The Secret of My Success – New Consumer Data Privacy Regulation for UAE Financial Institutions

Andrew Fawcett - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi

Introduction

Consumer data privacy has assumed great significance for financial services firms.

Banking, like most industries in the digital age, is undergoing a period of disruption from the likes of neobanks (direct banks that operate exclusively online), new financial technologies and the likes of bitcoin.

Critically, today's banks have to process unprecedented amounts of personal data relating to broad categories of customers in order to provide banking services and navigate an increasingly complex regulatory landscape relating to "Know Your Customer" (KYC) and "Anti-Money Laundering" (AML) laws.

Now, more than ever, banks need to think about their data management cycles in order to maintain client confidence. As consumers become more privacy conscious, and realize the impact of data sharing with financial institutions and the credit information system, data security and adherence to international data protection standards are now intrinsic to winning consumer confidence within the banking sector.

Against this landscape, the Central Bank of the UAE ("CB") has issued the Consumer Protection Regulations (Circular No.8 of 2020) ("Regulations") which apply to all Licensed Financial Institutions (LFIs) regulated by the CB whilst carrying out licensed financial activities. Specifically, the Regulations introduce requirements for LFIs relating to the protection of a client's personal data, which reflect those in the EU's General Data Protection Regulation ("GDPR") and other privacy legislations around the world.

The Regulations also empathize operational resilience which follows the implementation of similar legislations, such as the Digital Operational Resilience Act (DORA) Proposed in Europe.

Other notable aspects include the requirement for informed and express consent for direct marketing, identity verification online, data sharing and data localization (holding and storing customer data within the UAE).

Scope & Some Definitions

The scope of the regulations applies to all LFIs, whether incorporated in the UAE or in other jurisdictions. It is important to note that there is a transition period for compliance with the Regulations is until 31st of December 2021.

Consumers, are defined as any sole proprietor or natural person that receives products and services from LFIs, irrespective of whether such services or products are paid for

The term Personal Data is also used in the Regulations, and is similar to the definition in other data protection legislations such as the GDPR. It includes any information relating to an identifiable or identified

natural person such as economic, physical, biometric, mental, or cultural factors relating to the person.

In many ways, the Regulations go above, and beyond the general banking secrecy duty found in Article 120 of Federal Decree-Law No. 19/2019 which requires the customer's express permission before their data can be shared with third parties, except where data sharing is required for compliance with anti-money laundering laws.

Compliance in a nutshell – How to comply with Article 6 of the Regulations (Consumer Data Protection Requirements)

Article 6 of the Regulations emphasises consumer data protection, and Readers familiar with the GDPR will find many similar provisions within the Regulations.

Such similar principles to the GDPR, include:

- The need for technical / organisational measures or operational resilience
- Breach notification requirements to both the central bank & affected consumers
- Lawful basis for processing (consent or another lawful basis)
- Purpose limitation. Data must be collected for a lawful purpose directly related to the licensed financial activities of the LFI.
- The need for customer consent, and it being revocable
- Data minimisation. LFIs must ensure that data is adequate and not excessive in relation to the stated purpose
- Secure data sharing. The Regulations impose a legal duty on LFIs to take appropriate precautions to ensure data shared with any authorized agents remains confidential.

Under Article 6 senior management in LFIs have a duty of responsibility and accountability for data protection and management. LFIs must also implement adequate cybersecurity and monitoring infrastructure to protect consumer's information and data against any unauthorised access. Moreover, LFIs must have procedures, policies and control frameworks in place regarding the collection, confidentiality protection and authorised use of customer's data.

Who takes care of my data? Introducing the Data Management and Protection Function

Article 6.1.2 imposes a Data Management and Protection Function (the "function"), which is in many ways similar to the GDPR requirement to appoint a Data Protection Officer (DPO). The Regulations require LFIs to designate the duty to oversee and protect consumer data to a senior position in management, which emphasizes the significance of this function for LFIs. This department should specifically be responsible for oversight and compliance with the data protection requirements and privacy laws of the UAE and the CB.

The responsibilities of the data management and protection function/officer is to implement controls to identify and prevent data breaches. This includes an annual review of the data management control framework of the LFI, regular verifications of the legitimacy and integrity of data, and investigating data breaches. The function is also responsible for investigating privacy related consumer complaints, and should report the conclusion of the investigation to Senior Management and the board of the LFI.

When there is breach, stop the bleeding – Breach Notifications

Today's financial institutions face many cybersecurity challenges and the spectre of potential data breaches are part of banking's new reality.

The Regulations impose a breach/notification requirement which is similar to that found in data protection legislations such as the GDPR, or the ADGM and DIFC Data protection laws. The main difference here, is that the notification must be to the Central Bank in lieu of the data protection commission. At times, the LFI must, without delay, inform consumers of any breach to their personal data.

Data breach is explained as any unauthorized access to, and/or destruction, loss or alteration of consumer's personal data where it may reasonably pose a risk to the consumer's personal or financial security, or were it may pose reputational harm to a consumer.

It is the role of the LFI to monitor, prevent and identify potential data breaches in the first instance. The LFI could also become aware of breaches through third parties. As such, the function must promptly inform the senior management and the board of the LFI, who must subsequently notify the consumers and/or the central bank as appropriate, and without undue delay.

Further, LFIs must report all consumer complaints arising from any external, internal and/or attempted frauds to the Central Bank on a quarterly basis.

Consent, Consent, Consent

LFIs must have the consumer's express consent before using and sharing a consumer's personal data for direct marketing or prior to transferring it to any authorized agent.

Prior to obtaining consent, the LFI must proactively disclose to the consumer in writing its intent to use and or share personal data, and with who such personal data will be shared.

The Regulations require active, express consent. Moreover, consent must be freely given, explicit to a request for the use/and or sharing of personal data and must be withdrawable. The consumer shall have the right to withdraw expressed consent for either of the following:

- The processing of personal data by the LFI except were personal data is required for business operations.
- Personal data sharing with any other third parties for purposes such as sales or marketing.

Note that consent, is separate from, and does not replace the additional requirement for collecting data for a lawful basis directly related to the licensed financial activities of LFI. Overall, the requirements for what constitutes valid consent are almost identical to those in the GDPR. Additionally, the Regulations impose a minimum retention period of 5 years for consent/ a copy of the expressed consent.

Drafting Privacy Policies / Notices for LFIs

A carefully drafted privacy policy or notice is going to be of the utmost importance when complying with the Regulations as they require certain information to be provided to consumers at the time of collection of the consumer's personal data, such as how and why data will be disclosed and used. Specifically, the Regulations require the following disclosures to be made either in the form of a privacy policy or notice prior to obtaining the consumer's express consent.

- That the LFI will only collect personal data for a lawful basis directly related to a function or activity of the Consumer.
- Whether the collection is voluntary or obligatory to provide the services.
- Whether it is obligatory for the consumer to provide the data, and any consequences for failing to do so.
- A disclosure that the future withdrawal of consent by the consumer shall not affect any prior processing or its lawfulness.
- A description of the personal data being processed.
- The consumer's right and means to request access or correction of the data and how to contact the LFI with enquiries or complaints.
- The choices offered by the LFI for limiting the processing of Personal Data.

Data Sharing – When is it ok to share?

In spite of the overarching duty of confidentiality, LFIs may disclose the consumer's personal Data to third parties ("Authorized Agents") where it is:

- expressly authorized by the consumer or
- legally obliged to do so.

Examples of instances where data disclosure would be legally required include, for instance, for the purpose of compliance with the AML Law (UAE Federal Law No. 20 of 2018) or sharing data with government authorized credit information agencies as may be prescribed. Even where legally imposed,

LFIs have a duty to ensure that data shared is correct, and fair to the consumer. LFIs must promptly correct any errors or inaccuracies within 7 business days of becoming aware of them. Moreover, LFIs must be transparent with consumers, and must notify them where their data is being shared with credit information agencies.

LFIs also have a duty to educate consumers on the credit information system, and the possible limitations on accessing future financial products and/or services. This legal obligation is monumental as it recognizes the inequality of bargaining power between banks and consumers, and aims to encourage financial institutions to take responsibility for their client's financial education.

Where data sharing with third parties is not prescribed by law, e.g. where it is being shared for the purposes such as outsourcing, or sales or marketing, the LFI must obtain the consumers express written consent. Further the LFI must enter into an agreement with the third party (i.e. Authorized Agent), which secures the confidentiality of personal data, and warrants that the Authorized Agent has appropriate technical and organizational measures for safeguarding the data. Further, LFIs must use encryption and other measures used to secure data transfers where sharing data with Authorized Agents.

Retention

The minimum retention period for all personal data is 5 years. Following the minimum retention period, LFIs must ensure that personal data is either destroyed if no longer required for its initial purpose, or no longer required by law i.e. by government authorized credit information agencies. Records of express consent must also be held for a minimum of five years. In case of breach, the LFI must maintain records of such events and any disciplinary action taken for a minimum of five years after the event being recorded.

Data Localisation

The Regulations potentially impose a strict data localisation requirement. As such, LFIs must store transactional and consumer data "*within the UAE, as prescribed by*" the CB. Some further clarity is needed as to what these prescriptions are. That is, are the Regulations referring to existing (but limited) requirements of the CB concerning transaction data of payment processors or outsourcing by finance companies, or are there further prescriptions to be issued? LFIs must carefully observe this requirement when engaging cross border activities.

Online Identity Verification

The Regulations provide that where the consumer's identity verification is conducted online, the LFI must apply more than one evidence of identity verification for electronic services.

This is important as the CB is recognising that identity verification can be done by LFI's online and formally recognises the need for multifactor verification.

Regarding digital or online transactions, there is a further duty on LFIs to secure digital transaction processing and controls and enhance customer identification methods. Accordingly, Regulations recognise the prevalence of fin-tech and digital banking, and require LFIs to strengthen and amplify their digital channels.

State of the Art Security – Building operational resilience on an organisational level

With the global volume of data predicted to have doubled from 2018 to 2022, operational resilience and cybersecurity should be implemented from the outset, and the overriding duty of confidentiality must be integrated into technical and organizational processes, specifically, relating to where personal data is held, used or accessed by Authorized Agents.

With operational resilience high on the agenda of financial services, LFIs are legally required to control their operational risks, and also to manage disruptions when they do occur. Specifically, the Regulations requires LFIs to have a proper data management control framework with policies', procedures, system controls and checks and balances to protect consumer data. LFIs must ensure that they are able to identify and resolve information security incidents as soon as they occur. The Regulations recognise that a strengthened IT and cybersecurity infrastructure is only a part of successful incident response. As such, the Regulations require LFIs to conduct regular training and workshops for their employees in order to

familiarise them with common security incidents, and how to protect consumer data privacy. Finally, LFIs must report regularly monitor their data management systems e.g. such as through penetration testing and must report any apparent vulnerabilities in the security and online systems to the Central Bank on a quarterly basis.

Conclusion

The consumer privacy provisions of the Regulations bring financial regulation in the UAE closer to international data protection standards. Unlike the GDPR and other general data protection frameworks such as the California Consumer Protection Rules (CCPA), the Regulations have the added benefit of being sector specific and specially tailored to the financial services industry.

While sector specific, the significance of Article 6 of the Regulations is that it is a data protection regulation at the Federal level and applies outside of the financial free zones.

The Regulations recognise that banks, and other licensed financial institutions process significant amounts of sensitive consumer data, which can affect consumer’s security, reputation, or financial wellbeing in case of erroneous information entering the credit information system, and attempt to strengthen consumer’s rights over their data and privacy.