

# Know How

## 1 UAE2020 Moveable Assets Security Law

### (1) Introduction

The regime for taking security over movable assets in the UAE was recently updated by Federal Law No.4/2020 on Guaranteeing Rights Related to Movables, which came into force on 1 June 2020 (the “New Regulations”).

The Regulations repeal Federal Law No. 20/2016 on the Mortgaging of Movable Property as Security for Debts which was enacted on 15 December 2016 and came into force in March 2017 (the “Old Regulations”). The Old Regulations introduced the legal regime for registering a security interest over movable assets located in the UAE and addressed a number of previous shortcomings in the registration of moveable securities, which amongst others included the ability to create a security interest akin to a common law floating charge over future assets and dispense with the need to deliver possession of the secured asset. This security interest could be perfected by registration in the public register held by Emirates Development Bank and named the Emirates Moveable Collateral Registry.

One of the significant changes that the New Regulations has brought about is the introduction of a new security registry which will be established by a Ministerial Decision and will replace the Emirates Movable Collateral Registry.

It is not yet clear whether existing registered security interests will automatically migrate to the

new security register, because the New Regulations state that any security interest must be registered in the new security register within six months of the Implementing Regulations being published. The Implementing Regulations are expected to be issued by the Ministry of Finance within six months from the date of publication of the New Regulations. These Regulations will regulate the operations of the Register.

### (2) Significant Amendments

Some of the significant amendments in the New Regulations is the list of assets which cannot be used as collateral i.e. such as objects intended for personal or home use, unless these are used as mortgaged property to finance that property's purchase.

Entitlements of insured or beneficiaries from an insurance contract, are also no longer included unless these entitlements are considered proceeds of the security asset. Future rights entailed from inheritance or wills have also been excluded.

The definition of an accounts receivable or a right to receive money owed to the security provider by a third party now specifically excludes the rights to collect payments established in endorsable deeds, deposited in accounts payable at banks or under securities or financial instruments.

Under the New Regulations, it is possible to register a security interest before the conclusion of the relevant security contract or the agreement which creates that security interest, provided the security provider has given written consent to this.

A secured party may also assign their security interest in accounts receivable without the consent of the security provider and the assignment can be registered as an amendment to the original security registration. If the secured assets are sold or disposed of in the ordinary course of business, they then pass to the purchaser free from any security interest, provided the purchaser was unaware of the secured party's interest over these assets, at the time they entered into the sale agreement. This is very different to the position under the Old Regulations, where the goods could be disposed of, without any security interest even if the purchaser was aware of the security interest, provided the disposal was made at market price.

There are also provisions on the timing of registrations. Where the security interest relates to acquisition financing, for example, of equipment, inventory or intellectual property rights, the security interest over the financed assets must be registered in the register within seven working days of the security provider gaining possession of it.

It is also worth noting if multiple security interests are enforceable over the same fungible product or mass, these rights have equal priority status over the product or the mass and every secured party may claim their right from the product or the mass at the ratio of their security interest to the mass or the product at the time of integration.

There are points of note too where there is a breach by the security provider or the underlying obligor. In such cases the secured party may give seven days' written notice to the security provider and any third-party holder of the security assets if applicable, of their intention to seize, sell, lease or otherwise dispose of the assets and they must also provide the Court with details of the proposed sale, lease or disposal. In the current economic climate it is also worth noting a security interest under the New Regulations will survive commencement of any bankruptcy procedures against the security provider.

The security interest will also retain the priority it had before the launch of the bankruptcy procedures. Previously under the Old Regulations, none of the execution procedures on the mortgaged property under the Law were valid, if bankruptcy procedures against the security provider had been launched. This will be of particular concern to lenders who may need enforcement of their security interest against bankrupt security providers.

### **(3) Effect of the New Regulations**

There is currently some uncertainty on the rights of a secured party that holds a registered security interest on the Emirates Movable Collateral Registry, in line with the Old Regulations since the repeal of this Law. This will be particularly concerning to lenders, who have registered security interests to secure financing to borrowers and should to be urgently addressed, possibly through an amendment to the New Regulations to recognise the registrations already registered.

The New Regulations, however do provide that any obligee may publicise a Security Interest from any transaction which was made prior to the issuance and enforcement of the New Regulations without the need to obtain the Guarantor's consent" and that this will be done within six months from the date of the entry into force of the Implementing Regulation. All lenders should be prepared to re-register their existing security interests, currently on EMCR, to the new Registry within six months of the new Implementing Regulation, should it be required. The priority of the rights publicised during the six month period will be determined from the date of their enforceability under the New Regulations which they are created (i.e., the previous registration date) or from the date of their publicity in the new Register.

Public access to the information contained in the Register may be granted (and the procedures for

this will be further detailed in the Implementing Regulation) and that a request may be made to obtain a hard-copy or electronic report on the information contained in the Register; such a report will have binding force as evidence of the date and time of the publicity of the security interest to the Register.

#### **(4) Types of collateral considered in Federal Law No. 4/2020**

The New Regulations concern the creation, registration and enforcement of security interests over collaterals.

In accordance with Article 3 of the New Regulations, any moveable corporeal or incorporeal asset may be the subject of a collateral, be they current or future, including:

- accounts receivable (unless part of a property ownership transfer transaction);
- deposit and current accounts;
- written deeds and documents that can transfer ownership by delivery or endorsement and that establish the maturity of an amount or the ownership of goods;
- equipment and work tools;
- material and moral elements of a business concern;
- goods intended for sale or lease, raw materials and goods in the process of manufacturing or transformation;
- agricultural crops, animals and their products;
- fixtures to real property; and
- other moveable assets which other laws deem to be suitable subjects of collateral.

Article 4 of the New Regulations confirms that the following assets are not regulated:

- moveable assets over which security interests are entered in a special registry;

- expenses, wages, salaries and workers' compensation; and
- public funds, endowment funds and funds of foreign diplomatic and consular entities and intergovernmental organisations.

#### **(5) Creation and Perfection of Security**

To successfully create a security interest, Article 8 of the New Regulations prescribes the following conditions:

- a contract between the guarantor and obligee to create the security interest be concluded;
- the guarantor has the capacity to dispose of the collateral and is authorised to create the security interest;
- the contract contains an adequate description of the collateral;
- the contract contains a description of the obligation secured by the security interest; and
- the obligee has paid the consideration agreed upon in the contract.

#### **(6) Third Party Enforcement**

Only once the security Interest is registered in the Registry will it become effective against third parties.

Once registered, the secured party obtains priority over the collateral; priority is determined by the date and time at which the security interest enters the Register. The priority must cover all secured obligations, including the obligations that arise after the security interest becomes enforceable against third parties. The fact that a lender is aware of a competing security interest will not affect the priority of the security interest registered first and therefore, time is of the essence when it comes to a lender's registration of their security.

A secured party may assign their priority status in writing provided that the assignment is within the limits of their secured rights and it does not affect the rights of any other obligee. An assignment should be registered as an amendment to the publicity.

The enforceability of a security interest against third parties will ensure the secured party's right to pursue the collateral and claim their rights from any person to whom the collateral is assigned.

### **(7) Effect of bankruptcy**

Being a change from Federal Law No. 20/2016, security interests which are enforceable against third parties at the commencement of bankruptcy proceedings against the guarantor will now survive the commencement of bankruptcy proceedings and the obligee will retain their position of priority held prior to the proceedings.

### **(8) Satisfaction**

Should the security interest of the guarantor expire as a result of the full execution of the secured obligation, or for any other reason, the obligee must cancel the publicity within five working days from the date thereof. If the obligee fails to cancel the publicity within this time period, it will be liable for compensating the guarantor for any actual damage sustained as a result.

The secured party will be responsible for paying the fees and expenses relating to the registration of the security interest in the Register unless otherwise agreed.

## **2 What You Need to Know About the New UAE Federal Decree on Bounced Cheques**

- 1. Changes to legislation affects the prosecution of issuers of bounced cheques.*
- 2. This addresses the use of cheques as payment instruments in a positive manner.*
- 3. This enhances the use of cheques as security for obligations.*

The UAE cabinet has amended certain provisions of Federal Law No. 18/1993, the Commercial Transactions Law related to bounced cheques, in a Decree expected to come into force in 2022. The Decree further enhances the force of cheques as a payment instrument. and how it will help overcome challenges with commercial dealings and with securing payments.

### **(1) What are the criminal offences of a bounced cheque?**

The amended provisions outline the offences that constitute a criminal penalty in the case of cheques:

1. Cheque falsification;
2. Forgery of cheques;
3. Fraudulent use of cheques by ordering the Bank not to pay the cheque amount; and
4. Withdrawing the account balance prior the date of the cheque to prevent encashment.

In an effort to improve collection of payments through cheques, banks are now obliged to make partial payment of the cheque amount to the beneficiaries when a cheque is presented for payment and an account balance is available to partly (but not fully) satisfy the beneficiary's claim.

The amendments aim to ease enforcement options. A bounced cheque is now viewed as an executive document that could be enforced and executed directly by a judge in the UAE court. As a result, the Civil court can demand the issuer of a bounced cheque to pay a sum equal to the value of the cheque or its outstanding balance. If the convicted person fails to pay, his assets may be subject to enforcement to satisfy the balance and the convicted person must serve a jail term for failing to comply with the civil court decision.

### **(2) How are joint bank account holders affected by bounced cheques?**

In the case of death or legal incapacity of one of the joint account holders, the remaining holder shall notify the bank no later than 10 days from the date of death or incapacity. The bank shall immediately suspend withdrawal from the joint

account up to the limits of the share of the demised or legally incapacitated person in the account balance as of the date of death or designation of a successor.

### **3 Ras al Khaimah Courts Launch Digital Signature Service**

***The Ras al Khaimah Courts have launched a service for digital signatures in its judicial systems using the digital signature of the UAE Pass digital ID.***

The service enables judges to sign the judgments issued by them on judicial applications by enabling another feature to sign them digitally in addition to the electronic signature which has been in use for years.

Judges can now sign the decisions using protection and identification technologies available through the digital signature system.

### **4 Dubai: First Bitcoin Fund to be Launched**

***NASDAQ Dubai has announced it is going to launch the region's first Bitcoin Fund.***

The listing should happen by June 2021.

It will be run by 3iQ Digital Asset Management. They have received final approval from the Dubai Financial Services Authority.

It follows a listing on the Toronto Stock Exchange last year which was billed as the world's first regulated, major exchange listed Bitcoin fund.

The Fund will buy and hold Bitcoin but will not deploy in other crypto asset classes.

### **5 UAE Central Bank establishes a new data protection regime for financial Institutions**

***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.***

## **(1) Background**

In accordance with its objectives set out in Article 121 of Federal Decree-Law No. 14/2018 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 Regulations (GDPR).

## **(2) 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.

## **(3) 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.

#### **(4) Deadline for compliance**

LFIs have until 31 December 2021 to update their practices to comply with the CPR.

#### **(5) 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.

#### **(6) 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.

#### **(7) The new Consumer Data Protection requirements**

##### **CPR**

The CPR introduces a key data protection principle which bring 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.

#### **(8) 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.
- **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 of 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.

### **(9) 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.

### **(10) Express Consent**

The CPS defines “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.

### **(11) 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.

### **(12) Consumer Data Protection Rights**

The CPS provides 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.

### **(13) 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.

#### (14)Data Localisation

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.

#### (15)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.

#### (16)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:

Principle	Key requirements
Disclosure and transparency	proactively provide all information necessary to the consumer.
Institutional oversight	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.
Market conduct	observing ethical, non-abusive practices
Complaint management and resolution	put in place a fair, accessible, transparent and free process to address any complaints from consumers which must be resolved in a timely manner.
Financial inclusion including gender and race equality	consider the requirements of vulnerable groups and people of determination for their products and service designs.

#### (17)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 (Federal Decree-Law No. 14/2018 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.

### **(18)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:

putting in place the groundwork for a data protection department and a Data Management and Protection role; reviewing their data protection and privacy policies and processes; and

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.

## **6 UAE Signs Healthcare Services with Israel**

The Emirates Health Services Establishment has signed a cooperation agreement with Israel's Health Ministry to improve the quality of healthcare in the two countries.

It is aimed at protecting health data for patients better and facilitating the exchange of research between the two countries.

The two countries will cooperate on fighting global pandemics, protecting medical data, cyber security, medical education, innovation and using Artificial Intelligence and other advanced technologies.

They will also work to facilitate mutual visits by experts and set up major economic and health projects as well as strengthen cooperation between medical institutions in both jurisdictions.

It was signed for the Establishment by its Director General, Dr Yousif Al Serkal and for Israel by its Health Minister, Yuli Edelstein.

*The contents of this newsletter are based on information collated from various legal sources and are not necessarily a reflection of the views of the Firm, its clients, or any of its or their respective affiliates. These articles are for general information purposes and are not intended to be and should not be taken as legal advice.*