The UAE Central Bank has established a Financial Consumer Protection Regulatory Framework that introduces novel requirements for the protection of clients’ personal data. In this article, we consider the new framework, its scope and timeline for compliance and what this means for financial institutions.

Background

In accordance with its objectives set out in Article 121 of Federal Law No. 14 of 2018 on the protection of customers of Licensed Financial Institutions (LFIs), the UAE Central Bank (CBUAE) issued its Consumer Protection Regulation (CPR) in December 2020, followed by the Consumer Protection Standards (CPS) in January 2021, effectively establishing the CBUAE’s new “Financial Consumer Protection Regulatory Framework” (the Framework). The Framework introduces, among other things, requirements for LFIs that relate to the protection of clients’ personal data, which mirror those found in the European General Data Protection Regulation (GDPR).

Overview

The Framework draws upon a broad array of principles premised on international standards which enhance the competitiveness, integrity and stability of the UAE’s banking sector. Notably, the CPR introduces data protection-related requirements, in what can be regarded as a first for “Onshore UAE” (i.e. outside the financial free zones).

We note that the protection of consumers’ personal data and privacy is one of the many protections offered by the Framework in relation to disclosure and transparency, institutional oversight, market conduct, and conduct of business which are aimed at ensuring responsible financing practices, complaint management and dispute resolutions, consumer education and awareness, and financial inclusion.

Scope and timeline for compliance

Application of the Framework

The Framework applies to all LFIs (whether incorporated in the UAE or in other jurisdictions, or having a branch, subsidiary or representative office in the UAE) that are licensed by the CBUAE to carry on a “Licensed Financial Activity” in the UAE and which offer their products and services to “Consumers”. Licensed Financial Activities include, among others, providing credit or fund facilities of all types; providing currency exchange and money transfer services; providing monetary intermediating services; or arranging and/or marketing for Licensed Financial Activities.

Deadline for compliance

LFIs have until 31 December 2021 to update their practices to comply with the CPR.
Who/what is a “Consumer”?

“Consumers” are defined as any natural person (or sole proprietor) who receives products and services from LFIs, regardless whether such products and services are paid-for or not.

What is “Personal Data”?

“Personal Data” is defined in the CPR to mean any information relating to an identified or identifiable natural person, including factors specific to the biological, physical, biometric, physiological, mental, economic, cultural or social identity of that natural person. This definition is broadly in line with that of the GDPR.

The new Consumer Data Protection requirements

CPR

The CPR introduces a key data protection principle which brings the new CBUAE Framework closer to international data protection standards. Under the CPR, LFIs are required to (among other things):

- Establish a department to oversee and manage the protection of consumer “Personal Data”.
- Collect consumer Personal Data only to the extent required to allow LFIs to carry out their licensed activities. This reflects the “data minimisation” principle of international data protection legislation, such as the GDPR.
- Implement policies that specify the retention period of consumer Personal Data held by LFIs.
- Implement appropriate security measures to detect, track and record unauthorised access to consumer Personal Data, and to prevent the misuse of consumer Personal Data.
- Notify (i) the CBUAE of all “significant” breaches affecting consumer Personal Data; and (ii) affected consumers if the breach poses a “risk to their financial or personal security”. LFIs may be required to reimburse consumers for actual harm suffered from a data breach.
- Ensure that consumers can make informed choices and provide express consent in relation to the collection and use of their Personal Data by LFIs, and its sharing with third parties.
- Implement sound and effective management and business practices to protect consumer Personal Data, including internal controls to detect breaches, and to be able demonstrate the LFI’s compliance with the Framework.

CPS

The CPS take the obligations set out in the CPR a step further by adding clarifications and imposing additional, more onerous, data protection requirements that LFIs must comply with.

Data protection principles

The CPS set out a number of data protection principles that are similar to international data protection legislations, such as:

- Lawfulness: LFIs should obtain “express” consent of Consumers before collecting, using and/or sharing their Personal Data.
- Fairness: LFIs should have a lawful purpose to collect Personal Data, which should be directly related to the Licensed Financial Activities of the LFI.
- Transparency: Before requesting the consent of Consumers, LFIs should inform Consumers in writing with respect to how their Personal Data will be processed.
- Purpose limitation: Personal Data should be adequate and not excessive in relation to the purpose for which they are collected by the LFI.
Establishing a Data Management and Protection role

The CPS require LFIs to allocate the responsibility and accountability of data management and protection within the LFI to a senior position in management who reports directly to senior management of the LFI.

The Data Management and Protection officer should carry out a number of functions and responsibilities, which include putting in place controls to detect and prevent data breaches, annually reviewing and improving the "Data Management Control Framework" of the LFI, handle privacy related consumer complaints and issue reports to senior management and the Board of the LFI on significant data management violations and breaches.

Express Consent

The CPS define "express" consent as consent that is "freely and explicitly" given by the Consumer.

The CPS provide Consumers with the right to withdraw their consent at any time when their Personal Data is processed by LFIs (unless it is required for the LFI's business operations related to the Consumer's products and services) or when their Personal Data is shared with authorised agents or third parties for purposes such as sales and marketing.

Information Notices

Information notices should include, for example, information on how data will be collected, used, disclosed, data mined and profiled by the LFI.

Prior to entering into a contract with the Consumers, LFIs should disclose additional information about the data they collect from Consumers; such as the lawful purpose for which they collected their Personal Data; whether the collection of their data is obligatory or voluntary, and if obligatory, what the consequences are of the Consumer not providing their data; and a description of the data processed and its source.

Consumer Data Protection Rights

The CPS provide Consumers with the right to withdraw their consent under certain circumstances and the LFI must comply within 30 calendar days of the Consumer requesting withdrawal.

Consumers also have the right to request access to and correction of their data / Personal Data.

Data Sharing

The CPS require LFIs to include appropriate provisions for safeguarding the confidentiality of Personal Data in their contracts with "authorised agents" (i.e. entities that enter into transactions in the name and for the account of LFIs) who are used for outsourcing of functions and services where they may have access to Consumers' Personal Data.

When sharing Consumer data with third parties, LFIs should ensure that their contracts with such third parties contain appropriate provisions that restrict the sharing of the data.

Data Localisation

- Storage limitation: LFIs should not process or use Personal Data for any period longer than is necessary for the purpose for which the Personal Data was collected. However, the CPS imposes a minimum retention period off 5 years for all Personal Data, documents, records and files.
- Security: LFIs should ensure that Personal Data is collected with appropriate security and protection measures against data breaches.
The CPS appear to impose a strict data localisation requirement for all “Consumer and transaction data” collected by LFIs. It requires LFIs to hold and store all Consumer and transaction data within the UAE as prescribed by the CBUAE. However, no information is provided as to whether there are any exceptions to this requirement and how such data should be held within the UAE. This requirement therefore may be problematic for those LFIs that have operations outside the UAE.

**Reporting Data Breaches**

Data breaches must be notified to Consumers, *without delay*, where such a breach may “*reasonably pose a risk*” to the Consumer’s financial and personal security and/or where such a breach may pose “*reputational harm*” to a Consumer.

Any “*significant*” breaches must be notified to the CBUAE *immediately* in a manner as prescribed by the CBUAE (although the CPS do not provide further details on how LFIs should notify such breaches to the CBUAE).

The robust approach to the protection of banking consumers’ Personal Data in the CPR and CPS is reminiscent of the stance adopted by the UK Financial Services Authority in 2008, that any breach of a bank customer’s personal data should be treated as a financial crime.

**Other principles under the CPR**

In addition to the above data protection principle, LFIs should also take note of the other key principles and requirements introduced by the Framework. We set out a summary below of the other key principles which LFIs will need to consider when updating their systems and business processes:

<table>
<thead>
<tr>
<th>Principle</th>
<th>Key requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disclosure and transparency</strong></td>
<td>proactively provide all information necessary to consumer relationship at all stages of their relationship</td>
</tr>
<tr>
<td><strong>Institutional oversight</strong></td>
<td>implement a robust management oversight and responsibility structure to cover LFIs' activities, including compliance, risk and audit controls, as well as up to date policies, procedures and staff training</td>
</tr>
<tr>
<td><strong>Market conduct</strong></td>
<td>observing ethical, non-abusive practices</td>
</tr>
<tr>
<td><strong>Complaint management and resolution</strong></td>
<td>put in place a fair, accessible, transparent and free process to address any complaints from consumers which must be resolved in a timely manner</td>
</tr>
<tr>
<td><strong>Financial inclusion including gender and race equality</strong></td>
<td>consider the requirements of vulnerable groups and people of determination for their products and service designs and establish an anti-discrimination code of conduct</td>
</tr>
</tbody>
</table>
**Sanctions**

*Under the Framework*

Breaches of the Framework may be subject to supervisory action, which can lead to the CBUAE imposing sanctions and penalties. CBUAE-imposed sanctions may include fines or restricting the powers of LFIs’ senior management or board members.

*Under the Banking Law*

The sanctions the CBUAE can impose under the Framework are in addition to those which the CBUAE can impose under the **Banking Law** of 2018 (Decretal Federal Law No. 14 of 2018 Regarding the Central Bank and Organisation of Financial Institutions and Activities) which include: (i) issuing a warning; (ii) prohibiting the LFI from carrying out certain operations or activities; (iii) imposing conditions or restrictions on the LFI’s licence; or (iv) reducing or suspending the ability of the LFI to draw on CBUAE’s funds through the standing facilities.

**How to get ready**

LFIs should carefully consider how they intend to comply, long before the expiry of the grace period since some of the necessary changes may require an overhaul of their systems and controls as well as a significant shift in the approach of LFIs in relation to the novel data protection requirements. LFIs should start this process as soon as possible by:

1. putting in place the groundwork for a data protection department and a Data Management and Protection role;
2. reviewing their data protection and privacy policies and processes; and
3. updating their terms and conditions/client and third party agreements to ensure all of the above is communicated to consumers and their consent is duly obtained (as and where needed).

Our leading data privacy and financial regulatory teams can support you on the journey to compliance with the Framework. We have extensive experience in helping organisations to develop and implement privacy and compliance frameworks which are aligned with local and international legislation and best practice.

Please contact the authors for further information.