Directive for Account Information Service Provider (AISP) License Applicants and License Holders

Directive under Sections 4, 5, 27(c)(1), 35, 36, and 63(b) of the Account Information Service Law 5782-2021

EXPLANATORY NOTE

The Account Information Services Law 5782-2021 ("the Law"), which was enacted in November 2021, authorizes the Israel Securities Authority ("ISA") to issue account information service provider (AISP) licenses to corporations that meet the requirements stated in the Law, and to supervise said license holders in accordance with the principles stated in the Law. The Law regulates the field of open banking in Israel for the first time.

The Law concerns the provision of account information services. An account information service, which is an online service, is one in which an AISP license holder ("license holder" or "AISP license holder") collects account information about a customer that is held by financial entities from which the customer receives financial services ("information sources"), and provides a service on the basis of that information. Account information is collected through the license holder's access to an online system, through which information sources are obligated to grant access to account information ("the account information interface system").

Account information is information about a customer's financial activities that are administered by information sources, such as transactions (credits and debits) in the customer's current account and the cost of account management (account fees); information about the customer's credit including the total credit that the customer assumed and the interest on it; information about the customer's savings including the customer's total savings and the interest the customer is paid; information on the customer's securities portfolio and the fees the customer pays for buying and selling securities, and so on.

An AISP license holder may offer various account information services, such as consolidation of the customer's account information from multiple information sources, cost comparisons, transfer of information to financial entities in order to obtain offers of financial services that the customer uses or wishes to use (i.e., offers from competing financial entities) or for the purpose of assisting the customer in contracting with these entities. An AISP license holder may also provide advice to improve the customer's economic practices. We stress that this is not an exhaustive list of the uses that a license holder may make of a customer's account information; the only conditions are that a license holder's use of a customer's account information is related to the customer's economic practices, is beneficial for the customer, and is subject to the customer's explicit consent.

Another supplementary service that is offered in open banking is payment initiation services. To provide a payment initiation service, the license holder writes the details of a payment order in the customer's account, at the customer's request; Before the license holder executes the order, the customer is required to approve the payment order online vis a vis the customer's payment account administrator (for example, the license holder writes a payment order in the customer's bank account, and the customer then approves the payment order online to their bank). Payment initiation services are designed to simplify the payment process for the customer: The payment order is written for the customer, and the online procedure

prevents errors that might occur when the customer enters the details of the payment order independently. Payment initiation services may use the same interface system used for account information and in that respect, payment initiation services supplement account information services. As described below in the Directive, a license holder may offer payment initiation services provided that it meets the conditions of this Directive, the Rules for Submitting an AISP License Application, and the Standard.

The Aim of the Directive

The Law authorizes the ISA to make rules for account information services rendered by AISP license holders on various matters that are regulated by the Law, in order to ensure that license holders comply with the requirements of the Law and that their operations are efficiently supervised. The ISA was specifically authorized to make rules for license holders with respect to information security and protection of customers' privacy, which are at the core of the Law that pertains to services provided on the basis of customers' sensitive information. The Directive also defines requirements related to information security, risk management, and cyber defense, which are part of the conditions of the license that a license holder must meet. The Directive also defines insurance requirements and the required deposit, which are also part of the conditions of the license. Finally, the Directive defines the reports that a license holder must submit to the ISA, in order to facilitate supervision of the license holder's operations and its compliance with the requirements of the Law. Notably, rules concerning the submission of a license application and the details and documents that an applicant must attach to the application were published in Reshumot.[1]

[1] https://rfa.justice.gov.il/SearchPredefinedApi/Documents/qa0DjAH11hv4cTvqv8pm3yOgb8hweiVZJG+DJaJ6aBI=

CHAPTER A: GENERAL

1. In this Directive:

"Reporting site" – the ISA website on which reports are electronically submitted to the ISA, as defined in Securities Regulations (Electronic Signature and Reporting) 5763-2003;

"Open banking" – as this term is defined in Proper Conduct of Banking Business Directive No. 368;

"Payment order," "payment account," "Payor," "Payment service" – as these terms are defined in the Payment Services Law 5779-2019;

"Business day" – a day on which the majority of banking corporations in Israel are open for executing transactions with the public;

"Rules for Submitting an AISP License Application" – Rules for Submitting an Application for an Account Information Service Provider (AISP) License 5782-2022, published in Reshumot on May 26, 2022;

"Applicant" – a corporation that applies for an AISP license;

"CPI" – the Consumer Price Index published by the Central Bureau of Statistics;

"Sensitive information" – account information and any information subject to a duty of confidentiality under the Law;

"Payment Account Administrator" – as this term is defined in Proper Conduct of Banking Business Directive No. 368;

"Account Information Interface System" – as this term is defined in the Law; and with respect to payment initiation services — a secure, online technological interface that enables access to a payment account for the purpose of performing a payment initiation service according to Proper Conduct of Banking Business Directive No. 368;

"Information Source" – as this term is defined in the Law; and with respect to payment initiation services — a payment account administrator;

"Proper Conduct of Banking Business Directive No. 368" - Proper Conduct of Banking Business Directive No. 368 of the Bank of Israel concerning implementation of an open banking standard in Israel;

"Type of service" – One or more of the following: (1) the collection of account information and its transfer to another party; (2) the collection of account information and its use online by the party that collected the information; (3) the online use of account information collected by another party and transferred to the user, as described in paragraph (1);

"the Standard" – Regulatory Technical Standard (RTS), which is the open banking standard in Israel, described in Appendix A of Proper Conduct of Banking Business Directive No. 368, as revised, including inter alia, architecture, information security and cyber defense, definition of business procedures, information sources procedures to authenticate license holders, the process of obtaining a customer's consent and revocation of consent, rules related to service quality, definition of the services and the formats of the requests and responses for each type of service, version management method, and the services to be offered by information sources in the development environment;

"Open Banking Digital Certificate" – a digital certificate issued to a license holder by the e-Government Unit approved by the ISA, required for a license holder's open banking operations vis a vis information sources;

"Online channel" – URL of a website or an app;

"Developers' Portal" – as this term is defined in Proper Conduct of Banking Business Directive o. 368;

"Database registrar" – as this term is defined in Section 7 of the Privacy Protection Law;

"Payment initiation service" – as this term is defined in Proper Conduct of Banking Business Directive o. 368;

"Transport layer" – a secure channel for online messaging between an information source and a license holder over the internet.

"Digital certificate" – an electronic certificate that creates an association between the certificate holder (TPP) and a pair of encryption keys (public and private) that are used to encrypt and sign electronic documents;

"The Privacy Protection Regulations" – The Privacy Protection Regulations (Information Security) 5777-2017.

CHAPTER B: SUBMITTING AN APPLICATION FOR AN AISP LICENSE

2. A corporation that applies for an AISP license will submit its application on the reporting site according to the Rules for Submitting an AISP License Application.

3. Where a decision on an Applicant's application for a license is pending, the Applicant may submit an application for an Open Banking Digital Certificate for the test environment.

4. The ISA will issue an Open Banking Digital Certificate for the test environment to an Applicant after the ISA examined the Applicant's compliance with the requirements of trustworthiness; payment of the license application fee, and performed a preliminary examination of the Applicant's technological means, as stated in Section 2(6) of the Rules for Submitting an AISP License Application.

5. The ISA will conduct said examination of the Applicant with reference to the application for a license in totality, and the risks entailed in the Applicant's operations in the information sources' test environment. With respect to the auditor's opinion attached to the license application, the ISA will, among other things, examine the auditor's assessment of the level of the Applicant's information security in the test environments.

6. Issue of an Open Banking Digital Certificate for the test environment does not constitute confirmation that the Applicant meets all the qualification conditions for a license. If an Applicant's license application is rejected, the Open Banking Digital Certificate for the test environment issued to the Applicant will be revoked.

7. An Applicant whose application for a license is approved by the ISA may apply for an Open Banking Digital Certificate, to be issued by the ISA, as stated in Chapter E.

7A. An Applicant that wishes to provide a payment initiation service to complement an account information service will submit an application for a payment initiation service certificate, providing information on the Applicant's compliance with the

requirements of this Directive and the Rules for Submitting an AISP License Application, with the necessary changes with respect to payment initiation services.

7B. An Applicant whose request to provide payment initiation services was approved by the ISA may submit an application for a certificate, to be issued by the ISA as described in Chapter E, provided that the Applicant follows the Standard and meets the requirements stated in this Directive, with the necessary changes with respect to payment initiation services.

CHAPTER C: INSURANCE COVERAGE OR DEPOSIT

8. The license holder must meet the requirement to obtain insurance or make a security deposit as described below:

   a. The license holder insured its liability toward its customers; the insurance coverage, scope, and terms will be at such level as the board of directors of the license holder deems sufficient to insure the license holder's liability for any negligible act or omission toward a customer, and will be no less than NIS 500,000. Insurance will be issued by an insurer licensed under the Supervision of Insurance Business Law 52741-1981.

      Insurance issued under this section will cover claims for events that occurred in the insurance period including claims filed within one year from the end of the insurance period.

      The license holder's board of directors will, annually or upon the occurrence of a material change, review and approve that the insurance coverage, its scope, and its terms meet the requirements stated this section.

   b. The license holder made a deposit in such amount that, according to the license holder's board of directors, is sufficient to insure the license holder's full liability for any negligible act or omission toward its customers, and no less than NIS 500,000. The deposit will be in the form of government bonds that are traded on the stock exchange and are not convertible into securities that confer a right of participation or membership in a corporation, or in the form of investment-grade bonds traded on the stock exchange ("the Deposit").

      The Deposit will remain in effect for one year from the termination of the license holder's operations under the license.

      The license holder's board of directors will examine and approve annually or upon the occurrence of a material change, that the Deposit meets the requirements of this section.

      The Deposit will be held in an escrow account with a bank or a stock exchange member in the name of an attorney or accountant who serves as the trustee of the Deposit ("the Trustee"). The Trustee will manage the Deposit on behalf of the license holder's customers ("the Trust Account"). The Trust Account may be pledged, withdrawn, or seized only by an order of the Trustee and if one of the following obtains:

         (1) A court ruling was issued in a customer's lawsuit against the license holder regarding the latter's liability, or a settlement or ruling on an arbitration between said parties was certified by the court; Such court

ruling, settlement, and arbitration ruling will also include details of the parties entitled to receive payment and the amounts to which they are entitled.

(2) The license holder is involved in an insolvency proceeding and the Deposit is required for the execution of a court ruling or court-certified arbitration ruling in a lawsuit based on the license holder's liability toward their customers: In this paragraph, "insolvency proceeding" is a liquidation or receivership proceeding according to the Companies Ordinance [New Version] 5743-1983, or proceedings under Section 350 of The Companies Law.

c. The license holder's board of directors will take the following considerations into account when determining the scope of the insurance or deposit:

(1) The license holder's risk profile – the number of monetary claims filed for the liability of the license holder in its capacity as an AISP, and the number of accounts from which the license holder collected account information;

(2) The license holders' operations – Does the license holder only provide an account information service or does it provide additional services such as payment initiation service, payment services or other non-financial services;

(3) The scope of the license holder's operations – the number of the license holder's customers.

d. The amounts according to Section 8(a) or 8(b) will be revised on January 1 of every year ("the Revision Date") according to the percentage change in the most recent CPI published before the Revision Date compared to the base CPI, rounded to the nearest amount that is a multiple of NIS 1,000; For this purpose "the base CPI" is the last CPI published before the previous Revision Date.

CHAPTER D: RETAINING ACCOUNT INFORMATION REQUIRED FOR A LEGAL PROCEEDING, AN INTERNAL AUDIT, OR STATUTORY SUPERVISION

9. A license holder may save account information that is required for a legal proceeding, an internal audit proceeding, or statutory supervision for a period of up to seven years from the termination of the service to a customer. Such information:

a. will be saved in a database that is separate from other databases;

b. The information will be used exclusively for a legal proceeding, an internal audit proceeding, or statutory supervision related to service that a license holder provided to its customers;

c. A license holder will ensure that no access to said information is possible, unless a proceeding stated in Section 27(c) of the Law related to a certain customer was commenced and the information is required by a license holder in order to manage the proceeding. Among other things, a license holder will ensure that the

means of access to said information are secured according to these directives, that they are held only by a small number of parties in the license holder, that access to said information is subject to approval by authorized parties in the license holder, and that access entails a process of data retrieval.

d. Upon the elapse of seven years from the end of the service period, a license holder will delete the information, excluding information required to manage a proceeding that commenced as stated in paragraph (c) before the end of said period. For this purpose, a license holder will perform controls of the deletion of said information.

e. All directives applicable to information security requirements and privacy protection in these directives will also apply to this information.

CHAPTER D1: VERIFYING THE CUSTOMER'S CONSENT TO PROVIDE CONTINUED ACCESS TO ACCOUNT INFORMATION

9A. A license holder who was granted access to a customer's account information for a limited period that exceeds six months shall verify, once every six months during that period, pursuant to the provisions of Section 26(b) of the Law, that the customer is aware that the permission to access their account information is in effect, based on their consent. Verification entails an active step performed by the customer attesting to their awareness that the license holder has access to their account information. Verification will be performed in one of the following ways:

a. The license holder will verify that the customer uses the license holder's account information services, for example: the customer accessed the app or website; with respect to a service rendered through email, the license holder received periodic indication that the customer opened their email; the customer contacted the license holder about a service rendered by the license holder that involves access to the customer's account information.

b. The license holder contacted the customer and requested that the customer actively indicate that they are aware that they gave the license holder access to their account information for a predefined period. The contact to the customer will state the length of the predefined period and the information baskets to which the customer gave the license holder access.

9B. If the license holder fails to verify that the customer is aware that the license holder may access the customer's account information, the customer will be deemed to have canceled their agreement with the license holder, as stated in Section 28 of the Law.

9C. The license holder will document and retain a record of the actions that it performed in order to verify that the customer is aware that the license holder's access to the customer's account is in effect, and will document the customer's use, or confirmation of the customer's awareness that the license holder may access their account information, as stated in Section 9A.

9D. In the case of a service that primarily entails the transfer of account information to a customer's representative, and the customer confirmed to the license holder

that the customer granted power of attorney to the representative for the purpose of rendering services as an account or tax consultant, the license holder may consider an action performed according to Section 9A by the representative as an action performed by the customer, provided that when confirmation as stated in Section 9 of the Directive concerning the transfer of account information to others, the customer confirms that they also granted power of attorney to the representative with respect to confirming the customer's consent to the continued transfer of account information according to Section 26(b) of the Law.

CHAPTER E: INFORMATION SECURITY AND PRIVACY PROTECTION

Article A – General

10. Information security and privacy protection – General:

    a. The information security standard defined in these directives will apply to all sensitive information in the license holder's possession.

    b. A license holder's communications to another party that contain sensitive information will be made using a standard protocol and encrypted transport layer security (TLS) based on the latest technologies available in the market.

    c. A license holder is obligated to follow the Standard in all requests or notifications received from an information source made through the account information interface system; This includes requests or notifications made in accordance with Sections 28(c)(2), 41(a)(2), 41(a)(3) and 45(c) of the Law, which will be made according to the Standard; and when rendering a payment initiation service.

    d. A license holder will not use the customer's details that are designed to authenticate the customer's identity by the information source, for the purpose of providing a payment initiation service.

Article B – Customer's first-time registration – the customer creates a user account with a license holder

11. In order to verify the customer's consent to receive an account information service or payment initiation service, the license holder will record and verify the details given to it by the customer by confirming that the ID number that the customer gave the license holder match the customer's ID number in the information source's records.

    The license holder will not request the customer's debit card in order to authorize the license holder's access to the customer's account information. However, the license holder may request the customer's debit card information for the purpose of paying for the service rendered to the customer by the license holder.

12. After the customer's details have been recorded by the license holder, the license holder will refer the customer to the information source's online channel where the customer will indicate their consent to give the license holder's access to the customer's account information.

13. When a customer wishes to receive a service from the license holder for the first time, the license holder will guide the customer to complete an enrollment process on the

license holder's app or website, where the customer will also receive a second authentication factor.

Article C – Customer connects to the license holder on an ongoing basis

14. After the customer completes their initial registration and a user account is created with the license holder, the customer will use the following means to connect to the license holder on an ongoing basis:

    a. through the license holder's app installed on the customer's mobile phone: The customer will access the app using an authentication factor that is used in a mobile phone such as a code, password, fingerprint, facial recognition, etc.

    b. Access to the license holder's website requires multi-factor authentication. In addition to a password, access requires a factor such as an OTP code sent by SMS or read by voice in a telephone call.

Article D – Use of an Open Banking Digital Certificate

15. A digital certificate will be issued only by a license holder's authorized parties for this purpose, according to the certificate issuance procedure published by the ISA.

16. A license holder will ensure that its Open Banking Digital Certificate is valid and contains the appropriate details that match the information on the license holder's license.

17. A license holder will use its Open Banking Digital Certificate only according to the license it was issued and the permitted uses of the license. A license holder will make proper use of the interface system by ensuring that the requests are valid and the number of requests, including requests submitted within a payment initiation service, matches the type of service that the customer requested.

18. Every time a license holder sends a request to an information source's account information interface system, the license holder is required to identify itself online using a designated digital certificate. A license holder will not use a digital certificate that is invalid or has been canceled or suspended.

19. All communications from a license holder to the information source will be based exclusively on the Standard. Notwithstanding the provisions of the beginning of this section and Section 10(c), any serious security incident will be reported to an information source through the Developers' Portal in accordance with Section 31 of the Law.

20. A license holder will submit a request to the ISA to suspend or cancel its Open Banking Digital Certificate if it is suspects that an information security incident that might lead to unauthorized use of its digital certificate. The certificate is suspended or canceled automatically when such a request is submitted. The license holder will confirm receipt of notification from the ISA that the certificate was canceled or suspended or will confirm such cancelation or suspension directly with the e-Government Unit .

    When such suspicion is removed, the license holder will notify the ISA and request that the suspension be canceled. The suspension will be canceled automatically or a new digital certificate will be issued to the license holder, according to the digital certificate issuance procedures.

Article E – Cancelation of an Open Banking Digital Certificate following the revocation or suspension of a license

21. If an AISP license is revoked or suspended in accordance with Section 7 of the Law, the Open Banking Digital Certificate of that license holder will be revoked.

22. If the Chair of the ISA suspended a license immediately, subject to their authority under Section 7(d) of the Law, the digital certificate of that license holder will be canceled immediately.

23. When the suspension period of a license holder's license ends, the ISA will issue a new digital certificate to the license holder.

24. A license holder that wishes to discontinue the provision of an account information service will notify the ISA of the need to cancel its Open Banking Digital Certificate.

25. A license holder may not contact an information source using its Open Banking Digital Certificate to request account information through the account information interface system as long as its license is canceled or suspended.

Article F – Generating, managing, and saving digital certificates, including Open Banking Digital Certificates

26. Each digital certificate will be associated with a single responsible entity within a license holder, which will serve as the certificate manager who is responsible for the entire key lifecycle.

27. A license holder will use the latest known digital certificate storage technologies.

28. A license holder will define and assimilate appropriate procedures and mechanisms for installing, storing, and safeguarding digital certificate based on the risks entailed in the type and scope of the license holder's operations. The procedures and mechanisms will address the following issues:

    a. protecting the digital certificate against unauthorized use or activity, including but not limited to modification, substitution, penetration, and deletion of a digital certificate;

    b. preventing unauthorized disclosure of the non-public contents of a digital certificate;

    c. indications of the operating state of digital certificates to ensure their proper activation;

    d. identifying errors in digital certificate activation and preventing leakage of sensitive data and critical security parameters resulting from such errors;

    e. real-time control of modifications and operations performed using a digital certificate.

Article G – Risk management

29. A license holder will verify that all the risks entailed in account information services or payment initiation services, including information security risks, cyber risks, privacy abuse risks, operating risks, fraud and embezzlement risks, legal risks, and compliance risks, are managed in a way that is appropriate for the license holder's operations, and their volume and complexity, and with a view to the degree and type

of risks entailed in the provision of its account information services or payment information services.

30. Without limiting the generality of Section 29, a license holder will:

a. at least once a year, define and approve a risk management framework to be incorporated in its risk management policy, and define procedures to implement the policy accordingly. The policy document will address the following, among others:

(1) the purposes for which the information will be used;

(2) the various types of information contained in the database;

(3) mapping of the processes and systems to which information security risk management applies and how these risks are being addressed;

(4) the information protection approach – information security and privacy protection;

(5) the means to be used and the resources to be dedicated to the protection of information assets;

(6) principles of back-up, retrieval, and business continuity after a disaster or realization of a threat scenario;

(7) outsourcing;

(8) development and modifications to information systems, including use of new technologies, and secure development techniques.

b. develop and assimilate a policy that establishes an open banking management framework. The policy will include, among others, aspects related to risk management, customer service, connectivity to information sources, and transport layer security (TLS).

c. verify that areas of responsibility are well defined and appropriate resources have been allocated to risk management, which includes appointing an information security and cyber-defense officer with appropriate training and experience to be responsible for all the issues related to information management and protection, as described in this Directive, and specifically as described in Section 32 below.

d. implement procedures to oversee the assimilation of the risk management framework;

e. implement physical and logical means of security to prevent, detect, rectify, and document exposures and risks, and report them, all according to the risk assessment and with reference to the following aspects:

(1) identification and authentication;

(2) privacy;

(3) data integrity;

(4) non-repudiation.

f. continuously monitor technological developments, and match the level of security and access controls to its systems, based on changes in the level of risks that are a function of these technological changes.

g. take steps to separate the production environment from the development and test environments.

h. to perform individual one-to-one identification of each entity that has access to a license holder's information systems, as a condition for granting access; In exceptional cases of suppliers and employees that cannot be identified in that manner, a license holder will implement appropriate alternative means of identification.

i. periodically, according to the risk assessment but no less frequently than once every 18 months, initiate a security assessment of the license holder's information technology system. The review will assess the effectiveness of the means of defense with reference to the assessed risks, and will propose means to correct any faults discovered.

31. To implement the provisions of Sections 29 and 30, a license holder will appoint a risk management officer with appropriate training and experience who will be responsible for risk management of the license holder, and who will report to the license holder's management; This person may also serve as the information security and cyber-defense officer, as stated in Section 30(c).

Article H – Information security and cyber-defense officer

32.

a. An information security and cyber-defense officer who is appointed according to Section 30(c) will have experience and knowledge in management of security components and is certified and has one or more of the following certifications or similar certifications:

(1) CISSP

(2) CCSA

(3) CCNA

(4) CISO

(5) CISA

(6) CISM

(7) vendor testers that successfully passed the final exams of a course for testers of cyber-compatibility for organizational supply chains, by an entity recognized by the National Cyber Directorate.

b. The information security and cyber-defense officer will perform the following actions:

(1) prepare an information security procedure;

(2) review the need to revise the information security procedure at least once a year or when the officer identifies the occurrence of significant changes in the database system and data processing procedures or in the exposures to risk, and will revise the procedure accordingly;

(3) prepare an ongoing control program over compliance with the requirements of the Law, and the Privacy Protection Law and its regulations; implement the program and inform the license holder's management of the findings, periodically, as defined in the policy;

(4) monitor implementation and assimilation of information security policy and procedures, information security survey recommendations, and the guidelines of relevant laws.

(5) define requirements for protecting the information in each new system that is purchased or developed, and when existing information systems are upgraded; and will be involved in the procurement or development of new systems and in system upgrades;

(6) In the event that high risk exposures were not addressed within a reasonable period following an information security review, the information security officer will study the reasons for the failure to address these exposures and will submit its recommendations on this issue to the license holder's management;

(7) investigate irregular events and submit its recommendations to the license holder's management within a reasonable period;

(8) from time to time, at least annually, review the defined information monitoring procedures, their adequacy, and the quality of events that were identified;

(9) provide professional guidance to the organization on information security and privacy protection issues;

(10) regularly examine the procedures for deleting account information possessed by the license holder in accordance with the provisions of the Law, including whether the volume of information saved in the database is greater than required by the purposes of the database and the requirements of the Law and this Directive.

Article I – Privacy protection

33. A license holder will at all times comply with the provisions of the Privacy Protection Law and the regulations enacted under it. With respect to these provisions, a license holder that manages a database that is subject to a basic level of security, as this term is defined in the Privacy Protection Regulations, will at all times comply with the requirements that apply to a database that is subject to a moderate level of security or higher.

Notwithstanding the provisions of Regulation 10(d) of the Privacy Protection Regulations, with respect to payment initiation services, documented information of the control mechanism stated in Regulation 10(a) of the Privacy Protection

Regulations will be retained for a period of no less than seven years from the documentation date.

CHAPTER F: THE SUPPLY CHAIN AND OUTSOURCING

Article A – Outsourcing

34. A license holder may manage, process, and store its information or develop systems, including consultancy, knowledge-based and other services, through entities outside the license holder, on the condition that the license holder itself performed the main activities entailed in the provision of an account information service or a payment initiation service.

35. Notwithstanding the provisions of this chapter, a license holder may not transfer its responsibility to fulfill all its statutory obligations to other entities, and any action that is outsourced, including cloud services as stated in Chapter G, will be deemed an action performed by the license holder, for which the license holder will bear full liability. The provisions of this paragraph will also apply to a license holder's liability when rendering a payment initiation service.

36. Outsourcing commitments will be defined in a written agreement.

Article B – Material suppliers

In this article, a material supplier is an external entity that is part of a license holder's supply chain and that provides services that are significant for the license holder's activities in areas related to information technology or that expose the license holder to potential information security risks that, if realized, might allow the license holder to be attacked or its operations to be disrupted.

37. In outsourcing to a material supplier, a license holder will verify the material supplier's trustworthiness and financial strength, and will assess in advance the adequacy of its qualifications and its ability to perform its tasks.

38. When outsourcing to a material supplier, a license holder —

    a. will define detailed principles regarding material suppliers' obligations toward the license holder with respect to information security risk management;

    b. will include in the agreement with the material supplier specific references to information security risk management, and will verify that the material supplier complies with the principles defined in subparagraph (a) above;

    c. periodically, but at least once every 20 months, will perform:

        (1) a mapping of the license holder's material suppliers; will review the agreement with them and their compliance with their contractual obligations; and will also assess a material supplier's need for changes as a result of technological developments and changes or changes in the services rendered;

(2) an assessment of the risks that derive from the services rendered by the material suppliers also on the basis of the review stated in subsection (a) and the results of the surveys stated in Section 30(i).

39. A license holder's agreement with a material supplier –

a. The agreement between a license holder and a material supplier will explicitly address the following issues at minimum:

(1) definition of the areas of responsibility of each party to the agreement, including subcontractors;

(2) an SLA;

(3) obligations of confidentiality, information security, privacy protection, and emergencies;

(4) arrangements to terminate the agreement and conduct dispute resolution arrangements, including arrangements that will allow the license holder to operate and maintain the outsourced activities in the event that the material supplier no longer supplies the service;

(5) access to information on audits and inspections conducted on the materal supplier's operations;

b. A license holder will consider incorporating the following terms into the agreement with the material supplier, based on the risk assessment:

(1) The material supplier will harden its systems that are installed on the license holder's network according to the license holder's information security and risk management procedures;

(2) The material supplier will transfer log files from the material supplier's systems, at the license holder's request;

(3) The material supplier will perform periodic vulnerability surveys and penetration tests, at the license holder's request, and according to the risk management.

(4) The material supplier will resolve issues identified in the surveys and penetration tests within a reasonable time after their discovery;

(5) The material supplier will perform trustworthiness tests for the material supplier's employees involved in the license holder's operations;

(6) The material supplier will appoint an information security trustee in the material supplier, and define its authority and functions;

(7) The material supplier will periodically present a list of subcontractors that support the services rendered to the license holder by the material supplier, at such frequency as determined by the license holder;

(8) The material supplier will define arrangements for deleting the license holder's data that are stored in the material supplier's premises upon termination of the parties' agreement, at the demand

of the license holder, and according to the deletion requirements that apply to a license holder;

(9) The material supplier will create a separation between the material supplier's development and production environments;

(10) The material supplier will create a separation between the license holder's (tenants-based) work environments, if the material supplier provides services to additional corporations/service providers;

(11) The material supplier will report to the license holder of any information security incident related to the license holder's operations that occurred in the material supplier or a subcontractor thereof.

40. A license holder will define, based on the risk assessment, those activities for which the material supplier is subject to multi-factor authentication, such as remote access to the license holder's systems, maintenance activities on the license holder's systems, etc.

41. A license holder will define security and control mechanisms for a material supplier's remote access, based on the risk assessment, such as: prevention of unauthorized access; secure access from an operating environment that is separate from the material supplier's work environment; activation of a time-out mechanism after a period of no activity on the material supplier's side; recording and monitoring of maintenance activities, etc. Furthermore, no access to a license holder's production environment will be possible without the license holder's approval.

42. Upon a change in the ownership of a material supplier, the license holder will re-examine their agreement to ensure the new owners' compliance with the material supplier's obligations toward the license holder.

CHAPTER G: CLOUD COMPUTING

43. Before activating cloud-based systems, a license holder will conduct proper mapping and risk assessment, involving all relevant entities in the license holder, and will also detail the controls, tools, and actions required to mitigate the risks. The risk assessment will be revised regularly during the agreement period, according to, among other things, technological, legal, regulatory, business, and organizational changes in the license holder and in the cloud service provider.

44. In material cloud computing, before entering into an agreement with a cloud computing supplier, a license holder will perform due diligence, including with respect to the supplier's financial strength, its professional capabilities, and its experience in providing similar services. A license holder will perform such due diligence from time to time during the agreement period as well.

45. A license holder will develop a policy for using cloud computing technologies, which will refer, among other things, to the types of applications and services that use cloud computing technology, authority and responsibility, controls, legal issues, development, maintenance, monitoring, information security, etc.

46. A license holder may store sensitive information or customer data outside the borders of the State of Israel if the license holder verified that the cloud service supplier maintains the standard of security stated in the General Data Protection Regulation (GDPR) and notified the customer of the same.

47. Nothing in this Directive limits the obligations that apply to a license holder according to all the relevant laws and regulations for using cloud computing technologies, including the Privacy Protection Law and the Privacy Protection Regulations (Transfer of Information to Databases Outside State Borders) 5761-2001, and Database Registrar Guideline No. 2/2011 "Uses of Outsourcing Services for Processing Personal Information."

48. A license holder will verify that the cloud computing supplier complies with generally accepted standards of physical security and information security and has external certifications that also include reference to identification and authentication, access permissions, controls of activities and logs, cyber-defense surveys and inspections.

49. Data in the cloud will be accessed using secured methods of access such as authorized addresses only, multi-factor authentication, encryption, etc.

50. In the event that a license holder's data are stored in a multi-tenant system that is not used exclusively by the license holder, the license holder will ensure that technologies such as encryption, data masking, or tokenization are used to prevent the disclosure of sensitive information of customers' data to unauthorized entities.

51. In cloud computing, sensitive information will be encrypted, even if the infrastructure is used exclusively by the license holder.

52. A license holder will verify that it has the ability to monitor information security incidents that occur in the cloud.

53. In cloud computing, a license holder will verify that means of information security and cyber defense are in place in all channels of access from and to the cloud computing supplier, and these will, as far as possible, minimize the risk that these channels will be used to attack the license holder.

54. A license holder will also include the following terms in its agreement with a cloud computing supplier:

    a. the license holder has a unilateral option to terminate the use of the cloud computing supplier's services or to transfer to another supplier by transferring its relevant data from the supplier's systems within a short time, deleting the data in the supplier's systems, while the supplier undertakes not to retrieve this information in its systems.

    b. The license holder will receive information related to inspections and audits of the cloud computing supplier.

55. Upon any change of ownership of the cloud computing supplier, a license holder will review the agreement to ensure that the new owners also comply with the cloud computing supplier's obligations toward the license holder.

CHAPTER H: REPORTING

Article A - General

56. A license holder will report to the ISA about its operations, both periodically and regularly, as defined in these directives.

57. Any document or declaration that a license holder submits to the ISA under this chapter will be submitted or given by a senior officer of the license holder who is authorized to do so, in the manner defined in Section 4 of the Rules for Submitting an AISP License Application.

Article B – Annual reports

58. A license holder will report the following information annually, and no later than one month from the end of the reporting year:

    a. the company's revenues from the provision of the services in Israel in the reporting year;

    b. a certificate of insurance as stated in Section 8(a) (if the Applicant selected this alternative), which includes details of the license holder's terms of insurance, the insurer's name, the period of insurance, the insurance amount, and the co-payment, and the board of directors' confirmation that the scope and terms of the insurance are sufficient to fully insure the license holder's liability for any negligible act or omission toward a client, in view of the considerations listed in Section 8(c); or confirmation of details of the Deposit as stated in Section 8(b) (if the Applicant selected this alternative), and the Trustee's confirmation of the entity in which the Deposit was made, and that it is administered as required in Section 8(b), and confirmation by the board of directors that the amount of the Deposit was determined according to the considerations listed in Section 8(c).

    c. a current opinion of an auditor, highlighting any changes that occurred in the matters listed in Section 2(6)(a)(1) of the Rules for Submitting an AISP License Application .

    d. a current mapping of risks, highlighting any changes that occurred in the matters listed in Section 2(l2) of the Rules for Submitting an AISP License Application.

    e. a current list of the license holder's senior officers, controlling shareholder, and senior officers of the controlling shareholder (if it is a corporation), and their details, as listed in Section 2(2) of the Rules for Submitting an AISP License Application .

Article C – Monthly reports

59. A license holder will report to the ISA at the end of each month and no later than 10 business days thereafter about the following, using the relevant form on the reporting website:

    a. its operations in the open banking standard, including the number of requests made to information sources, the number of payment orders transferred by it, the number of customers, the number of times customers consented or

canceled their consent to collect information from information sources, and the number of reports about service standards;

b. the number of customer complaints, including complaints concerning flawed information, as this term is defined in Section 61(a) of the Law, difficulty in connecting to the information sources, or significant defects in the provision of an account information service or payment initiation service;

c. the number of rejected requests, the number of new customers and customer turnover.

Article D - Immediate reports

60. The deadline for submitting an immediate report is the end of the business day on which the license holder first learned of the event; For this purpose "the license holder first learned of the event" – means that the license holder learned of the event from one of the following: the chair of the license holder's board of directors, the CEO of the license holder, the license holder's chief business manager, the license holder's most senior officer in the field of finance, the company secretary, or anyone acting in any of these positions even if their title is different.

61. The report will state the date on which the reported event occurred, if known to the license holder, and the date on which the license holder first learned of the reported event.

62. A license holder will submit an immediate report to the ISA in the following events:

a. a change in the information that the license holder gave to the ISA;

b. a decision was made to make a significant change in a detail included in the license application that was submitted to the ISA, or in the license holder's most recent annual report to the ISA as stated in Section 58, and that has or may have a material effect on the license holder or its customers;

c. the occurrence of an event that has or may have a material effect on the license holder or its customers;

d. a decision was made to make a change or revision to the type of account information services that are offered or to make material changes in the nature of the license holder's business that may affect the license holder's business risks and operating risks;

e. if a severe security incident as this term is defined in Section 31 of the Law occurred, the license holder will immediately notify the ISA and will report the findings of its investigation and the actions taken in response to the incident.

f. an information source gave notice to the license holder under Section 41(a)(2) of the Law and the information source's reason for its refusal to grant access to information, and a notice of the removal of the impediment to access that the license holder received from an information source under Section 41(a)(3) of the Law.

g. an event that compromised information integrity, an event in which unauthorized use of information was made or in which there is an indication

that sensitive information about customers was exposed or leaked outside the license holder's premises, or any other significant event that occurred or almost occurred and had or might have had a significant effect on the management of the information and its protection.

h. operations of systems that contain sensitive information were damaged or suspended for more than 3 hours (excluding a planned suspension), or an interruption of material services resulting from an unplanned suspension of the operations of the automated systems for one or more business days.

i. any irregular event, including significant attempts to penetrate and attack the computer systems, actual penetration of the computer systems, collapse of major systems, activation of a response plan for irregular events, etc.

j. unauthorized use of an Open Banking Digital Certificate.

k. notice of an insurance event was given to an insurance company, in connection with insurance that was issued to the license holder under Section 8(a), including the content of the notice and its submission date.

l. a change in the coverage or amount of the insurance issued to the license holder under Section 8(a), including the details of the change, its date and its causes.

m. a change in the Deposit made by the license holder under Section 8(b) or in the details of the Deposit Trustee.

n. a notice given under Section 20(a) of the Law.

o. appointment of an individual as a senior officer of the license holder or of its controlling shareholder, including the details listed in Section 2(2) of the Rules for Submitting an AISP License Application.

p. appointment of an individual as the information security officer or the risk management officer of the license holder, including the details listed in Section 31 or 32 of this Directive, respectively.

q. an individual ceased to be a senior officer of the license holder or of its controlling shareholder, or ceased to be an information security officer or risk management officer in the company.

r. a change in the holdings of the license holder's controlling shareholder such that it ceases to be the controlling shareholder, or if a person became a controlling shareholder of the license holder without a control permit.

63. Notwithstanding the provisions of Section 60, reports according to Section 62(o) – (p) will be submitted no later than the end of 7 business days after the date on which the license holder first learned of the event.

CHAPTER I: COMMENCEMENT

This Directive will come into force on the date that notice of its issue is published in Reshumot.

Hebrew text published on the ISA website on March 15, 2022.

Revision 1: September 7, 2022

Revisions:

Version	Details	Date
Original Directive		March 15, 2022
Revision No. 1	New terms were added; Sections 2-5 were modified;[2] Sections 7A-7B were added; Sections 8, 10, 17, 29, 32-34, 57-59, 62 were amended; Chapter D1 (Sections 9A-9D) were added.	September 7, 2022

[2] These now appear in the Rules for Submitting an Application for an AISP License.