **21**

A Appendix **22**

A.1 Acknowledgements 22

A.2 Relevant regulatory requirements and/or guidance 22



01 Introduction

1.1 Background

The value of Regtech in banking is coming to the fore in Hong Kong, offering clear benefits to banks, customers and regulators. In November 2020, the HKMA released a two-year roadmap to promote Regtech adoption in Hong Kong, as laid out in a White Paper titled "Transforming Risk Management and Compliance: Harnessing the Power of Regtech".[1] The White Paper identified 16 recommendations across five core areas to accelerate the further adoption of Regtech in Hong Kong.

The White Paper acknowledged that since 2019, the HKMA has published a series of "Regtech Watch" newsletters, introducing banks to Regtech use cases on the adoption of innovative technology to enhance risk management and regulatory compliance. The banks interviewed for the White Paper cited these newsletters as a valuable source of information and guidance, especially the actual or potential Regtech use cases that have been rolled out or are being explored in Hong Kong or globally.

The White Paper identified 26 specific application areas of Regtech that can benefit banks. There are significant opportunities and a strong desire from the industry for the HKMA to develop and issue "Regtech Adoption Practice Guides" around these application areas.

As a successor, this Regtech Adoption Practice Guide (Guide) series builds on the "Regtech Watch" newsletters to include common industry challenges, guidance on implementation and examples of what others have done successfully to overcome adoption barriers. The Guides are to supplement other ongoing HKMA initiatives such as the Banking Made Easy initiative, Fintech Supervisory Sandbox and the Fintech Supervisory Chatroom. Ultimately, the Guides should enhance the sharing of experience related to Regtech implementation in the industry, which will help further drive Regtech adoption in Hong Kong.

This ninth Guide of the series focuses on Regtech solutions for Customer Data and Privacy. Over 40% of banks interviewed for the White Paper indicated that they were considering using technology tools to protect customer data and comply with their privacy obligations. However,

[1] Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf

18% of respondents were of the view that this type of Regtech solutions was not mature enough in Hong Kong and had deferred their adoption plan accordingly. This Guide will provide guidance on the implementation of these solutions and share a successful use case.

Banks and other financial institutions collect, transfer, use, process, store, and delete a sheer volume of information about customers when providing services to customers and managing their business. Customer data usually include names, contact details, identification document numbers, employment details, financial and credit information, biometric data (such as voice ID, thumb print and facial recognition), geographical /location data based on customers' electronic devices, etc.

Given the sensitivity of the data collected, customers expect banks to manage personal data with extra care. Global trends indicate the introduction of further new laws and regulations that will give customers more access and control over their personal data. Any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, such data can have dire consequences for both customers and banks.

Safeguarding customer privacy is therefore more important than ever for banks to earn and maintain customer trust. To implement effective privacy controls in this digital age, banks cannot solely rely on manual processes. They should consider enhancing their data protection capability by implementing appropriate privacy Regtech solutions.

1.2 Purpose

The purpose of this Guide is to provide an overview of Customer Data and Privacy Regtech solutions, outline the common challenges encountered when implementing these solutions, and share use cases of how financial institutions have addressed challenges to successfully adopt Regtech solutions and tackle data protection and privacy issues in their organisation. This Guide follows the outline below:

1 **Illustrate how Regtech solutions can be used to address privacy risk and support customer data protection**

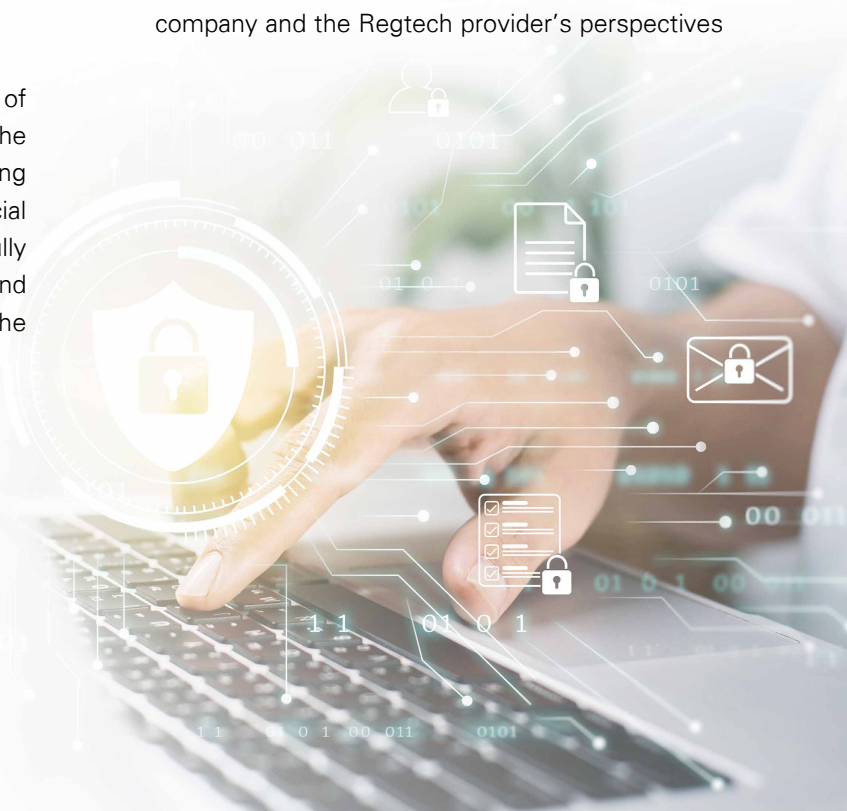
- Outline the key challenges that Hong Kong-based banks are currently facing in relation to management of customer data and privacy compliance
- Illustrate the benefits of leveraging Regtech solutions to manage privacy risk
- Describe key barriers/risks when adopting Regtech solutions

2 **Provide practical implementation guidelines to banks on the adoption of Customer Data and Privacy Regtech solutions**

- Outline key considerations when implementing Customer Data and Privacy Regtech solutions
- Provide insights on successful approaches to Regtech implementation

3 **Share use cases on the adoption of Regtech solutions to manage privacy risk**

- Describe the customer data protection challenges faced by a financial technology company and how the Regtech solution helped to resolve these challenges
- Outline the key learnings from successful Regtech implementation, from both the financial technology company and the Regtech provider's perspectives





02 Customer data protection and privacy risk management

Customer data is the lifeblood of modern banks. The amount of data collected and processed enables banks to provide more personalised services to customers, fulfil their KYC responsibilities and accelerate business growth. Yet, handling customer data lawfully, securely, fairly and transparently, while gaining efficiencies, is one of the biggest challenges for banks today. To ensure trust in financial institutions, banks need to protect and use personally identifiable data responsibly. The public's expectation is that a bank will protect customer data beyond just a compliance mindset and build ethical data use frameworks. Nevertheless, as illustrated below, there are a few factors that make customer data protection more difficult than ever for banks.

2.1 Key challenges and developments

Decentralised and fragmented customer data

Banks and their third-party service providers collect an enormous volume of customer data through multiple online and offline channels in their everyday operations. Customer data are dispersed across numerous systems and platforms, whether they are on-premises or cloud based, and even in hard copy formats managed by the banks themselves and/or their service providers. Given the large volume of customer data generated and the diversified storage across data devices and platforms, banks may struggle to have a full grasp of what types of customer data are being collected, where they are

stored, how they are used, who they are shared with, how they flow, and when and how they are deleted. In the absence of a clear picture of the data inventories and data flows, some banks may simply be unable to create a comprehensive privacy-compliant framework, thus lacking the confidence that customer data processing activities are in full compliance with relevant privacy regulations.

Regulatory divergence across jurisdictions

In the data-driven era, data protection and privacy laws are rapidly evolving in order to keep pace with technological advancements and give customers more access to and control of their data. Given that there is no international standard on the issues of data privacy, legal requirements on the meaning of personal data, how data could or should be collected, where the data should be stored, to whom data is allowed to be shared etc. , regulations vary from jurisdiction to jurisdiction. Furthermore, extraterritorial application of privacy laws has become a further consideration for banks.

As banks serve clients from around the globe and may have operations in multiple jurisdictions, managing the varying and sometimes conflicting regulations on processing customer data is particularly challenging. Banks may find it difficult to understand all of their obligations in order to comply with the applicable laws.

Siloed organisation

Protection of customer data and privacy is an effort that requires firm-wide attention and action. Nevertheless, these tasks are often regarded as purely a data security issue and the responsibility is delegated to the information technology department of the bank. Moreover, in day-to-day operations, various functions of a bank may have specific and sometimes competing interests as to how best to use and manage customer data. For example, for legal and compliance, data minimisation is a guiding principle for data collection, while the front office may prefer to obtain more (and sometimes unnecessary) customer data for client care and business development. Furthermore, on many occasions, different departments collect and manage customer data for their own purposes. A silo mentality to data management is an obstacle that banks need to overcome to properly handle customer data privacy consistently and holistically. The use of customer data in silos creates potential risks of compliance failures and data breaches.

Limited budget and resources for privacy compliance

In some cases, customer data protection and privacy has yet to gain the right level of attention from a bank's leadership despite the financial, regulatory, and reputational impacts of a breach. As a result, budget and resources allocated for achieving privacy compliance are usually limited. Due to recent events, customers are more aware of their privacy rights and the regulatory consequences that banks could face for their failures in data protection and privacy. From a bank's perspective, any data breaches will disrupt business operations, causing significant distraction to management focus, and requiring substantial effort to remediate reputational damage. Therefore, privacy teams need sufficient monetary and non-monetary resources to upgrade the privacy tools that protect one of the most valuable assets of a bank, customer data, and to minimise the risk of any data incidents. Investment in this area can also lead to more data-driven insights, for example to gain a better understanding of the demographic and financial status of customers for business development purposes, and garnering increased customer confidence in coverage of legal, regulatory, and compliance risks.

2.2 How can customer data and privacy Regtech solutions help?

Privacy compliance may be regarded by some as a cumbersome, time-consuming and costly issue for banks. However, privacy Regtech solutions can be adopted to demonstrate compliance, improve customer experience, and enhance competitiveness. This section, whilst not exhaustive, outlines some key benefits of adopting privacy Regtech solutions.

Improving compliance processes

Traditionally, privacy compliance activities have been conducted through highly manual processes, which require considerable time and resources. For example, members of a bank's front and back offices may use paper forms to collect customer data and then manually input that data into various databases. Compliance teams need to rely on various sources such as emails, spreadsheets, data dumps and paper documents to record data flows, track their tasks (for example conducting a data privacy impact

assessment, or replying to customer data access requests that have a statutory response deadline) and timelines, as well as communicate with and seek support from internal and external stakeholders. These manual processes are prone to human error, lack efficiency and in many cases are simply not able to keep up with the bank's increased privacy obligations.

Privacy Regtech solutions can improve banks' overall compliance and risk management in the following ways:

- **Reduction in human error:** Privacy Regtech tools automate some regular compliance obligations, such as data mapping to ascertain banks' data inventory and flow, managing customer consent and privacy impact assessments, and responding to customer data access requests, thus requiring less manual work. These tools also run simple consistency and accuracy checks and therefore reduce exposure to human error and can minimise any subsequent need for remediation of data associated with traditional manual compliance processes.

- **Improving data quality and accuracy:** Privacy Regtech tools can help banks to identify, monitor and address anomalies, analyse information for consistency, and create a holistic view of entities and relationships. For instance, data mapping solutions help banks determine data flows throughout different functions and may uncover any unauthorised access, while data discovery tools assist banks in determining and classifying what kind of personal data each business function possesses. Furthermore, they can eliminate duplication of data more quickly, thereby improving the quality of customer data captured and stored in banks' systems and platforms.

- **Enhancing control access:** Implementation of privacy Regtech tools can provide a greater control on access to customer data and can assist banks in complying with their internal data governance requirements.

- **Enhancing accountability:** Manual and siloed processes can mean that some functions of a bank may be unaware of their privacy obligations and their role in the firm's privacy protection efforts. The adoption of automated privacy Regtech tools can reduce such gaps and fortify a streamlined and standardised compliance process that connects each step with the right people. With privacy Regtech tools, responsible staff members and banks as a whole can have a more thorough understanding of the compliance activities as well as the associated accountability. Privacy Regtech solutions thereby strengthen banks' compliance framework by enabling greater transparency and accountability.

- **Early identification of privacy risk:** Many privacy risks arise from a lack of understanding of data protection among employees and inadequate monitoring of how customer data are being accessed and processed by personnel. Privacy Regtech tools enable banks to locate customer data, map the flow of data, thereby helping to identify any compliance gaps within processes and



create a proper framework for managing and accessing customer data. Ultimately, the use of privacy Regtech solutions can support banks in detecting, reviewing, investigating, mitigating and preventing potential privacy issues, which may include non-compliance with legal obligations, detection of suspicious activities, improper use of data and many other issues.

- **Speedy response to data breaches and incidents:** Given the sheer volume of data handled, the complex web of daily processing activities, and the sophistication of 'bad actors', it is likely that banks may experience a data breach at some point in a data lifecycle. Many privacy and financial regulators tend to require banks to report breaches and take mitigating steps within a very short timeframe of the discovery of a data breach and/or incident. The reporting and notification to regulators and/or customers varies depending on the circumstances stated in the applicable regulations and privacy laws. Privacy Regtech solutions provide ready-to-access information in the event of a breach. Banks are required to understand and assess the impacts of the breach, as well as act with an appropriate speed in organising activities with key stakeholders in order to meet the regulatory breach response requirements. Key stakeholders usually include IT security teams, legal and compliance, operations and communications departments, as well as executive management to contain, investigate and remediate a data breach in a timely manner.

Reducing costs and time associated with compliance

Privacy Regtech solutions can make compliance processes simpler and cheaper since many of the tasks become automated and standardised. These technology solutions save time associated with compliance issues, thus allowing a bank and their staff to allocate more resources to deal with other tasks to drive business growth. In the long run, banks gain a competitive advantage over competitors by adequately protecting customer data.

Boosting consumer trust and confidence

As discussed in the White Paper, with the appropriate privacy Regtech tools, banks can significantly improve their customer experience by speeding up any regulatory compliance checks and enhancing the protection of their customers' data. Further, privacy Regtech solutions, such as those focusing on handling data subject rights, will allow customers to have greater control over their personal data by understanding, monitoring and reviewing the data they have entrusted to banks. Adequately protecting and properly managing customer data are significant factors in earning customer trust in financial institutions.



2.3 Key considerations when adopting customer data and privacy Regtech solutions

Whether privacy Regtech solutions are developed in-house or by vendor partners, it is important for banks to establish proper governance and controls to manage the related risks. Below are some key risks and barriers that banks should consider when adopting privacy Regtech solutions. Section 3 of this Guide will further explore the approaches and methods that banks may adopt to overcome these barriers or mitigate the impact of these risks.

Staying current with proliferating privacy regulations

Around the world, privacy laws and regulations, many with extra-territorial effect, continue to evolve. Keeping track of all of these new laws in order to set a benchmark for privacy compliance is challenging for all organisations. Constantly changing data privacy laws also increase the difficulty of developing and adopting Regtech solutions that are capable of keeping up with the latest privacy rules. Also, banks may be reluctant to invest in Regtech solutions as they may have concerns that a solution's functionalities may not be future-proof and unable to keep up with regulatory changes. Thus, the privacy Regtech solution should possess the ability to adapt to the evolving regulation landscape over time.

Assessing technology readiness

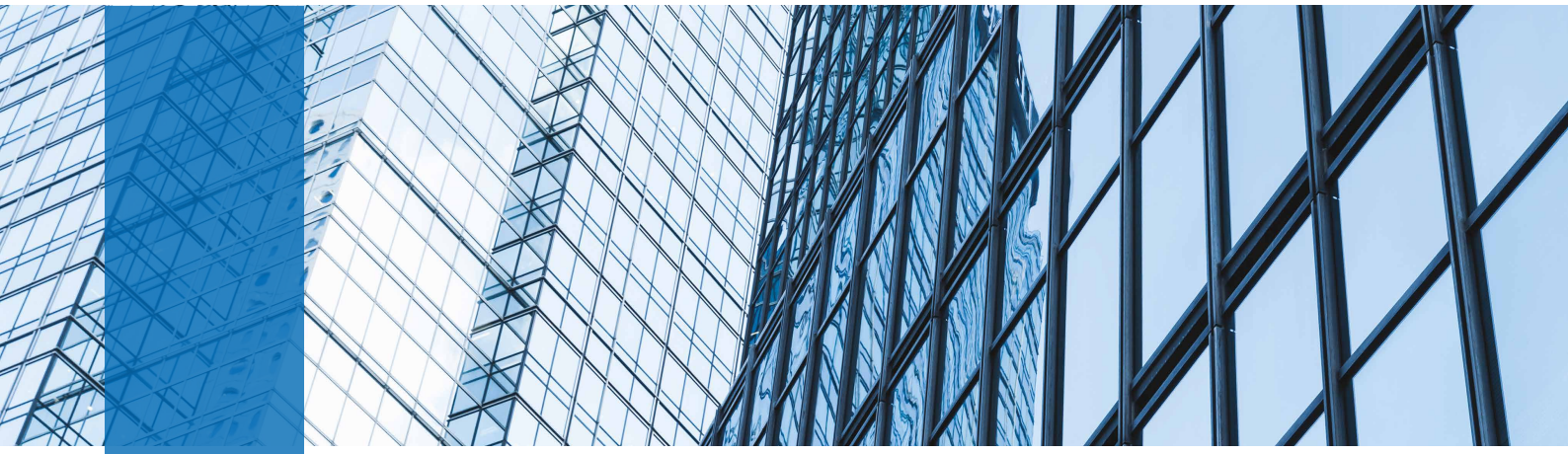
It is unsurprising that banks are using different systems and platforms in collecting, using, sharing, processing and storing customer data as data requirements have evolved over time. Each system and platform might have been part of a bank's infrastructure for many years and has become ingrained into the bank's operations. Most privacy Regtech solutions in the marketplace are designed to be integrated with banks' existing systems for the purpose of searching data, detecting gaps and providing real-time responses to address compliance needs. There is a chance that these solutions and tools may not be fully compatible with legacy systems. Therefore, issues around integration with legacy infrastructure are key obstacles for banks to consider when adopting a privacy Regtech solution. Prior to deploying any privacy Regtech solution, it is crucial that banks assess and test their technological capabilities and readiness to integrate a privacy Regtech solution into their existing system environments.

Cost and benefit analysis

Although the need to demonstrate compliance is the biggest driver for adopting privacy Regtech solutions, a lack of budget and resources also remains a longstanding barrier for privacy technology adoption. To overcome this, the adoption of privacy Regtech solutions should be considered as an investment in the business as opposed to an additional cost. The benefits of adopting privacy Regtech solutions, such as enhancing risk management, minimising privacy incidents, improving efficiency and effectiveness of privacy compliance, reducing exposure to fines, etc., should be highlighted in the business case. Given the on-going escalation of data privacy requirements, taking a short-term view on saving money and not investing in proper privacy risk management is most likely to lead to greater spending on remediation actions at a later time. Banks should also consider the cost of losing trust and confidence of existing customers in the event of a data breach, and the considerable effort that is required to regain that trust and rebuild a bank's reputation. There is also an increasing risk of regulatory fines for data privacy failures which are also widely published by regulators.

Lack of necessary in-house knowledge, capability and training

In adopting privacy Regtech solutions, banks need specialists and subject matter expertise as part of the process, e.g. privacy law experts, data scientists and engineers to identify, assess, operate, and maintain updated Regtech solutions. In some cases, in-house personnel at some banks may not have sufficient knowledge and skills to build and maintain a privacy Regtech solution. An assessment of internal skills and knowledge should be taken into consideration at the initial stages of such a project. Even if banks acquire privacy Regtech solutions from a third-party vendor, there still needs to be adequate training and support provided to personnel so as to facilitate a successful and smooth implementation of the relevant solutions.



03 Implementation guidance

In order to ensure successful implementation, banks should carry out a careful project planning process prior to adoption and put in place appropriate governance structures. This section outlines some specific implementation considerations to address the challenges and barriers outlined in section 2.3.

3.1 Establish the right operating model with the right people and capabilities

Customer data protection and privacy is not purely a compliance topic; it is also a business issue. Banks need to form cross-functional project teams consisting of members from different functional areas, such as privacy, compliance, legal, IT infrastructure and security, administration, and operations departments, as well as relevant stakeholders from the business units. A cross-functional project team enables a bank to adopt a structured approach to identify privacy issues and choose the appropriate deployment pathway to test, implement and maintain the selected solution. Having the involvement of representatives from different business units at the commencement of a project can ensure that the different priorities of various functions are addressed and considered. It also allows the expertise of various personnel to be leveraged when assessing and implementing the solution, and ultimately achieve the goal of choosing the right privacy Regtech solution, which will bring the best possible benefits to the bank as a whole.

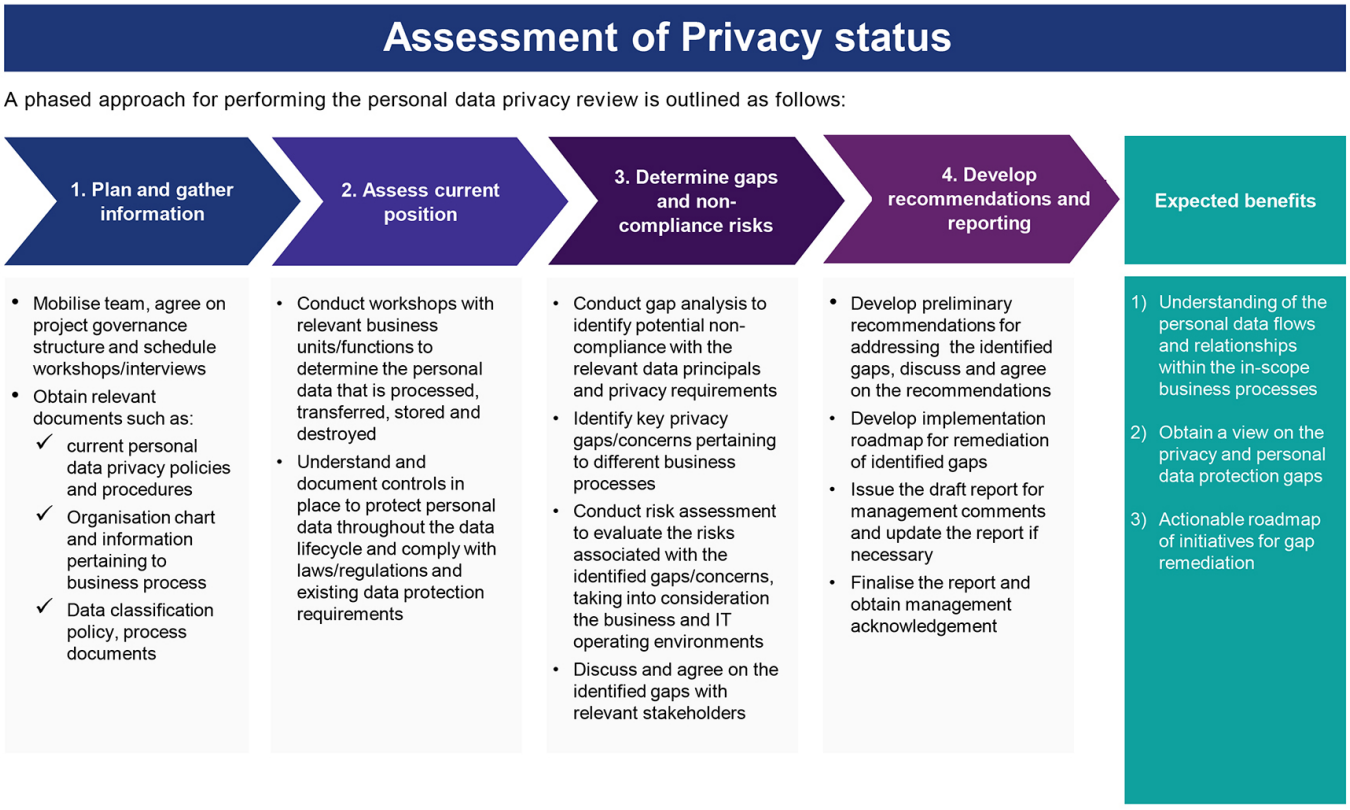
3.2 Identify data being collected and processed

Banks collect a wide range of personal data from consumers and try to get valuable insights through analytics. It is therefore important for banks to map and maintain an inventory of what customer data is collected, where customer data is located, its purpose for collection, use and disclosures, how it is used, and who it is shared with in and outside of the bank. Without an inventory and mapping of data collected and stored by the bank to determine data flows throughout its operations, it is very difficult to ensure an effective data management process and implementation of broader data protection and privacy initiatives.

3.3 Privacy risk assessment

Prior to banks deploying any solution, they should conduct a privacy risk assessment to understand the risks/gaps present in the bank's existing customer data handling framework and processes. A privacy audit should be conducted to identify the current state, assess the risks and recommend the required remedial action. The below figure sets out the methodology and approach for carrying out a privacy status or gap assessment.

Figure: Assessment of privacy status



3.4 Determine the suitable deployment model: build vs buy

When a bank has identified the type of privacy issues it needs to address, the next decision is whether to 'develop' or 'buy' the privacy Regtech solution. There are a number of factors a bank needs to consider when choosing a suitable deployment model. Key considerations include development/implementation time, pilot testing period, adequacy of skill sets, upfront/hidden/ongoing monetary costs, existing infrastructure compatibilities, functionality, and performance.

The choice of a suitable deployment model should link back to the objectives of the bank's privacy management programme, the key privacy issues to be resolved, the bank's ability to develop such a solution by itself, the strength of the in-house team, and the maturity and flexibility of external privacy Regtech solutions. The bank should take a risk-based approach and conduct a cost-benefit analysis to determine the suitable deployment model.

Building a privacy Regtech solution

If a bank decides to build its own privacy Regtech solution to address its privacy gaps/risks, some key steps should be taken in the various stages of the development lifecycle, such as:

- Evaluate how the development of the privacy Regtech solution can resolve the identified privacy risks and gaps and resonate with the banks' goals and working culture.

- Identify the people and tools required for development of the privacy Regtech solution and consider whether additional hires, such as data specialists, IT engineers, and other IT infrastructure personnel, are required.

- Determine the key requirements for the privacy Regtech solution from a data protection and data security perspective.

- Estimate the costs for rolling out the privacy Regtech solution.

- Establish a planned timeline for development, testing and rolling out of the privacy Regtech solution.

- Allocate sufficient time to train the relevant stakeholders to manage and use the Regtech solution.

- Determine how to ensure the upkeep of the privacy Regtech solution to maximise uptime and customer satisfaction.

- Conduct a pilot programme to test the platform using an appropriate selection of the business units' data and an appropriate profile for a sample of test data. A pilot programme can help to identify wider issues within the bank and find any problems to be addressed before the wider implementation.

- Identify the controls a bank has in place and which controls are still needed.

- Identify business processes to be impacted by this new platform and which of those will need adjustments.



3.5 Provide up-to-date training and education

In order for a privacy Regtech solution to be effective, all members of a bank must be actively engaged in customer data protection. They need to be educated in privacy protection in general. For those who handle customer data directly, they will need additional training tailored to their roles and learn how to make good use of the Regtech tools available to them. Recurrent and up-to-date training should be offered to employees so that they appreciate their role in handling and protecting customer data lawfully and in line with the bank's expectations about their day-to-day roles.



04 Regtech use cases

Banks need reliable, flexible, and secure systems to manage customer data and privacy in a sustainable way and assist the bank in transitioning from a defensive position around privacy to finding values of customer data. Various privacy Regtech solutions have therefore been developed by Regtech solution vendors to help banks meet privacy requirements in a way that is automated, integrated, scalable, and robust. These solutions can generally be categorised as follows:

- **Data mapping and inventory solutions:** Able to automatically scan various platforms, Enterprise Resource Planning (ERP) systems, customer relationship management systems, marketing applications, and document management platforms to identify the data collected by a bank and determine data flows throughout its operations. The records of data processing activities and data flow maps generated form the foundation for facilitating the implementation of broader data protection and privacy initiatives.

- **Privacy impact assessment solutions:** Help banks identify, allocate, and manage actions across business, technology, and compliance teams to mitigate privacy risk caused by new projects or initiatives that involve the processing of customer data. This type of solution can usually be integrated within a bank's existing systems to detect system changes requiring escalation and trigger the impact assessment process on a near real time basis.

- **Consent management:** Assist banks in collecting, recording, tracking, and removing consent preferences given by customers for processing their personal data for designated purposes, such as direct marketing. The consent managers can serve as a central repository, allowing banks to maintain an up-to-date and complete record of consent, including who have and what was given consent to, as well as when and how they consented. The consent management solution can usually be integrated into most existing business applications and systems of a bank, depending on the compatibility of legacy systems.

- **Data subject request management solutions:** Help banks to manage the evaluation, data gathering, collation and redaction of requests made by customers who wish to exercise their data rights. These can include a customer's right to access and correct personal data held by the bank. This type of solution may also include

a secure portal for customers to access and download a copy of their personal data.

- **Data breach and incident response solutions:** Provide banks with the ability to obtain records regarding the location, business and function impacted by a potential customer data breach. This type of solution also coordinates activities following a potential data breach incident, including impact analysis, risk assessment, communication to key stakeholders, and escalation within the relevant timeframe for reporting breaches to authorities and notifying impacted customers in the affected jurisdictions.

- **Privacy information solutions:** Provide extensive and automated information on the latest privacy and security laws and frameworks. The information platform gives banks access to an organised and structured database that keeps them informed of changes to privacy laws, regulatory decisions, enforcement actions, and guidance from around the world for ongoing compliance and benchmarking.

Some of the above solutions have been adopted by banks and other financial institutions. A use case and the key learning points are summarised below.

4.1 Use case #1 - Automating privacy control against evolving regulatory landscape

Challenges

Staying compliant with rapidly changing privacy laws and regulations is one of the biggest challenges for banks and financial institutions. With a view to maintaining compliance with new privacy laws, a US based financial technology company would like to evaluate how far its existing privacy programme was in compliance with the regulations, what the potential compliance gaps were and which mitigating steps needed to be taken to fulfil its regulatory obligations. The company was also looking to invest in a user-friendly privacy management Regtech solution to support its ongoing compliance work.

Upon review, there were gaps between actual operational practices and the stated corporate policies required to resolve privacy risks. In addition, the company needed to address the following challenges:

- **Centralised data inventory:** The company did not have a data inventory in place, while mapping of how data is stored, processed, shared with other systems and used throughout the company was also not available. This made it difficult for the company to conduct a privacy impact assessment to identify any non-compliance or risks of data breaches and other incidents, as well as their consequences.

- **Consent and Data Subject Access Rights (DSAR) management:** Managing the consent to process customer data and responding to requests to access personal data being stored is a complex task for the company. Customer consents are obtained via different channels. In the absence of an automated manner to keep track of the consent to process data and responding to the DSAR in a timely manner, there is a risk of breaching privacy regulations.

- **Privacy governance framework and accountability model:** It was a significant challenge for the company to effectively identify accountable parties across the three lines of defence in the risk management model[2] for the identification and management of privacy risks. There were no assigned risk owners within the company that could help drive timely mitigation measures for privacy and compliance risks identified.

- **Enterprise-wide privacy Regtech implementation:** The California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Utah Consumer Privacy Act, the Connecticut Data Privacy Act and the Colorado Privacy Act (collectively referred to as the "New State Privacy Laws" in this guide) would come into force in 2023. The New State Privacy Laws regulate the collection, use, and sharing of personal information and impose requirements in relation to disclosures, consumer rights, data protection assessment etc. The New State Privacy Laws have created new challenges for international banks and other financial institutions to properly manage their records of processing activity, obtain customer consent, deal with data subject access requests, and more. The client did not have the technology and operations capability to fully comply with the requirements under the New State Privacy Laws as there was no privacy governance solution in place.

[2] The three lines of defence within organisations are as follows: First line: consists of the executive management team and functional areas within the business that are responsible for the day-to-day ownership and management of risks.
Second line: responsible for establishing an appropriate and effective risk management framework, policies, tools, and techniques for ensuring ongoing oversight and support risk and compliance management.
Third line: provides independent and objective assurance on the appropriateness and effectiveness of controllership across the business, the effectiveness of risk management activity (undertaken by the first and second lines), and the overall effectiveness of governance.

Approach

Stage 1: Identifying compliance gaps and mitigating steps

The company was aware of the new privacy laws that would come into effect, and that it must fully comply with new data protection requirements relevant to it by 2023. As the company needed an independent review of its data, a privacy consulting firm was engaged to assess the existing privacy governance framework, create governance tools and provide support in implementation of any steps required for complying with the new laws.

Apart from the appointment of an external consultant, a project team was also set up and headed by its Privacy Manager, comprising members from the following functions:

- **Infrastructure** – Responsible for defining the tools and processes used for managing customer data
- **IT security** – Responsible for defining the security requirements currently in place to protect customer data
- **Business and marketing** – Responsible for identifying how customer data was being collected, processed and shared within or outside the company
- **Risk and compliance** – Responsible for validating the recommendations made by the external consultant
- **Project management** – Oversaw the gap analysis provided by the external consultant, managed the implementation of the recommended steps by the responsible team and provided updates to management

Stage 2: Evaluating vendors

The external consultant recommended an enhanced governance model and charter for the company's privacy management programme. In order to put the privacy management programme into practice, the external consultant also recommended the company to deploy privacy Regtech solutions to handle inventory and data mapping, cookie consent and data subject right requests, etc.

Based on the external consultant's recommendation, the project team issued a request for a proposal to Regtech solution vendors, followed by an evaluation of each vendor's response against the criteria set out. A privacy Regtech vendor was then appointed and approved for full adoption.

The selected privacy Regtech vendor was chosen based on the following significant advantages:

- **Robust Governance, Risk and Compliance (GRC) solution:** The vendor had a cross-functional GRC programme, that helped identify and manage risks within many functions of the company. This particular solution enabled assessment cooperation across the company and the rapid generation of reports and dashboards. It therefore successfully met the company's objectives.
- **Integrated privacy workflow between different modules:** The solution consisted of different modules that were able to conduct tasks such as privacy impact assessments, data mapping, and website scanning for cookies compliance. With the correct integration, these modules were able to effectively communicate with each other, fulfilling the majority of the company's requirements in a centralised location for a privacy Regtech solution.
- **Up-to-date privacy solutions for regulatory compliance:** The vendor continuously monitored new and relevant regulations, sending out notifications and updating the solution as appropriate. The vendor also consistently wrote technical blogs to assist customers, for example on how to make use of key features for enabling implementation and integration. This allowed users to stay up-to-date.
- **Affordable pricing:** The privacy Regtech vendor provided a multitude of solutions, in arranged packages with various scalable systems that were able to fit both business and compliance needs. In regard to the solution's vast capabilities and prominence in the privacy Regtech sector, the solution package was reasonably priced.

Stage 3: Full implementation of privacy Regtech solution

Due to the large volume of customer data, including records of client consent, the company needed to deploy the privacy Regtech solution to fulfil the obligations of complex regulations. Examples of these obligations include maintaining activity records of customers' data processing, obtaining customer consent for activities such as direct marketing, and responding promptly to customers' request for data. To integrate these solutions into the company's existing workflow, the company first set up a testing environment to review the functionality of the privacy Regtech solution. The vendor, along with the external consultant, configured and implemented the different modules into the company's existing systems phase by phase:

Inventory and data mapping (including Privacy Impact Assessments): The external consultant created a centralised inventory system to assist in scanning and maintaining information on the types of customer data being collected, who had access to it, where it was stored, how it was processed, and how customer data flowed throughout different functions of the company. Also, with the help of these inventories, the company was now able to visualise the cross-border transfer of customer data as per certain regulations, such as GDPR, and the level of access required to maintain their inventory correctly. As part of this implementation, the external consultant also assisted in creating assessment questionnaires to evaluate their processing activities from the privacy front, whether a particular processing activity was of high risk, needed to obtain a specific consent from the customers or required enhanced security measures. In particular, conducting a Privacy Impact Assessment for any new or updated data processing activity was a mandatory obligation for the company and a properly done assessment might also be audited by the relevant authority.

Consent and preference management: This module supported the company to manage customer consents using the DSAR webform. Customers were able to give, withdraw or modify their consent preferences, for example whether they wanted to receive any direct marketing materials via phone, text messaging or email, or whether the company can use the customer data for automatic decision-making, through the DSAR webform. Configuring and implementing preference centres also supported the company in managing customers' various consent preferences appropriately.



DSAR requests: This included a targeted data discovery function within the company's systems. To assist in managing the data subject rights in a centralised manner, the company implemented a specific module supporting the DSAR request webform onto its website. The external consultant created different workflows as per the different regulatory requirements, helping the company manage the DSAR requests promptly. Dashboards and reports to visualise DSAR requests across various metrics were created from the DSAR webform. Regarding integration of systems, the company set up the integration between the privacy Regtech solution add-on and its ticket management system, which facilitated the DSAR fulfillment process.

Key learnings

Key factors that contributed to the successful implementation of the privacy Regtech solution:

Vendor selection and management: The use of an external vendor is appealing as it likely requires lower upfront capital investment and enables faster implementation time than building the solution from start to finish in an in-house environment. Outsourcing an activity to a third party, however, does not relieve a bank of its ultimate responsibility to ensure compliance and a proper implementation. A privacy Regtech solution should tie together data policies, business processes, risk policies and regulatory requirements, and have the right user-friendly functionality. As such, selecting a credible and reliable vendor for the right solution is the key to a successful privacy Regtech adoption.

There are a number of privacy Regtech vendors offering a broad range of solutions in the marketplace. Banks should take note of the following when assessing the suitability of privacy Regtech solutions offered by vendors:

- Banks can refer to privacy technology vendor reports published by various privacy professional associations such as the International Association of Privacy Professionals[3] to understand the available solutions in the marketplace and the latest trends. These reports usually cover information about vendors, such as products/services offered and their capabilities in this space, which may assist in shortlisting a few vendors.

[3] The International Association of Privacy Professionals has published Privacy Tech Vendor Report since 2017. The report has identified some key vendors in the marketplace. The latest Privacy Tech Vendor Report can be found at: https://iapp.org/resources/article/privacy-tech-vendor-report/



- As privacy Regtech solutions usually need to integrate with existing IT systems and platforms that are already processing customer data, banks should evaluate whether the existing infrastructure can incorporate solutions as an add-on, and if they are able to do so, whether existing IT security measures will be compromised in that process.

- The privacy legal and regulatory landscape is constantly evolving across all jurisdictions. The privacy Regtech solution and its functionality should be flexible to ensure compliance with all applicable jurisdictions' laws and allow updates to address emerging laws and regulations. The ability to easily update, make changes, and customise the solution should be taken into account when selecting the solution.

- The capability of the vendor to continuously improve the Regtech solution and adapt it to evolving privacy regulations and technological advancements should be an integral part of the assessment. Banks should ask the vendors for their product enhancement roadmap and provide different historical versions of the development of the product to showcase their ability to promptly respond to changes.

Furthermore, banks should also evaluate vendors' capability by referencing the following criteria:

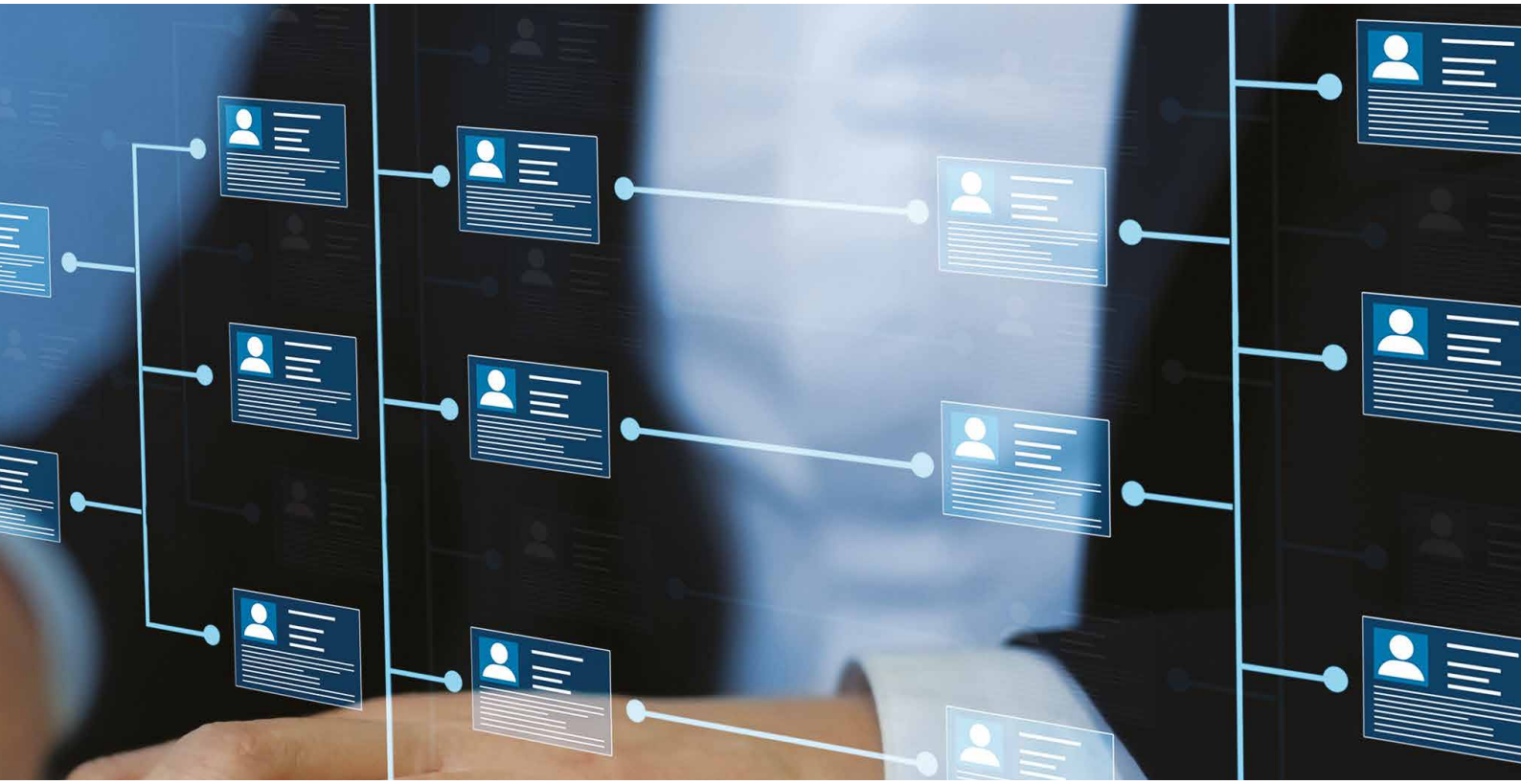
- Products and/or services – A vendor's technical capabilities and product maturity in privacy technology, its capabilities to keep pace with innovations and advancements in the privacy regulatory landscape.

- Financial – The financial health of a vendor, this may be reflected by the number of employees and customers, and its geographical presence.

- Pricing – Pricing models (upfront costs, yearly subscriptions and maintenance), options and flexibility.

- Customer experience – Any customer success stories and endorsement from customers for quality services.

- Operations – Ability to meet commitments and service level agreements, including proper safeguards to protect the integrity and confidentiality of customer data from collection, use and storage to deletion.



Executive buy-in of the privacy Regtech solution: The project team provided a clear business plan and implementation roadmap that was aligned with the company's overall objectives and future aspirations. Thus, it got the support of the senior leadership for the budget and other resources needed to roll out the solution.

Clear mapping of all roles and responsibilities: This enabled each data protection step to be considered, executed, and maintained by the right personnel. Below are a few key roles and responsibilities defined within the privacy Regtech solution:

- Privacy Manager: Responsible for putting the company's privacy strategy into action, including standards, processes, and initiatives. Collaborates with cross-functional teams and actively seeks feedback from various working groups to ensure that privacy is ingrained in the activities and aligns to the strategic goals of the organisation.

- Privacy Counsel: Provides critical legal advice and assistance to the company's cross-functional teams on any privacy-related issues. This function ensures that the company's personal data processing complies with privacy laws and regulations.

- Privacy Engineer: Assists with technical infrastructure improvements, monitoring privacy controls, and employing data anonymisation techniques. This role is responsible for partnering with the products team to implement privacy-by-design at the onset of the privacy Regtech development and implementation.

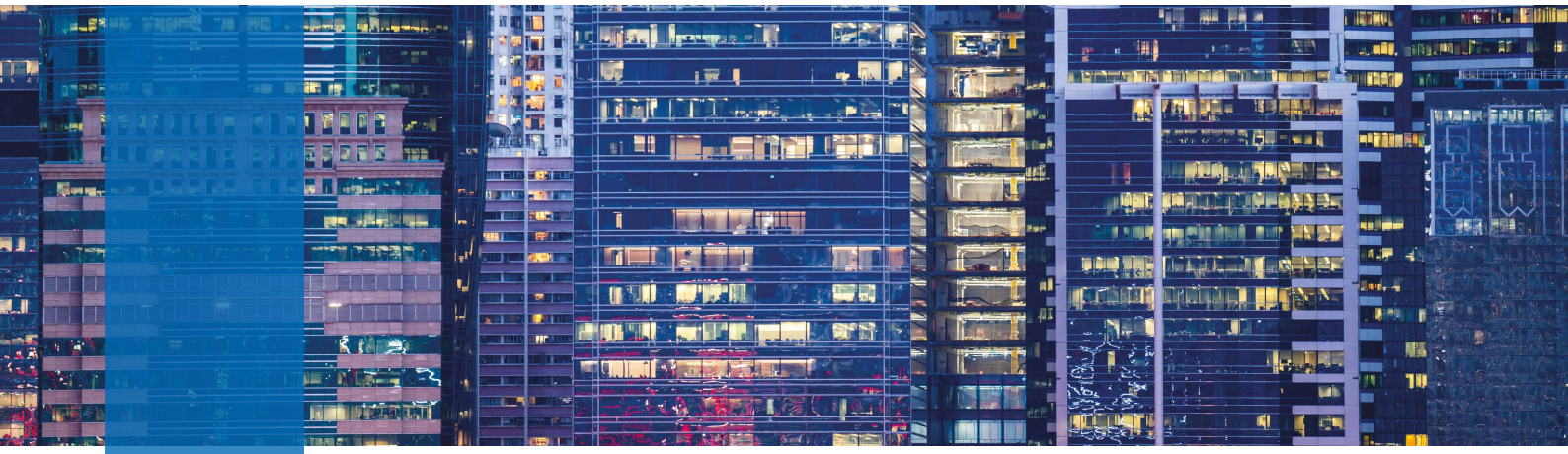
- Privacy Analyst: Controls the privacy operational risks and provides the privacy programme with relevant information to make informed business decisions.

- Privacy Tool Admin: Assists with maintenance and managing issues with the privacy Regtech solution.

Open to change management: In most cases, the adoption of any privacy Regtech solution will change existing workflows and processes. While the external consultant assisted the company in visualising and implementing the new workflows necessary for end-to-end privacy operations, members from across the organisation were willing to adapt to the changes.

Configuring the solution to make it scalable and sustainable: The privacy Regtech solution supported the company in complying with the new regulations. However, privacy laws and regulations and business operations are not static. The privacy Regtech solution vendor was required to monitor for updates that need to be actioned and to notify the company in a timely matter. If there is any change in the business workflow, members of the organisation can also make configuration changes to the solution either on their own and/or through the vendor.

Ongoing monitoring and compliance: A continuous control should be maintained over the privacy Regtech solution post-implementation. Regular training should be given to the bank's staff to equip them with the necessary skillsets to use the privacy Regtech solution. Furthermore, a periodical review and audit of the solution should be carried out to look into its appropriateness in order to ensure the accuracy of the outputs generated and the bank's ability to stay compliant with regulatory changes.



05 Conclusion

The implementation of any privacy Regtech solution is a highly complex and detailed initiative to deliver. A thorough analysis must be performed to understand all costs and benefits of adoption. A clear implementation roadmap should be formulated and the support and co-operation of all the different business functions within a bank is vital for success.

Bringing in external subject matter experts should be considered if banks do not have the relevant in-house expertise in this area. Evaluation of third-party vendors and their solutions should be conducted thoroughly in order to engage the right experts and products.

Banks are facing evolving and complex privacy laws and regulations across all jurisdictions. Current manual privacy programmes may not be able to cope with these changes and take account of future developments. While implementation may be a painful exercise and comes with some expense, the adoption of a privacy Regtech solution will allow banks to build long-term, scalable, sustainable and agile privacy programmes. The return on such investment is transformational for data management and places a bank in a position to considerably improve its operations, outperform its competitors and gain more customer trust.



A Appendix

A.1 Acknowledgements

KPMG co-authors and subject matter expert contributors: Paul McSheaffrey, David Murray, Bessie Chow, Stanley Sum, Manoj Thareja, editor Philip Wiggenraad.

A.2 Relevant regulatory requirements and/or guidance

Name	Link
HKMA Supervisory Policy Manual – Outsourcing (SA-2)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
HKMA Circular - Customer Data Protection	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf
HKMA Circular - Sound practice for customer data protection and its annex	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220404e1.pdf Annex: https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220404e1a1.pdf
HKMA Circular - Guidance on Sharing Customer Data by Authorized Institutions for Direct Marketing by Third Parties Annex - Guidance on Sharing Customer Data by Authorized Institutions for Direct Marketing by Third Parties	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20211119e1.pdf Annex: https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20211119e1a1.pdf
Office of the Privacy Commissioner for Personal Data (PCPD) – Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry	https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_banking_e.pdf
Office of PCPD – Code of Practice on Consumer Credit Data	https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/CCDCode_2013_e.pdf