VERUM PAYMENTS LIMITED

PUBLIC OFFER

Terms of Use (User Agreement)

e-Residency Kazakhstan service

Programme Operator - Verum Payments Limited, AIFC

DOCUMENT	OPERATOR	PROGRAMME	EDITION
Public Offer (User Agreement)	**Verum Payments Limited, AIFC**	**e-Residency Kazakhstan**	**November 2026**

SECTION 1

INTRODUCTION

These Terms of Use (the “Agreement”, the “Offer”, the “Terms”) constitute a public offer. By acceding to them (by registering, clicking the “I Agree” button, entering a one-time password or otherwise using the service), you (the “User”, the “Client”, “you”, “your”) enter into a contract of adhesion with the Operator of the e-Residency Programme on the terms set out below. The Agreement is supplemented by, and shall be construed together with, its Annexes and the Privacy and Data Processing Policy.

Operator of the e-Residency programme: Verum Payments Limited (the “Operator”, “we”, “us”, “our”), acting through its own mobile application and/or embedded frames (WebView) within the mobile applications of second-tier banks of the Republic of Kazakhstan (the “Partner Banks”), as well as through integrated eSIM services and payment widgets.

Verum Payments Limited is a private company incorporated under the applicable law of the Astana International Financial Centre (AIFC), business identification number 231240900271, acting under license Ancillary Services (Providing Consulting Services) AFSA-O-LA-2026-0008 dated 25-06-2026, registered address: Republic of Kazakhstan, Astana, 55/22 Mangilik El Avenue, block C 4.3, office No. 228, Z05T3E5.

By accepting these Terms, you expressly acknowledge and agree to the following:

i) Age and legal capacity - you are at least eighteen (18) years old and have the legal capacity to enter into binding agreements;

ii) Acceptance of the Terms - you have carefully read, understood and agree to comply with these Terms and with the Privacy and Data Processing Policy;

iii) Consents - you consent to biometric verification; to anti-money laundering and counter-terrorist financing procedures (AML/KYC) and identification; to the processing and cross-border transfer of your personal data to the recipients listed in Annex 2, to the extent and for the purposes set out in Section 12, including the routing of data to the Ministry of Internal Affairs of the Republic of Kazakhstan (MIA RK) for the issuance of a digital identity document with an individual identification number under the e-Residency programme, to the selected Partner Bank, crypto exchange, insurance company and mobile network operator; to the engagement by the Operator of marketing operators in the manner set out in clause 12.6; and to the receipt of service, informational and advertising messages in the manner set out in clause 12.6, with the right to opt out of advertising messages at any time.

You acknowledge that AML/KYC fees (including a repeat AML/KYC check where required) are non-refundable.

iv) No guarantee of outcome - you acknowledge and agree that recognition as a digital resident with the issuance of a digital identity document bearing an assigned e-Residency IIN, the provision of an eSIM, as well as any decisions of international banks, commercial banks or crypto exchanges regarding the opening or servicing of accounts and/or cards, fall exclusively within the competence of the relevant governmental authorities and/or financial institutions. Accordingly, we do not state, guarantee or confirm that any such applications, requests or processes will be approved, completed or supported.

SECTION 2

SCOPE OF SERVICES

2.1. The Operator provides digital infrastructure and services for:

- a) remote identity verification (KYC) and anti-money laundering (AML) screening, including NFC reading of the passport, liveness detection, and screening against sanctions lists / watchlists / adverse media / reputational sources;
- b) submitting verified identification data to request an e-Residency IIN and a digital identity document within government systems;
- c) transferring verified data and the e-Residency IIN to Partner Banks and/or crypto exchanges for remote account opening / card issuance;
- d) transferring to insurance companies the data required to arrange a medical insurance policy;
- e) enabling the issuance and activation of an eSIM through an accredited mobile network operator (aggregator model), including a “white list” of incoming SMS messages while abroad;
- f) displaying in the Operator's application the status of applications, the e-Residency IIN data and, subject to your consent, information on cards/accounts issued by Partner Banks.

2.2. The Services or their scope may be amended, updated or suspended at the Operator's discretion.

2.3. The Operator does not guarantee: (i) the issuance of an e-Residency IIN and a digital identity document by governmental authorities; (ii) the opening of an account / issuance of a card by any particular bank or crypto exchange; (iii) the uninterrupted operation of governmental or partner systems; (iv) the acceptance by a bank of the results of our KYC procedure without its own checks.

2.4. Applying for a digital identity document with an e-Residency IIN and applying for a visa are not interrelated; these are two separate processes with different requirements, governed by different laws. Holding a digital identity document with an e-Residency IIN is not a ground for obtaining a visa, and vice versa.

2.5. Remote incorporation of a company by digital residents in the Astana International Financial Centre (AIFC) is carried out through the AIFC Digital Residency information system in accordance with the applicable law of the AIFC. Company registration is permitted solely within the AIFC jurisdiction and constitutes a separate procedure. Obtaining a digital identity document with an e-Residency IIN does not in itself mean that a business has been automatically established.

SECTION 3

KEY DEFINITIONS (TERMS)

- **AML (anti-money laundering)** - a set of measures aimed at preventing the use of financial systems for money laundering and terrorist financing.
- **Account** - the account created by you to access the e-Residency services.
- **Digital resident (e-Residency)** - a foreign national or stateless person who has obtained a digital identity document with an e-Residency IIN through the Operator's mobile application.
- **Operator of the e-Residency programme** - Verum Payments Limited, which provides identification, AML/KYC/sanctions screening, fraud prevention, routing of data to governmental authorities and to Partner Banks/crypto exchanges, as well as the issuance/activation of an eSIM through an accredited mobile network operator. The Operator is not a governmental authority, does not issue the digital identity document and does not assign the e-Residency IIN.
- **e-Residency IIN** - the individual identification number of digital residents, being a unique 12-digit numeric code assigned by the MIA RK to a non-resident under the e-Residency programme. The Operator does not assign the e-Residency individual identification number.
- **Digital identity document with an e-Residency IIN** - a digital document intended solely for use in the electronic environment for the purposes of identifying the user, confirming their identity and authorship in various digital processes, and providing digital signatures. It does not confer any

right of entry into or residence in Kazakhstan. The Operator does not issue the digital identity document.

- **eSIM** - a digital SIM card in the form of an embedded software module that allows mobile communication services to be activated and used remotely without the need to physically insert a SIM card into the device.
- **KYC (Know Your Customer)** - the customer identity verification process used by financial institutions and other organisations to prevent fraud, money laundering and terrorist financing.
- **Mobile network operator** - a communications operator accredited by the Operator for the issuance of eSIMs.
- **Marketing operators** - third parties engaged by the Operator to create, personalise, technically prepare, deliver and assess the effectiveness of marketing and informational messages, including advertising agencies, providers of email/SMS/push messaging platforms, CRM and CDP systems, call centres and web analytics service providers.
- **NFC (Near Field Communication)** - a short-range wireless data transmission technology used, among other things, for contactless payments and the exchange of information between devices.
- **Partner Banks** - second-tier banks of the Republic of Kazakhstan integrated with the Operator under bilateral agreements.
- **Crypto exchange** - a licensed venue for the exchange and trading of digital assets, integrated with the Operator under bilateral agreements.
- **2FA/OTP** - multi-factor authentication technology using one-time passwords and/or additional user identification factors to enhance the security of access to the services.

SECTION 4

REGISTRATION AND ACCOUNT

4.1. Use of the Services requires: (i) creation of an Account; (ii) completion of remote identification; (iii) acceptance of these Terms, the Privacy and Data Processing Policy and the Cookie Policy.

In order to use our services, you must create an Account. To create an Account you must meet at least the following conditions:

- you are a natural person and must be of legal age to enter into a legally binding contract (18 years or older);
- you have a valid email address, mobile telephone number and postal address;
- you have full authority to enter into these Terms without breaching any other agreement you have entered into;
- you are not restricted from using our services (the “Conditions”).

In addition, you may be required to comply with further requirements in order to open an Account or use the Services. We will make reasonable efforts to notify you of any additional requirements, but your ability to open an Account and use the Services is governed by those additional requirements regardless of whether notice has been given. By creating an Account or using the Services, you represent and warrant that you meet all the Conditions. If you cease to meet the Conditions, you must notify us immediately and stop using your Account and the Services. We may require evidence that you meet the Conditions. Even if you meet the Conditions, we may determine at our discretion that you are not eligible to create an Account or use the Services.

4.2. You undertake to:

- a) provide accurate, complete, truthful and up-to-date information (including your email address, mobile telephone number and postal address) when using any Account or service;

- b) not transfer, grant or disclose access to your Account to any third party, or permit any other person to use your Account, including by sharing your login credentials, password, one-time passwords (OTPs), verification codes, authentication credentials or any other data enabling access to your Account. Your Account is intended solely for your personal use and may not be transferred, shared or made available for use by any third party;
- c) not use your Account for the benefit of anyone other than yourself;
- d) protect your device / SIM card / email and one-time passwords;
- e) keep your Account secure, including by using a strong password that you do not use anywhere else;
- f) be responsible for all actions performed under your Account and assume all risks of any authorised or unauthorised access to your Account, to the maximum extent permitted by applicable law;
- g) notify us immediately if you discover or suspect any security breach relating to your Account.

4.3. You authorise us to make enquiries, directly or through third parties, that we consider necessary to verify your identity, confirm the eligibility requirements set out above, protect you or us from fraud or other financial crime, and that we consider may be necessary to ensure compliance with these Terms and applicable law. You understand and agree that we may take such action as we reasonably consider necessary based on the results of such enquiries, that we are not obliged to inform you of the results of any enquiry, and that you expressly waive any obligation to notify you of any possible remedial measures. In carrying out these enquiries, you acknowledge and agree that your personal information may be disclosed to credit bureaux, governmental financial crime authorities or any other governmental authorities as required by law.

4.4. We reserve the right, at our sole discretion, to refuse, suspend or restrict the provision of the Services in whole or in part at any time and without any obligation to provide an explanation. Such measures may be taken, among other things, where:

- (i) inconsistencies, falsification or forgery of documents or information are detected;
- (ii) the client presents a high risk under applicable sanctions, anti-money laundering (AML), counter-terrorist financing (CTF) or other regulations; we may refuse users from restricted jurisdictions without giving reasons;
- (iii) these Terms, contractual obligations or any applicable laws and regulations are breached;
- (iv) fraud or illegal, unethical or abusive activity is suspected;
- (v) engagement with the client is considered to present reputational, regulatory, operational or security risk;
- (vi) we are obliged to act at the direction of competent authorities, regulators or other lawfully empowered bodies;
- (vii) we detect that you have transferred your Account, granted access to your Account to any third party, or permitted any person other than you to use your Account. In such circumstances, we reserve the right to immediately block your Account and suspend your access to the Programme Services in whole or in part, without prior notice, for the duration of an investigation into the circumstances of the violation. We reserve the right to maintain such restrictions until the reasons for their imposition have been remedied, or to discontinue the provision of the Services and terminate these Terms in accordance with these Terms and applicable law.

4.5. We may determine at our discretion whether it is necessary or appropriate to temporarily suspend or even delete your Account.

4.6. You are solely responsible for all acts and omissions carried out under your Account; all actions performed using your Account will be deemed to have been performed by you.

SECTION 5

REMOTE IDENTIFICATION (NFC, LIVENESS, AML/KYC)

5.1. As part of the registration process, you must provide us with the information requested at account opening in order to identify and verify your identity, and to detect money laundering, terrorist financing, fraud or any other financial crime, and you must allow us to keep records of that information. You will need to complete certain verification procedures before you are permitted to start using the Services.

5.2. Mandatory stages: NFC reading of the biometric passport, liveness detection, upload of scanned data, completion of the questionnaire and provision of consent to the processing and verification of biometric data.

5.3. The information we request may include certain personal information, including but not limited to your full name (surname, given name, patronymic (if any)), address, telephone number, email address, date of birth, taxpayer identification number, information about your bank account (for example, bank name, account type, routing number and account number), network status, customer type, customer role, billing type, mobile device identifiers (IMEI) and other subscriber status data. By providing us with this or any other information that may be required, you confirm its accuracy and correctness and undertake to inform us of any changes to the information you have provided. We will handle this information in accordance with data protection provisions.

5.4. We may request additional documents/translations, including notarised ones, where required by law or by a governmental authority, bank or crypto exchange (including confirmation of transliteration).

5.5. We carry out sanctions, politically exposed person (PEP), adverse media and reputational risk screening using external data sources (in particular Sumsub, Dow Jones Risk & Compliance, LSEG World-Check, Dun & Bradstreet Onboard, Factiva, Kompra, ATTIS and other similar providers), as well as fraud screening. The list of providers may change; the current categories of data recipients and jurisdictions are set out in Annex 2.

SECTION 6

E-RESIDENCY IIN: PROCESS AND LIMITATIONS

6.1. Validation and routing. If your personal data is successfully validated, we will submit it to the relevant government databases. The decision to assign a digital identity document with an e-Residency IIN is taken exclusively by the MIA RK. We make no representation, warranty or undertaking as to the outcome of that decision.

6.2. Refusal of issuance. In the event that the MIA RK refuses to issue a digital identity document with an e-Residency IIN, any related claims, appeals or objections must be addressed directly to the MIA RK. We may, at our discretion, provide reasonable assistance with re-submission of applications; however, we are not obliged to carry out additional AML/KYC procedures free of charge in connection with such re-submission.

6.3. Update upon entry. Upon physical entry into the Republic of Kazakhstan for the purpose of conducting business or commercial activity, your e-Residency IIN may require updating, including removal of the “e-Residency” designation, in accordance with the rules of the MIA RK and other applicable legal requirements. Tourists and visitors entering Kazakhstan without the intention of conducting business or trade may not be required to update it, in accordance with the laws and regulations in force at the relevant time.

6.4. Limitation of liability. We act solely as an intermediary in the transfer of data and bear no responsibility for the acts, decisions or omissions of any governmental authority, including but not limited to the approval, refusal or delay of the issuance or updating of the digital identity document

with an e-Residency IIN. All decisions remain within the exclusive competence of the relevant governmental authority.

SECTION 7

BANK / CRYPTO EXCHANGE ACCOUNTS AND MIRRORING

7.1. Data transfer. Following successful completion of AML/KYC procedures and the assignment of a digital identity document with an e-Residency IIN, we will, on your express instruction, transfer to the Partner Bank and/or crypto exchange selected by you only the minimum necessary identification data together with the assigned e-Residency IIN. Such transfer is limited to the information required to establish a relationship with the relevant institution.

7.2. Independent AML/KYC system. Each Partner Bank or crypto exchange conducts its own independent AML/KYC procedures in accordance with its internal policies and applicable law. These institutions retain the full right to approve or refuse the opening of an account, the issuance of cards or the provision of services, and may refuse without providing any explanation or justification. We bear no responsibility for such decisions.

7.3. Duplication of information. With your prior and express consent, information about accounts and/or cards opened through our services may be duplicated and displayed in the Operator's application for convenience and compliance monitoring purposes. Similar information may also be displayed in the Partner Bank's application. Such duplication is intended solely for informational and compliance purposes and does not create, amend or extend any contractual rights or obligations.

7.4. Subsequent accounts and renewed checks. Where you open additional accounts or cards with other Partner Banks, the Operator is required to carry out renewed or updated AML/KYC checks in order to comply with regulatory requirements, maintain the currency of verification and reduce the operational and compliance risk of the participating banks. Such procedures will be carried out in accordance with applicable law and the rules governing interaction between Partner Banks and the Operator.

7.5. Restriction of the provision of financial services based on information received from competent authorities. Where the Operator receives an official request, notification, demand, order, resolution, letter or other communication from law enforcement, investigative, prosecutorial, judicial, special state or other authorised authorities of the Republic of Kazakhstan, or from competent authorities of foreign states, containing information regarding the possible unlawful use by you of your e-Residency IIN, digital identity document with an e-Residency IIN and/or other identification data obtained under the Programme, including for the purpose of committing or facilitating the commission of an administrative offence or criminal offence, the Operator shall be entitled to notify the relevant Partner Bank, crypto exchange or other financial service provider that is a partner of the Programme of the existence of such information and the need to suspend, restrict or discontinue the provision of the relevant financial services to you.

The Operator may also send such notification where the information received from a competent authority indicates that a verification, pre-investigation inquiry, investigation, criminal prosecution or other proceedings relating to the suspected unlawful use of your e-Residency IIN, digital identity document with an e-Residency IIN or other identification data obtained under the Programme are being conducted in respect of you.

The relevant Partner Bank, crypto exchange or other financial service provider shall independently decide whether to suspend, restrict or discontinue the provision of financial services to you in accordance with applicable law, financial monitoring requirements, orders and decisions of competent authorities, its internal rules and its agreement with you.

The Operator is not a party to the agreement between you and the relevant financial service provider and does not make decisions regarding the opening, blocking or closure of bank accounts, the

issuance or blocking of payment cards, the suspension of transactions on accounts or the discontinuation of other financial services, unless expressly provided otherwise by applicable law or by an agreement between the Operator and the relevant financial service provider.

The Operator shall be entitled not to notify you that such notification has been sent to a financial service provider or of the contents of the information received from a competent authority where such notification is prohibited by applicable law or by the requirements of the relevant competent authority, or where such notification may impede a verification, operational-search activities, an investigation, criminal prosecution or other proceedings.

SECTION 8

ESIM AND CONNECTIVITY

8.1. Issuance. The eSIM is issued exclusively by an accredited mobile network operator using our embedded technology platform. We act solely as an intermediary in this process and bear no responsibility for the performance, coverage or service level of the mobile network operator. The issuance and continued provision of the eSIM are determined solely by the accredited mobile network operator and in accordance with its policies.

8.2. Restrictions outside Kazakhstan. When used outside the Republic of Kazakhstan, the following restrictions apply to the eSIM:

- incoming SMS messages are received only from numbers included in a pre-approved “white list”;
- outgoing SMS messages and voice services are disabled;
- the eSIM may not be used for registration in applications or services not included in a pre-approved “white list”;
- data-only packages remain available in accordance with the applicable tariffs.

8.3. Activation of services upon entry/exit. Upon physical entry of the eSIM user into Kazakhstan, the full range of services (including incoming/outgoing SMS, voice and data) will be enabled in accordance with the applicable tariffs. Upon departure from Kazakhstan, the above restrictions applicable to use outside the country will be automatically reinstated.

8.4. Tariffs and included period. The price specified in item 1 of Annex 1 additionally includes 30 (thirty) calendar days of eSIM service, calculated from the date of eSIM activation. Upon expiry of that period, you may at your discretion renew the eSIM service in accordance with the tariffs in force at the time of renewal. The applicable tariffs of the mobile network operator are made available to you in the application before activation and before each renewal. In the absence of renewal, the eSIM is deactivated; such deactivation does not affect your e-Residency IIN, digital identity document or digital resident status. We reserve the right not to disclose or itemise the internal cost structure of eSIM services.

8.5. Use for authentication. The eSIM may be required by Partner Banks, crypto exchanges or financial service providers for the provision of 2FA/OTP services, unless expressly provided otherwise in the specific agreements concluded with those partners.

8.6. Deactivation. The eSIM is deactivated upon expiry of the included or renewed period, upon termination of these Terms, or upon suspension or termination of your Account. If the eSIM is used for the delivery of 2FA/OTP, you are responsible for having an alternative authentication method with the relevant institution.

SECTION 9

PAYMENTS, FEES, CURRENCY

9.1. Payments are processed through integrated acquiring systems that support the acceptance of both local and international cards and other payment instruments.

9.2. The cost of the Services is set out in Annex 1.

9.3. AML/KYC fees are non-refundable. The AML/KYC service is deemed fully rendered, and the fee earned, once the verification process has commenced, irrespective of its outcome. You agree that the service paid for shall not be the subject of chargebacks under the dispute procedures of payment systems initiated by you after the verification process has commenced, irrespective of its outcome.

9.4. The billing currency and conversion are determined in accordance with the rules of the applicable payment system; issuing bank and acquirer fees may apply.

SECTION 10

ACCEPTABLE USE AND PROHIBITIONS

10.1. Prohibited use. You may not, directly or indirectly:

- a) provide or attempt to provide any false, forged, misleading or fraudulent documents, information or biometric data;
- b) attempt to circumvent, evade or otherwise breach any applicable sanctions, export controls or restrictions, or use the Services for purposes connected with money laundering, terrorist financing, fraud or any other unlawful activity;
- c) use VPNs, device emulators, jailbroken devices or other technical means to interfere with, circumvent or otherwise compromise the integrity of identification or verification processes;
- d) interfere with the normal operation of the Services, attempt to decompile, reverse engineer, disable or circumvent any technical protection measures, or otherwise attempt to gain unauthorised access to systems;
- e) infringe the intellectual property rights, privacy rights or data protection rights of third parties, or act in breach of applicable export control legislation or other regulatory restrictions.
- f) transfer, assign, make available for use or otherwise provide any third party with access to your Account, login credentials, authentication credentials or verification codes, or permit any person other than you to use your Account or the Services, including for the purpose of circumventing identity identification, identity verification or AML/KYC procedures.

10.2. Enforcement and reporting. We reserve the right to immediately suspend or terminate your access to the Services in the cases specified in clauses 7.5 and 10.1 of these Terms, as well as where we have reasonable grounds to suspect, or establish, that you have engaged in any prohibited activity. In such cases, we may also notify the competent authorities and regulators as part of our cooperation with them.

Where any of the circumstances specified in clauses 7.5 and 10.1 of these Terms are identified, the Operator shall be entitled to notify the relevant Partner Bank, crypto exchange or other financial service provider of the need to take measures in respect of the financial services provided to you, as provided under applicable law and the internal procedures of the relevant financial service provider.

SECTION 11

INTELLECTUAL PROPERTY AND LICENCE

11.1. The application, technology platforms, interfaces, content, trademarks, service marks, trade names, logos, databases and any other related intellectual property (collectively, the “Operator Materials”) are and shall remain the exclusive property of the Operator and/or its licensors. The Operator Materials are protected by the legislation of the Republic of Kazakhstan, AIFC acts and applicable international intellectual property law.

11.2. You are granted a limited, revocable, non-exclusive, non-transferable and non-sublicensable licence to use the Operator Materials solely for personal, lawful and non-commercial purposes and only for the term of these Terms. This licence does not grant you any ownership rights in the Operator Materials and terminates automatically upon suspension or termination of these Terms.

11.3. You may not, directly or indirectly, copy, reproduce, modify, adapt, translate, reverse engineer, decompile, disassemble, rent, lease, sell, sublicense, distribute, commercialise or otherwise use the Operator Materials in any manner not expressly permitted by these Terms. Any unauthorised use will result in immediate termination of your licence and may give rise to legal liability.

SECTION 12

PERSONAL DATA, BIOMETRICS AND MARKETING COMMUNICATIONS

12.1. The collection, storage and processing of personal and biometric data are carried out in accordance with this Section and the Privacy and Data Processing Policy, which forms an integral part of these Terms. Processing is governed by the AIFC Data Protection Regulations.

12.2. The use of biometric verification methods, including facial recognition, liveness detection and identity confirmation via NFC, requires your express informed consent.

12.3. Consent to the processing of personal data

By acceding to these Terms, you grant the Operator consent to collect and process your personal and biometric data, including:

- surname, given name, patronymic (if any), including in transliteration;
- date and place of birth, sex, citizenship, country of tax residence;
- identity document data, including the machine-readable zone and data obtained through NFC reading;
- email address, mobile telephone number, address of residence (registration) and postal address;
- taxpayer identification number;
- the e-Residency IIN once assigned by the MIA RK;
- biometric data: facial photo and video images, liveness detection results, biometric matching results;
- device identifiers and subscriber data (IMEI, IMSI, eSIM ICCID, network status, customer type and role, billing type);
- information on payment transactions made in connection with payment for the Operator's services;
- data obtained during AML/KYC checks, including information on source of funds and source of wealth, and the results of sanctions, PEP and reputational screening;
- information on your status in the Programme, the composition of the services purchased, the date of the last update and the history of your interaction with the Operator's services;
- other information required under applicable law and by the requirements of data recipients.

12.4. Operations with personal data

The consent extends to the collection, recording, systematisation, accumulation, storage, clarification (updating, amendment), extraction, use, transfer (including cross-border transfer and granting of access to third parties), depersonalisation, blocking, deletion and destruction of personal data, whether by automated means or otherwise.

12.5. Purposes of processing

Processing is carried out for the following purposes:

- conclusion and performance of these Terms, provision of the Services and user support;
- remote identification, AML/KYC screening, enhanced due diligence (EDD), sanctions and PEP screening, fraud prevention;
- submission of identification data to government information systems for consideration of the issuance of a digital identity document with an e-Residency IIN;
- transfer of the minimum necessary volume of data to the Partner Banks, crypto exchanges, insurance companies, mobile network operator and acquiring providers selected by you for the provision of the relevant services;
- annual data updating and maintenance of your status as a Programme participant;
- sending you informational, advertising and marketing messages about services, tariffs, changes and new features of the Programme, about the partner and referral programmes, and about the products and offers of the Operator's partners listed in Annex 2;
- creation of relevant offers by means of profile segmentation using non-special categories of data (country of residence, status in the Programme, composition of services purchased, date of update);
- providing the Operator's partners (Partner Banks, crypto exchanges, insurance companies, mobile network operators) with the data required for preliminary assessment and the formation of individual offers for their products and services sent to you;
- engagement by the Operator of third parties (Marketing operators) to create, personalise, technically prepare, deliver and assess the effectiveness of marketing and informational messages, and to conduct surveys on satisfaction with the quality of the Services;
- performance of statutory obligations regarding record retention and the provision of information to competent authorities;
- notification of Partner Banks, crypto exchanges and other financial service providers that are partners of the Programme of circumstances identified by the Operator relating to the possible unlawful use by you of a digital identity document with an e-Residency IIN and/or other identification data obtained under the Programme, including where the Operator receives relevant information, requests, notifications, demands or other communications from competent governmental authorities, for the purposes of preventing and addressing the unlawful use of the Programme and related financial services, and protecting the rights and legitimate interests of the Operator, its partners and other persons;
- protection of the rights and legitimate interests of the Operator, including the handling of complaints and the conduct of disputes.

Automated decision-making producing legal effects concerning you is not carried out on the basis of segmentation for marketing purposes.

12.6. Consent to receive messages and to the engagement of Marketing operators

By acceding to these Terms, you consent to receive from the Operator and its partners messages of an informational, advertising and marketing nature by email, SMS, push notifications, in-app messages, messengers and telephone calls.

You agree that, in order to create and deliver such messages, the Operator may engage third parties - marketing operators, advertising agencies, providers of messaging platforms and CRM/CDP systems, call centres, web analytics and targeted advertising service providers (the “Marketing operators”) - and may transfer to them the volume of data required for that purpose, including: surname and given name, email address, mobile telephone number, device and application identifiers, country of residence, language of communication, status in the Programme, composition of services purchased, date of last update and data on interaction with previously delivered messages.

Marketing operators act solely on the instructions and under the control of the Operator, on the basis of data processing agreements concluded with them, and may not use the transferred data for their own purposes, transfer it to third parties, combine it with other data sets or retain it after termination of the relevant engagement.

The Operator transfers to Marketing operators the minimum necessary volume of data and does not transfer to them biometric data, identity document data, the e-Residency IIN, AML/KYC screening results or source-of-funds information.

You may opt out of receiving advertising and marketing messages at any time - via the opt-out link in the message, the mobile application settings, or in writing to support@eresidency.gov.kz. An opt-out is processed within no more than 3 (three) business days, results in the exclusion of your data from the data sets transferred to Marketing operators, and does not affect the provision of the Services, their scope or their cost.

An opt-out from advertising messages does not extend to service notifications (application statuses, update requirements, changes to the Terms and tariffs, security matters), which are sent pursuant to clause 16.1 throughout the term of these Terms.

12.7. Cross-border transfer

The Operator is a company incorporated under the applicable law of the AIFC. You expressly acknowledge and agree that the provision of the Services is impossible without the transfer of personal data outside the AIFC jurisdiction, including:

- to the territory of the Republic of Kazakhstan - to governmental authorities and information systems (the MIA RK, the State Database of Individuals and other registers in accordance with legislation), Partner Banks, mobile network operators, insurance and acquiring organisations;
- to other jurisdictions - to providers of identity verification, sanctions screening and fraud prevention services, cloud infrastructure providers, and Marketing operators (clause 12.6), whose categories and jurisdictions are set out in Annex 2.

Transfers are made on the basis of your express consent and/or the necessity of performing the contract, provided that the Operator has concluded with each recipient-processor a data processing agreement providing for a level of protection equivalent to the requirements of the AIFC Data Protection Regulations. The current list of categories of recipients and jurisdictions is published in the Privacy and Data Processing Policy.

The Operator does not transfer personal data to jurisdictions classified as high-risk in accordance with Annex 3, except in cases expressly provided for by applicable law.

12.8. Restriction on dissemination

Dissemination of your personal data in publicly available sources is not envisaged. The Operator does not sell personal data to third parties.

12.9. Rights of the data subject

You have the right to: obtain confirmation of the fact of processing and information about it; obtain access to your data; request the correction of inaccurate or incomplete data; request the deletion of

data, other than data subject to mandatory retention; object to processing for particular purposes, including marketing; and withdraw the consent given. Requests should be sent to support@eresidency.gov.kz; a response is provided within 30 (thirty) business days.

12.10. Term of consent and withdrawal

The consent is valid for the term of these Terms and thereafter for the mandatory AML/KYC record retention period established by the applicable AIFC AML/CFT rules, calculated from the date of termination of the business relationship.

You may withdraw your consent to the processing of personal data in full by sending a written application to support@eresidency.gov.kz. Full withdrawal of consent entails the complete cessation of the provision of the Services, since the processing of personal data is a necessary condition for their provision.

Withdrawal of consent to receive advertising and marketing messages (clause 12.6) is effected separately, does not require written form and does not entail cessation of the provision of the Services.

Withdrawal of consent has no retroactive effect and does not affect: (i) the Operator's obligations to retain AML/KYC data; (ii) the lawfulness of processing carried out prior to withdrawal; (iii) data previously transferred to governmental authorities, Partner Banks, crypto exchanges and other recipients, whose further processing is governed by their own policies and their contracts with you. Withdrawal of consent is not a ground for the refund of fees paid and does not annul an assigned e-Residency IIN.

SECTION 13

LIABILITY AND DISCLAIMER

13.1. The Services are provided strictly on an “as is” and “as available” basis, without any warranties, express, implied or statutory, to the maximum extent permitted by applicable laws or regulations. Without limiting the foregoing, we bear no responsibility for:

- i) refusal by the MIA RK to issue a digital identity document with an e-Residency IIN;
- ii) refusal by Partner Banks or a crypto exchange to open and/or service an account or card;
- iii) downtime, unavailability or malfunction of third-party services or government information systems;
- iv) losses, damage or delays caused by you, your representatives or third parties.

13.2. We bear no liability for any indirect, consequential, punitive, special or incidental damages, including (without limitation) loss of profit, revenue, business opportunities, goodwill, reputation or data, arising in contract, tort (including negligence) or otherwise, even if we have been advised of the possibility of such damages.

13.3. All fees paid by you are non-refundable.

13.4. Indemnity. You agree to indemnify us against any liabilities, losses and expenses (including legal fees and any fines, charges and/or penalties imposed by any regulator) reasonably incurred in connection with any claims, demands or losses arising out of or in connection with your breach and/or our performance of this Agreement or any of our Policies, or your breach of any law, rule or regulation, or the rights of any third party.

13.5. Nothing in these Terms excludes or limits liability that cannot lawfully be excluded or limited under applicable law, including liability for fraud, fraudulent misrepresentation, gross negligence, wilful misconduct, or death or personal injury caused by negligence.

SECTION 14

FORCE MAJEURE

14.1. General rule. Neither Party shall be liable for any delay in or failure to perform its obligations under these Terms if and to the extent that such delay or failure results from events, circumstances or causes beyond its reasonable control ("Force Majeure").

14.2. Examples of force majeure. Force Majeure includes, among other things:

- a) failures or interruptions in the operation of government information systems and/or registers;
- b) sanctions, embargoes or trade restrictions;
- c) war, armed conflict, civil unrest or terrorism;
- d) epidemics, pandemics or public health emergencies;
- e) large-scale cyber incidents, including DDoS attacks;
- f) power outages or network failures;
- g) acts, omissions or restrictions of regulators or other competent authorities;
- h) natural disasters, natural phenomena or acts of nature.

14.3. Effect of force majeure. Where a force majeure event prevents or delays a Party's performance of its obligations, performance of the affected obligations is suspended for the duration of the force majeure event. The affected Party must promptly notify the other Party of the event and use reasonable efforts to mitigate its consequences.

SECTION 15

TERM, AMENDMENTS AND TERMINATION

15.1. Entry into force and term. These Terms take effect from the moment of your acceptance (including by registering for, accessing or using the Services) and remain in force until terminated in accordance with this Section.

15.2. Amendments. We may amend these Terms, the Tariffs or related Rules unilaterally by publishing an updated version in the mobile application and/or on our website. You will be notified of material changes through the mobile application, by email or by other appropriate means. Your continued use of the Services after such publication or notification will constitute your acceptance of the updated version.

15.3. Termination at your initiative. You may stop using the Services at any time and request deletion of your Account. However, such deletion will be subject to statutory obligations, including AML/KYC record retention. You may not cancel your Account in order to avoid an investigation or to evade payment of amounts due. Upon cancellation, you authorise us to cancel or suspend any pending transactions and to withhold the related funds until settlement and refund periods have expired.

15.4. Suspension or termination at our initiative. We may immediately suspend or terminate your access to the Services and/or your Account, with or without notice, if:

- a) you breach these Terms or any applicable laws;
- b) your activity, in our reasonable opinion, presents an elevated regulatory compliance, fraud or reputational risk; or
- c) such suspension or termination is required or recommended by a regulatory, supervisory, law enforcement, investigative, prosecutorial, judicial or other competent authority, or is necessary to comply with any request, demand, order, resolution or other lawful requirement of such authority;

- d) we detect that you have transferred your Account or granted access to your Account to any third party in breach of clause 4.2 of these Terms.

15.5. Survival. Any provisions of these Terms that are intended to survive termination (including but not limited to provisions on liability, indemnity, intellectual property, confidentiality and data retention) remain in full force and effect after termination.

SECTION 16

ELECTRONIC COMMUNICATIONS AND SIGNATURE

16.1. Delivery of notices. All notices and communications required or permitted under these Terms may be sent by us via in-app messages, email, SMS or push notifications. Such communications are deemed received by you at the moment of transmission, unless proven otherwise. The sending of advertising and marketing messages is governed by clause 12.6.

16.2. Validity of electronic execution. Your consents, acceptances, instructions and confirmations given through the application and confirmed by one-time passwords (OTP), liveness checks, NFC verification or other secure electronic methods are deemed to have the same legal force as those made in writing and signed by hand, unless applicable law or regulation expressly requires a stricter form.

16.3. Consent to electronic form. By accepting these Terms, you acknowledge and agree to receive all communications, notices and records in electronic form.

SECTION 17

GOVERNING LAW AND DISPUTE RESOLUTION

17.1. Governing law. These Terms and any non-contractual obligations arising out of or in connection with them are governed by and construed in accordance with the law of the AIFC, without regard to conflict-of-law principles.

17.2. Jurisdiction. Any disputes, disagreements or claims arising out of or in connection with these Terms, including any questions regarding their existence, validity or termination, are subject to the exclusive jurisdiction of the Court of the Astana International Financial Centre (the AIFC Court).

17.3. Pre-action complaint procedure. Before filing a claim with the AIFC Court, you must send us a written complaint to support@eresidency.gov.kz. We will consider the complaint and provide a response within thirty (30) business days of its receipt. Only after the expiry of that period, or where the complaint cannot be resolved to the mutual satisfaction of the Parties, may you apply to the AIFC Court.

SECTION 18

MISCELLANEOUS

18.1. Entire agreement. These Terms, together with all incorporated annexes, policies or supplements, constitute the entire agreement between you and us in respect of their subject matter and supersede all prior discussions, arrangements, understandings or agreements (whether oral or written).

18.2. No agency. Nothing in these Terms shall be construed as creating any agency, partnership, joint venture, employment or fiduciary relationship between you and us. Neither Party has the right to bind the other in any way without prior written consent.

18.3. Severability. If any provision of these Terms is held to be invalid, unlawful or unenforceable under applicable law, that provision shall be severed and the remaining provisions shall continue in full force and effect.

18.4. Assignment. We are entitled to assign or transfer our rights and obligations under these Terms, in whole or in part, to any successor without your prior consent. You may not assign or transfer your rights and obligations under these Terms without our prior written consent, and any attempted assignment in breach of this clause shall be void.

18.5. Language. These Terms are drawn up in English and Russian. Translations into other languages may be provided solely for convenience. In the event of any inconsistency or discrepancy between the English and Russian versions or a translation into any other language (if applicable), the English version shall prevail.

SECTION 19

FEEDBACK, ENQUIRIES AND COMPLAINTS

19.1. Contacting us. If you have any feedback, questions or complaints, you may contact us at support@eresidency.gov.kz or by submitting a support request through the application. To enable us to handle your request efficiently, please state your full name, address and any information required to identify you, your digital residency account and the transaction or issue in question.

19.2. Filing a complaint. When filing a complaint, you should clearly state the reason for the complaint, your preferred means of resolution and any other information you consider important. We will acknowledge receipt of your complaint if it is sent by email to support@eresidency.gov.kz. An authorised compliance officer will consider your complaint impartially, taking into account both the information you have provided and any information available to us.

19.3. Resolution of a complaint. Within thirty (30) business days of receipt of your complaint, the compliance officer will consider all matters raised and send you a written resolution notice by email (the “Resolution Notice”), which will either:

- a) resolve your complaint in accordance with your wishes;
- b) reject your complaint, stating the reasons for rejection; or
- c) propose an alternative resolution.

In exceptional circumstances beyond our reasonable control, if we are unable to resolve the matter within thirty (30) business days, we will send you a response setting out the reasons for the delay and a final deadline for resolving the matter, which may not exceed sixty (60) business days from our receipt of your complaint.

19.4. Effect of resolution proposals. Any resolution proposal made by us will take effect only if accepted by you. A settlement proposal does not constitute an admission by us of liability, fault or wrongdoing in respect of you and/or the subject matter of the complaint.

ANNEX 1

TARIFFS AND FEES

1. Tariffs and fees under the e-Residency programme

No.	Service	Price	Frequency
Service 1.	AML/KYC screening and identification, obtaining a digital identity document with an e-Residency IIN, eSIM service*	**299 USD**	First year (one-off on joining the programme) (eSIM - 30 days**)
Service 2.	Annual data update: verification of identification details, confirmation of source of funds, profile update (AML/KYC), and other items required for status renewal	**229 USD**	Annually, starting from the second year
Service 3.	Repeat AML/KYC screening upon re-application after a refusal	**299 USD**	On request, no earlier than 30 calendar days after the refusal

* Verum Payments Limited is entitled to enter into agreements granting discounts on the cost of services with partners distributing its services, specifying the exact discounted price and the volume limit of services provided under the discount.

** The price under item 1 additionally includes 30 (thirty) calendar days of eSIM service from the date of eSIM activation. Further use of the eSIM is at the discretion of the e-Resident and is paid for separately.

2. Preferential terms for advance payment of the “Annual data update” service

The service “AML/KYC screening and identification, obtaining a digital identity document with an e-Residency IIN” is paid separately in the amount of **299 USD** upon joining the programme.

Where several periods of the “Annual data update” service are paid in advance in a single payment, a preferential discounted tariff applies:

Price with advance payment for Service 2 together with Service 1:		One year of updating (2 years of programme participation in total)	Two years of updating (3 years of programme participation in total)
Service 1.	AML/KYC screening and identification, obtaining a digital identity document with an e-Residency IIN, eSIM service*	**449 USD**	**549 USD**
Service 2.	Annual data update: verification of identification details, confirmation of source of funds, profile update (AML/KYC), and other items required for status renewal*		
	Price without advance payment	**528 USD**	**757 USD**
	Discount (USD)	**79 USD**	**208 USD**
	Discount (%)	**15%**	**27%**

- The preferential tariff applies solely where all payable periods are paid in a single advance payment.

Consequences of failing to complete the annual update

If a Programme participant fails to complete the annual data update procedure within the established period in accordance with the chosen format, the participant's status in the Company's database is switched to inactive until the update procedure is fully completed.

Switching the status to inactive entails suspension of the services provided directly by the Company, including but not limited to: access to the personal account and the Company's digital platform, support services, and other Company services whose operation is conditional on a valid e-Resident status.

Switching the status to inactive does not entail annulment of the participant's IIN.

The participant's relationships with other partners of the Company are governed by the contracts concluded between them and by applicable law; such partners take their own decisions based on the date of the last data update and the change in the e-Resident's status, in accordance with their own terms of service. The Company is entitled to notify partners of the change in the participant's status and of the date of the last data update.

Restoration of status and resumption of the Company's services take place no later than 3 (three) business days from the successful completion of the update procedure.

Note: The Company is entitled to amend tariffs and fees by giving the participant no less than 30 (thirty) calendar days' notice before the changes take effect, by sending a notice to the participant's contact email address.

ANNEX 2

DATA RECIPIENTS, JURISDICTIONS AND GROUNDS FOR TRANSFER

List of categories of personal data recipients, the scope of data transferred, jurisdictions and legal grounds for transfer in accordance with Section 12 of these Terms.

Category of recipient	Scope of data transferred	Jurisdiction	Ground for transfer
Governmental authorities of the Republic of Kazakhstan: MIA RK, the State Database of Individuals and other registers	Identification data, biometric data	Republic of Kazakhstan	Consent + statutory requirement
Partner Banks and crypto exchanges	Minimum necessary identification data, e-Residency IIN	Republic of Kazakhstan	Consent + performance of contract
Mobile network operators	Data required for the issuance and servicing of the eSIM	Republic of Kazakhstan	Consent + performance of contract
Insurance companies	Data required to arrange a medical insurance policy	Republic of Kazakhstan	Consent
Acquiring providers and payment systems	Payment and identification data	Republic of Kazakhstan, EU, United Kingdom	Performance of contract
Providers of verification, sanctions screening and fraud prevention services	Identification and biometric data, screening results	United Kingdom, EU, USA, Republic of Kazakhstan	Consent + DPA
Cloud infrastructure and hosting providers	All categories of processed data	EU, Republic of Kazakhstan	DPA
Partners of the Operator for the purpose of creating individual offers	Contact details, country of residence, status in the Programme	Republic of Kazakhstan	Consent (clause 12.5)
Marketing operators: email/SMS/push messaging platforms, CRM/CDP systems, advertising agencies, call centres, web analytics services	Contact details, device and application identifiers, country of residence, language, status in the Programme, composition of services, message interaction data. Biometrics, document data, the e-Residency IIN and AML/KYC results are not transferred	EU, United Kingdom, USA, Republic of Kazakhstan	Consent (clause 12.6) + DPA

The Operator concludes with each recipient-processor a data processing agreement providing for a level of protection equivalent to the requirements of the AIFC Data Protection Regulations. The current version of this list is published in the Privacy and Data Processing Policy.

ANNEX 3

HIGH-RISK JURISDICTIONS

The Operator of the e-Residency Kazakhstan programme applies a risk-based approach in accordance with AIFC/AFSA AML/CFT requirements and FATF recommendations.

For the purposes of the Programme, high-risk jurisdictions include:

- jurisdictions on the FATF list of High-Risk Jurisdictions Subject to a Call for Action - applications from citizens and residents of such jurisdictions are not accepted;
- jurisdictions on the FATF list of Jurisdictions under Increased Monitoring;
- third countries included by the European Commission in the list of high-risk countries under Delegated Regulation (EU) 2016/1675 (as amended), including the Russian Federation;
- other jurisdictions classified as high-risk by the Operator's internal risk model, taking into account the applicable sanctions regimes of the UN, the EU, OFAC (USA), UK HMT and the Republic of Kazakhstan.

The lists apply in the version in force on the date the application is considered.

Applications from citizens and residents of high-risk jurisdictions are accepted for consideration and are subject to enhanced due diligence (EDD), including in-depth identity verification, confirmation of source of funds and source of wealth, and sanctions list screening. Risk assessment is carried out individually for each applicant.

Submission of an application and payment of fees do not guarantee approval and do not create any obligation on the Operator to provide services.

Services will be refused to persons included on sanctions lists, to persons acting on behalf of or in the interests of such persons, and in other cases where this is required by applicable law or the Operator's internal policies. Processing times for applications subject to EDD may exceed standard timeframes.

The Operator is entitled to refuse to provide services without giving reasons where disclosure of the reasons is prohibited by applicable law.

The Operator does not engage providers of verification, screening or cloud infrastructure services that are registered in, or process personal data in, jurisdictions classified as high-risk in accordance with this Annex.