Consultation Paper

AFSA № AFSA-F-CE-2021-0003

Regulation of digital banking services

Unrestricted

July 2021

PART A - INTRODUCTION

1. SCOPE AND PURPOSE

1.1 This paper presents a proposed policy to be adopted by the Astana Financial Services Authority (the "**AFSA**") for the regulation of digital banking services in the Astana International Financial Services Centre (the "**AIFC**") (the "**Framework**").

1.2 Terms not defined herein have the meaning given to them in the AIFC Glossary.

1.3 The proposed Framework will aid the economic and social development of Kazakhstan by diversifying who provides banking services, what those banking services are and how Clients[1] use these services.

1.4 This will support the five-year programme for 'Digital Kazakhstan', which is seeking to improve the competitiveness of Kazakhstan's economy and quality of life through the progressive development of the digital ecosystem. This programme also includes the development of financial technologies, non-cash payments and electronic commerce, as well as progressive regulations that create a vibrant environment to promote greater inclusion and innovation. The AFSA is being supported by and working with the European Bank of Reconstruction and Development (the "**EBRD**") in implementing aspects of the 'Digital Kazakhstan' programme within the AIFC. The AFSA and the EBRD are engaging consultants, such as Clifford Chance in this case, to assist it with this programme. The proposed Framework is a part of this programme.

1.5 The aim of the proposed Framework is to enhance and build on the existing regulatory framework in order to support the licensing of digital-only banks and to regulate banking services provided remotely (e.g. online; in a mobile app), in support of the introduction of "Open Banking".

1.6 The proposed Framework will provide regulatory certainty to Authorised Firms providing banking services, and to their Clients. It will also promote new and innovative ways for banking services to be provided in the AIFC.

2. BACKGROUND

2.1 Digital banking is transforming how banking services are provided around the world. It is expanding the ways that banking services can be offered, which is opening it up to clients that were previously under-served. This means that traditional banking products, such as accepting deposits and providing credit, do not need to be offered through physical branches, but can be provided remotely; for example, online or in a mobile app. Clients can therefore access more banking services in any location.

2.2 In addition, the concept of 'Open Banking' has gained traction over the past few years. This allows a client's banking data to be used not only by his or her own bank, but also by third party providers in order to enable the provision of new products and services which will benefit clients. It establishes a secure way for a wide variety of providers to access a client's banking information and receive improved financial services and other related services.

2.3 Over the past few years, an increasing number of jurisdictions have been putting in place the regulatory infrastructure to enable remote access through digital banking, and to develop 'Open

---

[1] As per the AFSA Glossary, "Clients" is a broad term including individuals, corporate and government bodies, which can be located within Kazakhstan or externally.

Banking'. Against this background, the AIFC is seeking to put in place the proposed Framework so that Kazakhstan can benefit from these developments and become an attractive location for both local and international providers of such services.

PART B – REGULATORY APPROACH

3. OVERVIEW AND SCOPE OF ACTIVITIES

3.1 The proposed Framework is being developed by the AFSA as part of its plan to enhance regulatory policies aimed at facilitating the adoption of technological innovations in the AIFC.

3.2 In formulating the proposed Framework, it has been proposed to:

3.2.1 develop a standalone regulatory framework for digital-only banks (please see Sections 5 to 8 below with respect to "Authorised Digital Banks" and "Authorised Digital Banks (Limited Licence)");

3.2.2 offer a phased approach to full authorisation for digital-only banks to encourage new providers into the AIFC (i.e., to lower the barriers to entry into the banking market) (please see Section 8 below with respect to "Authorised Digital Banks (Limited Licence)");

3.2.3 consider ways to access online banking;

3.2.4 define new Regulated Services to permit 'Open Banking' activities;

3.2.5 consider what additional infrastructure may need to be developed so that 'Open Banking' can operate fully; and

3.2.6 put in place suitable safeguards that recognise and address the security and other challenges posed by digital banking.

3.3 Following various policy discussions, it has been decided to include provisions related to "Open Banking" in the separate Payment Services and Electronic Money Framework ("PSEM Framework").

4. LEGISLATION

4.1 When developing the proposed digital banking framework, the starting point will be to review the existing AIFC Acts which apply to Banks generally. When conducting this review, the question in each case will be: should this rule apply to an Authorised Digital Bank and, if so, does the rule need to be modified in any way in respect of its application to Authorised Digital Banks. The acts to be reviewed are:

4.1.1 AIFC Financial Services Framework Regulations ("**FSFR**");

4.1.2 AIFC General Rules ("**GEN**");

4.1.3 AIFC Conduct of Business ("**COB**");

4.1.4 AIFC Banking Business Prudential Rules ("**BBR**");

4.1.5 AIFC Market Rules ("**MAR**");

4.1.6 AIFC Anti-Money Laundering, Counter – Terrorist Financing and Sanctions Rules ("**AML**");

4.1.7 AIFC Fees Rules ("**FEES**"); and

4.1.8 AIFC Glossary.

4.2 New rules for digital-only banks will also be drafted - the new AIFC Digital Bank Rules ("**DBR**").

PART C – SUMMARY OF POLICY POSITIONS

5. DIGITAL-ONLY BANKS - SCOPE

5.1 Traditionally, banks have physical infrastructure through which they provide banking services to clients. For example, retail banks operate networks of branches where clients receive key banking services (e.g. open bank accounts) and they provide ATMs where clients can withdraw cash from their bank accounts (either through their own ATM network or through an agent bank's ATM network).

5.2 The AIFC wants to establish a regulatory framework for digital-only banks. The aim of this is to enable Clients to receive banking services remotely, without the need for the physical infrastructure of traditional banks. In order to achieve this, there would need to be sufficient technological infrastructure (both at a network level and at a corporate/individual level) and technological literacy. Enabling Clients to receive banking services remotely would benefit them, as they would have immediate access to banking services wherever they are. Digital-only banks would also benefit from reduced operating costs.

5.3 Digital-only banks will need to be defined to distinguish them from traditional banks. We propose that the core concept of the definition is a bank which provides only digital banking services, and which has only limited physical infrastructure. For example, it could have a head office but no branch network. Digital kiosks and ATMs will be permitted in order to help attract Clients and assist with Client on-boarding and Client queries (such kiosks could be manned or unmanned).

5.4 Applicants would have their own application process (see Section 6 below) to become "**Authorised Digital Banks**", and their own rules, the DBR (see Section 7 below). Please also see Section 8 below where it is proposed that there is an intermediate step for "**Authorised Digital Banks (Limited Licence)**", where more limited rules would apply.

5.5 Authorised Digital Banks will come within the definition of Authorised Firms, as will Authorised Digital Banks (Limited Licence). We understand that under the Payment Services and Electronic Money ("**PSEM**") Policy Paper, certain Authorised Firms do not need separate authorisation to carry out the new payment services Regulated Activity; such Authorised Firms include those with permission to Accept Deposits, Provide Credit and Provide Money Services. Authorised Digital Banks with these permissions will not therefore require separate authorisation to provide payment services as a Regulated Activity.

5.6 There is then also a policy question around whether Authorised Digital Banks should be permitted to carry out the new Regulated Activity under the PSEM Framework of issuing electronic money. Our view is that Authorised Digital Banks should be permitted to do so on the basis that this would be consistent with the banking and payment services activities that Authorised Digital Banks are proposed to be able to carry out and supportive of the general objectives for the DBRs, of expanding the use of financial technology and non-cash payments within the AIFC.

5.7 Authorised Digital Banks would be limited to providing certain existing Regulated Activities set out in Schedule 1 (Regulated Activities) to the AIFC General Rules ("**GEN**")[2]. They would be allowed to carry out the following Regulated Activities:

5.7.1 17. Accepting Deposits;

5.7.2 18. Providing Credit; and

5.7.3 26. Opening and Operating Bank Accounts.

They may then also carry out one or more of the following Regulated Activities:

5.7.4 19. Advising on a Credit Facility; and/or

5.7.5 21. Providing Money Services.

5.8 In addition, Authorised Digital Banks will be permitted to carry out the new Payment Services Regulated Activity, proposed as part of the PSEM Framework, including those activities introduced for "Open Banking". Further review will be required of the PSEM Framework, once drafted, to ensure that the DBRs and the PSEM Framework are consistent. Given the broad definition of Client in the AIFC Glossary, Authorised Digital Banks could not only provide these Regulated Activities and other non-regulated activities to corporates etc., but also to other banks or financial institutions. Authorised Digital Banks will also be able to accept limited deposits of up to USD 10,000 from Retail Clients, unlike other Banks in the AIFC.

5.9 Another issue is as to whether there should be any limit on an Authorised Digital Bank when providing credit to Retail Clients. Policy options for AFSA here include:

5.9.1 allowing Authorised Digital Banks to provide unlimited credit to Retail Clients in the same way that an existing AFSA-authorised Bank would be permitted to;

5.9.2 allowing Authorised Digital Banks to provide microloans of up to USD 10,000 only per Retail Client;

5.9.3 allowing Authorised Digital Banks to provide microloans of up to USD 10,000 per Retail Client but permitting uncapped loans to Retail Clients where either:

(a) the funds for loans over the USD 10,000 cap are not derived from client deposits; or

(b) reasonable and proportionate security for the loan is taken by the Authorised Digital Bank.

5.10 In our view, there are pros and cons for each of these approaches, based on considerations including consumer protection, ease of implementation and enforcement and ensuring that Authorised Digital Banks are able to grow stable and sustainable businesses. Whilst capping the amount that can be loaned to each Retail Client may be an appropriate way of protecting consumers, allowing Authorised Digital Banks some flexibility to provide further credit to such customers, especially with additional protections, also seems worthwhile in order to support sustainable business growth.

---

[2] We note that some of these activities, in particular providing Money Services and Opening and Operating Bank Accounts, may be amended as part of the introduction of the PSEM Framework and this will be taken into account as part of the drafting process, to ensure the PSEM Framework and DBRs are consistent.

5.11 The application process for becoming an Authorised Digital Bank will allow for an Authorised Firm that is not an Authorised Digital Bank to set up a subsidiary which is an Authorised Digital Bank, or itself become an Authorised Digital Bank, subject to meeting relevant criteria. The AFSA shall have discretion to accelerate the Authorised Digital Bank (Limited Licence) phase for an existing AFSA-authorised Bank wishing to become an Authorised Digital Bank or to establish a subsidiary which is an Authorised Digital Bank.

6. DIGITAL-ONLY BANKS – APPLICATIONS

6.1 Applicants to become Authorised Digital Banks will have their own set of application forms. This will include choosing which of the Regulated Activities that are available to Authorised Digital Banks the applicant wishes to provide (see Section 5.5 above).

7. DIGITAL-ONLY BANKS - RULES

7.1 The AFSA wishes to make its regime attractive to digital-only banks. Part of its appeal will be to reduce unnecessary burdens in the application process. A key part of the work that an applicant will do is to assess the rules that will apply to it.

7.2 The AFSA will need some new rules for Authorised Digital Banks. These will be set out the DBR. In particular, the DBR will set out what defines an Authorised Digital Bank, the application process and any requirements specific to Authorised Digital Banks. The DBR will also do this for Authorised Digital Banks (Limited Licence) (see Section 8 below). As noted in Section 11, there are certain security and consumer protection provisions which should be put in place where banking and other services are provided remotely. As these will also be relevant to other Authorised Firms who provide such services remotely, these will not be included in the DBRs but may be issued as separate guidelines by the AIFC or be included in another AIFC Rulebook (e.g. in the AIFC General Rules or the rules to be drafted for the new PSEM Framework).

7.3 In addition, some existing AIFC Acts applicable to other types of firms will also apply to Authorised Digital Banks. Current rules which may need to apply to Authorised Digital Banks are contained in the following AIFC Acts:

7.3.1 AIFC Financial Services Framework Regulations ("**FSFR**");

7.3.2 AIFC General Rules ("**GEN**");

7.3.3 AIFC Conduct of Business ("**COB**")[3];

7.3.4 AIFC Banking Business Prudential Rules ("**BBR**");

7.3.5 AIFC Market Rules ("**MAR**")[4];

7.3.6 AIFC Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Rules ("**AML**");

7.3.7 AIFC Fees Rules ("**FEES**"); and

---

[3] Namely COB 2 (Client Classification), COB 3 (Communication with Clients and Financial Promotions), COB 4 (Key Information and Client Agreement), COB 7 (Conflicts of Interest), COB 15 (Complaints Handling and Dispute Resolution), COB 16 (Record Keeping and Internal Audit), COB 18 (Banks), Schedule 2 (Key Information and Content of Client Agreement) and Schedule 5 (Financial Promotions).

[4] Namely MAR 2 (Governance of Reporting Entities), MAR 3 (Financial Reports), MAR 5 (Market Abuse), MAR 6 (Market Disclosure) and Schedule 3 (Corporate Governance Best Practice Standards).

7.3.8 AIFC Glossary.

New rules are also currently being developed under the PSEM Framework, some of which (such as conduct of business rules) will also apply to Authorised Digital Banks when carrying out payment services; these rules will need to be considered when drafting the DBRs.

7.4 Whilst it would be simpler for Authorised Digital Banks to have all their rules in one place (e.g. no need to follow cross-references to other parts of the AIFC Acts), it would create a lengthy rulebook. In addition, care would need to be taken that any future updates are reflected, where relevant, in both the existing AIFC Acts and in the DBR. Instead, the DBR will set out only specific new rules applicable to Authorised Digital Banks or, existing rules which need to be modified when they apply to Authorised Digital Banks. It will also cross reference however to other existing rules in existing AIFC Acts which will apply to Authorised Digital Banks, to help make the DBR easier to follow, without setting out these existing rules in full.

7.5 The BBR sets out detailed requirements for Banks, including principles relating to Banking Business, prudential reporting requirements, capital adequacy, credit risk and concentration risk, market risk, operational risk, interest rate risk in the Banking Book, liquidity risk, group risk, supervisory review and evaluation process and public disclosure requirements. It is understood that these will also apply in full to Authorised Digital Banks (but not for an Authorised Digital Banks (Limited Licence) as discussed in Section 8 below).

7.6 Authorised Digital Banks will also require corporate governance rules. Currently, corporate governance rules for listed entities are set out in MAR and apply to a Reporting Entity, which is a Person who: (i) has Securities or Units admitted to an Official List; (ii) is the Fund Manager of a Listed Fund; or (iii) is declared by the AFSA to be a Reporting Entity. To the extent that an Authorised Digital Bank is a Reporting Entity, they will be subject to these rules, in the same way as other Banks under AFSA's current approach.

8. DIGITAL-ONLY BANKS – AUTHORISED DIGITAL BANK (LIMITED LICENCE)

8.1 In order to encourage new entrants to the banking sector, there will be an intermediary stage between applying for and becoming a full Authorised Digital Bank. This will allow applicants to provide limited Regulated Activities and to not be subject to the full set of rules for an Authorised Digital Bank. They are intended to be known as Authorised Digital Banks (Limited Licence). This is similar to the approach taken in Singapore and is designed to lower the barriers to entry to new entrants to the banking sector.

8.2 All applicants to become an Authorised Digital Bank must first become an Authorised Digital Bank (Limited Licence), until the AFSA have carried out an evaluation to check that the Authorised Digital Bank (Limited Licence) has satisfied certain conditions and can become an Authorised Digital Bank. The Authorised Digital Bank (Limited Licence) phase will be time limited period and an Authorised Digital Bank (Limited Licence) will be required to cease doing business in the AIFC if they fail to satisfy the AFSA's evaluation to become an Authorised Digital Bank within the required time period.

8.3 Limitations on an Authorised Digital Bank (Limited Licence) being considered include:

8.3.1 when providing the Regulated Activities of Accepting Deposits and Providing Credit:

(a) no Deposits will be accepted from Retail Clients; and/or

(b) a cap on the Credit provided to each Retail Client of USD 10,000.;

8.3.2 The BBR will apply in a reduced manner, such as lower capital requirements (e.g. USD 5 million[5]);

8.3.3 restrictions on holding safeguarded funds for Payment Institutions and Small Payment Institutions pursuant to any requirements under the PSEM Framework for safeguarded sums to be held with an authorised Bank.

Further rules could also not be applied or be applied in a reduced manner if that is required.

8.4 An Authorised Digital Banks (Limited Licence) will come within the definition of Authorised Firms and so be required to comply with other AIFC Acts applicable to Authorised Firms, subject to modifications set out in the DBR.

8.5 We understand that under the PSEM Policy Paper, certain Authorised Firms do not need separate authorisation under the PSEM Regime, providing they have permission to carry out Regulated Activities such as Accepting Deposits. If an Authorised Digital Bank (Limited Licence) is an Authorised Firm with such permissions, this would ensure that they do not require separate authorisation when acting as payment service providers.

9. ACCESS TO ONLINE BANKING

9.1 Clients want increased flexibility in how they access banking services. This means that they do not want to have to visit a physical branch to receive banking services. Clients want to be able to transfer funds, view their account balance and undertake other account activities wherever they are. In the AIFC, clients will want this regardless of whether they receive remote banking services from an existing Authorised Firm such as a Bank or, in the future, from an Authorised Digital Bank or Authorised Digital Bank (Limited Licence) (i.e. standards and processes around remote access to Regulated Activities should apply to all Authorised Firms).

9.2 It is important that the Framework is suitably robust and technologically neutral in order for its rules and requirements to apply wherever relevant Regulated Activities are accessed remotely, regardless of what interface is used (e.g., web-page; mobile app; tablet; watch). In the past, some jurisdictions developed a standalone licensing regime for mobile banking. However, leading jurisdictions now rarely have a licensing regime exclusively for mobile banking. This is because they require a technologically neutral licensing regime which is flexible enough to permit banking services to be provided through a variety of interfaces and which therefore does not need to be constantly revised to take account of technological changes. Standards and processes around access and conduct of business are therefore required to ensure that any remote access to banking services is secure and safe for Clients.

9.3 In order to facilitate this, it is likely that certain security standards will need to be implemented in the AIFC in order to allow Clients to access banking services securely. Whilst certain specific security standards should be implemented as rules as discussed in Section 11 below (e.g. SCA (as defined in Section 11)), the AIFC may also wish to develop security guidelines as, for example, the European Banking Authority ("**EBA**") has done in the EU.[6]

---

[5] Under Rule 4.10(a) BBR, the Base Capital Requirement of a Bank is USD 10 million. USD 5 million therefore seems a reasonable Base Capital Requirement for an Authorised Digital Bank (Limited Licence)

[6] https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf

10. OPEN BANKING – API AND OTHER STANDARDS

10.1 In order to be able to provide Account Information Services and/or Payment Initiation Services, Authorised Firms, such as Banks, will need to open up their application programming interfaces ("**APIs**") to share information securely with Authorised Firms providing Account Information Services and/or Payment Initiation Services.

10.2 APIs are codes and protocols which allow different applications to communicate with each other by deciding how different software components should interact. Open data API specifications are available publicly. These allow API providers, such as Banks, to develop API "endpoints" which can be accessed by Authorised Firms providing Account Information Services and/or Payment Initiation Services through building compatible online applications. Open data API specifications are crucial to ensuring the technological neutrality of the Framework, and to allowing the broadest pool of firms to provide Account Information Services and/or Payment Initiation Services.

10.3 The AFSA will need to decide how it wishes to control APIs. For example, in the UK, Open Banking Limited has set out certain API specifications which must be adhered to.[7] This helps ensure the widest possible access through the use of common standards. However, this is less about financial regulation and more about the technical standards and associated boundaries which the AFSA wishes to put in place to foster innovation and encourage new and existing Authorised Firms to provide Account Information Services and/or Payment Initiation Services.

10.4 Furthermore, using the example of the UK's Open Banking Limited, the AFSA may wish to put in place additional guidelines around security, customer experience and operations.[8] However, this is again less about financial regulation and more about the technical standards and associated boundaries which the AFSA may wish to put in place. As these requirements will apply more broadly than just to Authorised Digital Banks, AFSA's powers to issue such guidelines will be set out, if necessary, elsewhere in the AIFC Rules.

11. SECURITY AND CONSUMER PROTECTION

11.1 Where any banking services take place remotely, there are inherent security risks. This is an issue for all Authorised Firms (including Authorised Digital Banks and Authorised Digital Banks (Limited Licence), regardless of whether they come within the definition of Authorised Firms). However, the Framework offers an opportunity to put in place requirements that will increase security and reduce fraud for all Clients.

11.2 One solution to this is to put in place security standards and processes which must be complied with if Clients:

11.2.1 access Bank Accounts online;

11.2.2 initiate an electronic payment transaction; or

11.2.3 carry out any other action through a remote channel which may imply a risk of payment fraud.

This would therefore affect not just the new Regulated Activities of Account Information Services and Payment Initiation Services, but also existing Regulated Activities where these take place remotely (e.g. online or in a mobile app).

---

7 https://standards.openbanking.org.uk/api-specifications/

8 https://standards.openbanking.org.uk/

11.3 AFSA intends to follow the EU's approach, which is to require Authorised Firms to apply strong customer authentication ("**SCA**") where a client wishes to take any of the actions in Sections 11.2.1, 11.2.2 or 11.2.3. SCA would also apply to providers of Account Information Services and/or Payment Initiation Services. SCA requires authentication based on two or more independent elements from the following:

11.3.1 'Knowledge Factor' – something only the Client knows (e.g. password);

11.3.2 'Possession Factor' – something held only by the Client (e.g. card verification number); and/or

11.3.3 'Inherence Factor' – something inherent to the Client (e.g. biometric fingerprint, facial recognition or voice recognition).

Given the importance of business-to-business services, the AFSA may wish to introduce specific exemptions for corporate Clients which either disapply SCA for them, or permit them to implement their own equivalent security processes (with equivalence to be determined by the AFSA).

11.4 Where any banking services are accessed online, there are also other factors which will be considered as part of the DBR drafting process, although these will also be applicable to other Authorised Firms carrying out business remotely. By way of example, please see the summary below.

11.4.1 Client on-boarding – If a Client is on-boarded remotely (e.g. by an Authorised Digital Bank), which documents it would need to provide and how (e.g. PDF copies of invoices as proof of address, passports etc.). Careful consideration needs to be given to Client due diligence that is done remotely. We understand that this will sit within the AIFC's (and/or Kazakhstan's) existing AML/CFT framework. Generally, jurisdictions do not have specific rules for remote Client due diligence. However, there may be some benefit in including some express requirements (e.g. a "selfie" video) where Client due diligence is done remotely.

11.4.2 Cybersecurity – If Authorised Firms provide Regulated Activities online, what security measures they should put in place for their websites, mobile apps and other interfaces to prevent them succumbing to cyber-attacks and to Client data being stolen.

11.4.3 Business recovery – As Clients will be relying upon a remote interface (e.g. online platform or mobile app), what back-up measures Authorised Firms must put in place in order to ensure continuity of service (e.g. servers in an alternative location; multiple data stores).

11.4.4 Outsourcing – To what extent Authorised Firms will be permitted to outsource operational functions, and to the extent that they do, how the AFSA monitors that (e.g. requests to see draft contracts) and the continuing liability of Authorised Firms for outsourced functions. The AFSA may wish to develop guidelines around such outsourcing and what standards need to be adhered to.[9] Whilst we understand that drafting such guidelines are outside the

[9] For example, the EBA and the UK FCA have drafted guidelines to complement their regulatory regimes. https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

scope of this project, these could be developed by the AFSA to complement the Framework.

11.4.5 Client terms – If Client terms must contain any specific provisions (e.g. treatment of alleged unauthorised transactions; liability for unauthorised transactions; fees) and whether they would differ between Retail Clients and other Clients. However, this is not specific to banking services taking place remotely.

11.4.6 Authorised status – Where and how Authorised Firms should set out their authorised status online.

11.4.7 Consumer protection – Whether Authorised Firms are required to apply any particular security features to Retail Clients or, if security features apply to all Clients, can non-Retail Clients consent to disapply them. Also, whether a higher degree of liability should apply to Authorised Firms when they deal with Retail Clients. These are issues which go beyond just the Framework.

11.4.8 Data protection – Where Authorised Firms provide Regulated Activities on a remote basis, data protection will clearly be important in a number of ways. For example, access to Clients' records, the sending and receiving of messages/instructions and how Authorised Firms use, store, access, move and ultimately dispose of Client data. The Client should be able to access its own data and move it elsewhere, including cross-border, if it so wishes. We understand that data protection will sit within the AIFC's existing data protection framework.

11.5 The AFSA would need to consider whether to take a prescriptive approach in such areas, or to set out certain areas where Authorised Firms need to provide policies and procedures to address these which satisfy the AFSA. By way of example, the EU has adopted a very prescriptive approach, as demonstrated in the EBA's 'Guidelines on the security measures for operational and security risks of payment services under PSD2'.