



# Consumer Protection Regulation

**A brief summary of  
Article 6 requirements on  
data protection**

March 2021

---

[kpmg.ae](http://kpmg.ae)







# Contents

Introduction	04
To whom is the Regulation applicable?	06
What is the primary objective of the Regulation?	06
What is covered in the Regulation?	07
Accelerate compliance with KPMG's Data Protection and Privacy Framework	13

# Introduction

The digital landscape is evolving rapidly, accompanied by the increased usage of advanced technologies to process consumer data. This has emphasized the need for consumer protection and associated rights.

The Central Bank of the UAE (CBUAE) has issued the Consumer Protection Regulation (the Regulation), acting as an overarching regulatory framework for licensed financial institutions (LFIs). The Regulation ensures consumers' interests are protected when using any financial product and/or service or when a relationship with an LFI exists.

By introducing this regulation and the accompanying standards, the CBUAE seeks to ensure that LFIs' approach to consumer protection is in line with international standards. The Regulation focuses on developing a variety of capabilities to understand, manage and protect consumers' data and associated complaints/inquiries.





# To whom is the Regulation applicable?

This regulation and accompanying standards apply to all LFIs licensed by the CBUAE, in relation to activities specified in Article 65 of the Decretal Law No. 14 of 2018.

# What is the primary objective of the Regulation?

The primary objective of the Regulation is to protect consumers and contribute to the overall stability of the financial services industry. The Regulation aims to strengthen governance and promote responsible financing practices and protect consumer rights.



# What is covered in the Regulation?

The Regulation comprises 15 articles, providing information about the minimum measures all financial institutions are required to take in order to protect customers' data.

<b>Definition</b> Article 1	<b>Disclosure and Transparency</b> Article 2	<b>Institutional Oversight</b> Article 3	<b>Market Conduct</b> Article 4	<b>Business Conduct</b> Article 5
<b>Protection of Consumer Data and Assets</b> Article 6	<b>Responsible Financing Practice</b> Article 7	<b>Complaint Management and Complaint Resolution</b> Article 8	<b>Consumer Education and Awareness</b> Article 9	<b>Financial Inclusion</b> Article 10
<b>Shari'ah Compliance for Financial Services</b> Article 11	<b>Conflict with Other Regulations</b> Article 12	<b>Enforcement and Sanctions</b> Article 13	<b>Interpretation of Regulation</b> Article 14	<b>Publication and Effective Date</b> Article 15

Many organizations struggle to manage a sprawling data footprint, which continues to grow in size and complexity. To enable risk-based data protection and compliance, Article 6 (Protection of Consumer Data and

Assets) emphasizes protection of consumer data and rights. This paper will focus on the data privacy elements of the Article.

Article no.	Sub-Article no.	Article description	KPMG’s cybersecurity and privacy analysis	Mapping with KPMG framework
<b>Article 6: Protection of Consumer Data and Assets</b>				
6.1 Consumer Data Protection	6.1.1	Licensed Financial Institutions are required by the Article 120 of the Decretal Federal Law No. (14)	<p><b>Confidentiality of consumer data and purpose limitation:</b></p> <ul style="list-style-type: none"> <li>– Clearly identify, document and communicate the purpose or purposes for processing consumer data</li> <li>– Regularly review the processing purposes and, where necessary, update the documentation</li> <li>– Limit access to consumer information by implementing access control mechanisms</li> <li>– Implement security and monitoring measures to detect and track unauthorized internal access or use of consumer information</li> </ul>	<ul style="list-style-type: none"> <li>– Security for privacy</li> <li>– Policies, notice and consent</li> <li>– Inventory/data mapping</li> </ul>
	6.1.2.1	Licensed Financial Institutions must establish a function in their organization that is responsible for Data Management and Protection including responsibility for maintaining policies, procedures, systems and controls to protect Consumers’ Personal Data and information against misuse, unauthorized access and undue processing and analysis	<p><b>Data management function:</b></p> <ul style="list-style-type: none"> <li>– Establish a function that is responsible for data management as well as data protection and privacy of consumer data</li> <li>– Define responsibility for maintaining data protection and privacy policies, procedures, systems and controls to protect consumers’ personal data</li> </ul>	<ul style="list-style-type: none"> <li>– Governance and operating model</li> <li>– Data strategy</li> </ul>
	6.1.2.2	Licensed Financial Institutions must have policies that specify duration of record keeping and Data retention in accordance with the applicable laws, regulations and business	<p><b>Data retention management:</b></p> <ul style="list-style-type: none"> <li>– Establish data retention policies in line with the regulatory/standard requirements</li> <li>– Ensure the data retention policies are enforced for digital and non-digital consumer data</li> </ul>	<ul style="list-style-type: none"> <li>– Information lifecycle management</li> </ul>

6.1.2.3	<p>Licensed Financial Institutions must have appropriate security and monitoring measures in place to detect and track unauthorized internal access or use of Consumer information. Any breach of access, misuse or unauthorized release must be recorded including any harm done by such breach for future reporting to and review by the Central Bank</p>	<p><b>Logging and monitoring for access management:</b></p> <ul style="list-style-type: none"> <li>– Implement capabilities that can identify unauthorized access by systems and resources in real time</li> <li>– Implement capabilities for logging and monitoring of all activities performed on consumer data</li> </ul>	<ul style="list-style-type: none"> <li>– Security in privacy</li> <li>– Processes, procedures and technology</li> </ul>
6.1.2.4	<p>Licensed Financial Institutions must notify the Central Bank of all significant breaches of Consumer Data and information and notify any Personal Data breach to Consumers where a breach may pose a risk to the financial and personal security of the Consumer without undue delay. Licensed Financial Institutions are liable for reimbursing any direct costs incurred by the consumer for actual harm done as a result of the breach</p>	<p><b>Breach notification:</b></p> <ul style="list-style-type: none"> <li>– Document breach communication plan and assign respective roles within the function that is responsible for data protection and privacy of consumer data (as well as who will communicate the breach notification to the Central Bank and the consumer)</li> <li>– Document indemnification clauses in the contract with consumer</li> </ul>	<ul style="list-style-type: none"> <li>– Incident management</li> </ul>
6.1.2.5	<p>Licensed Financial Institutions must ensure that Consumers are able to make informed choices with respect to providing expressed consent as to their Data being collected, used and shared with third parties and within the Licensed Financial Institution</p>	<p><b>Consent management:</b></p> <ul style="list-style-type: none"> <li>– Below mentioned practices shall be followed while seeking consent from consumer: <ul style="list-style-type: none"> <li>– Outline why their personal data is being collected</li> <li>– Ensure consumers know how their personal data will be used</li> <li>– Be certain your organization has clear policies and procedures regarding the collection, use or disclosure of personal data</li> <li>– Ensure consent forms are time limited and capture all necessary requirements that should be known by the consumer</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>– Policies, notice and consent</li> </ul>

	6.1.2.6	Licensed Financial Institutions must prevent the misuse of Consumer information and Data	<b>Data handling and awareness:</b> <ul style="list-style-type: none"> <li>– Implement security awareness and training programs</li> </ul>	<ul style="list-style-type: none"> <li>– Training and awareness</li> </ul>
6.2 Protection of Consumer Assets, Information and Data against Financial Crimes, Misappropriation and Misuse	6.2.2.1	Without prejudice to other laws and regulations, Licensed Financial Institutions must treat Consumers information relationships and business affairs as private and confidential	<b>Confidentiality:</b> <ul style="list-style-type: none"> <li>– Ensure the users processing consumer personal data are obliged to confidentiality and non-disclosure clauses</li> </ul>	<ul style="list-style-type: none"> <li>– Risk, control and monitoring</li> </ul>
	6.2.2.2	Licensed Financial Institutions must put in place strict internal controls to effectively protect Consumers' deposits, savings, funds held by stored value facilities and other assets as well as Consumer information and Data, against internal frauds.	<b>Regulatory compliance:</b> <ul style="list-style-type: none"> <li>– Ensure compliance with Stored Value Facilities Regulation issued on 30 September 2020, the CBUAE for SVF providers or entities carrying out any SVF business functions</li> <li>– Implement adequate internal and access controls and logging of IT systems to protect consumer information and data against internal fraud</li> </ul>	<ul style="list-style-type: none"> <li>– Regulatory management</li> </ul>
	6.2.2.3	Licensed Financial Institutions must apply sufficient resources to be able to detect both external and internal frauds quickly and ensure they are fully addressed with future prevention measures	<b>Security monitoring:</b> <ul style="list-style-type: none"> <li>– Implement proactive security measures such as vulnerability assessment, pen testing, red-teaming exercises, etc.</li> </ul>	<ul style="list-style-type: none"> <li>– Security for privacy</li> <li>– Processes, procedures and technology</li> </ul>
	6.2.2.4	Licensed Financial Institutions must compensate Consumers in a timely manner for financial losses and expenses resulting from Financial Crimes, misappropriation, cyber-attacks and misuse of assets and information unless it can be proven that the loss was due to the gross negligence or fraudulent behavior of the Consumers	<b>Breach management:</b> <ul style="list-style-type: none"> <li>– Document indemnification clauses in the contract with the consumer</li> </ul>	<ul style="list-style-type: none"> <li>– Risk, control and monitoring</li> <li>– Incident management</li> <li>– Third-party management</li> </ul>

6.2.2.5	Licensed Financial Institutions must ensure their security and protection systems are updated and have the capacity to develop and adopt new approaches to cyber security as required	<p><b>Continuous improvement:</b></p> <ul style="list-style-type: none"> <li>- Demonstrate processes and technologies are up to date with the newest approaches</li> <li>- Implement leading design and technologies to enhance the data protection and privacy measures of consumer data</li> </ul>	<ul style="list-style-type: none"> <li>- Security for privacy</li> <li>- Processes, procedures and technology</li> </ul>
6.2.2.6	Licensed Financial Institutions must demonstrate they have carried out sufficient Consumer awareness activities related to educating Consumers of the need to protect themselves from Financial Crime	<p><b>Consumer awareness and training:</b></p> <ul style="list-style-type: none"> <li>- Develop customer awareness training plans which focusses on data security, privacy, financial frauds on frequent basis</li> <li>- Utilize statistics to communicate the importance of security and privacy to the consumer</li> <li>- Keep consumers informed about current threats to personal data</li> <li>- Encourage consumers to share potential errors/issues immediately</li> </ul>	<ul style="list-style-type: none"> <li>- Training and awareness</li> </ul>





# How can KPMG assist?

## Our global data privacy footprint

KPMG's cyber security and privacy practice is present in major markets around the world – 29 countries in total. We assist organizations in transforming their security, privacy, and continuity controls while maintaining the confidentiality, integrity and availability of critical business functions.



## Data strategy and governance

KPMG utilizes proven frameworks, such as advanced data management (ADM), to support organizations. Our teams conduct assessments and provide insight into the current state in order to identify gaps and translate insights into next steps and implementation roadmaps.

Our goal is to assist organizations in developing a data management practice that is built on the right foundation and has a clear data strategy, target operating model and roadmap to drive the best value from data assets.



*The information contained herein is of a general nature and is not intended to address the specific circumstances of any particular individual or entity. Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.*



# Contact us



## **Timothy Wood**

Partner | Cyber Security  
and Privacy

**m:** +971 56 409 6842

**e:** [timothywood@kpmg.com](mailto:timothywood@kpmg.com)



## **Maliha Rashid**

Director | Data Privacy Lead  
Digital & Innovation

**m:** +971 50 608 2013

**e:** [mrashid5@kpmg.com](mailto:mrashid5@kpmg.com)

[kpmg.com/ae](https://kpmg.com/ae)

Follow us on:



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International. Designed by KPMG Lower Gulf Creative team.

Publication number: 3391

Publication date: March 2021