Trust Service Practice Statement (TSPS) of

AlfaTrust Certification S.A.

Table of contents

1. INTRODUCTION

Purpose

The **Trust Service Practice Statement (TSPS)** comprehensively describes the practices, policies, and procedures used by AlfaTrust Certification S.A. (hereinafter referred to as the Trust Service Provider – TSP) for the provision of trust services. The purpose of this document is to ensure transparency regarding the provider's mode of operation, in accordance with the applicable national and European legislation, in particular Regulation (EU) No. 910/2014 (the eIDAS Regulation) and the relevant European standards. The TSPS meets the requirements of Articles 19 and 24(2) of the eIDAS Regulation, as well as the requirements imposed by ETSI standards (such as EN 319 401, EN 319 411-1, EN 319 421) and national legislation (ADR Order no. 449/2017 and subsequent regulations).

Through this statement, AlfaTrust Certification S.A. sets out the commitments undertaken and the controls implemented in order to provide qualified trust services with a high level of security and compliance. The TSPS explains the roles and responsibilities of all parties involved, the operational requirements for the issuance and management of digital certificates, the security measures applied, as well as the approach to risk management, security incidents, data protection, and service continuity.

The document also serves as a reference for AlfaTrust's internal policies (e.g., Information Security Policy – ATC-PS-18 "Information Security Management," Code of Practices and Procedures – CPP, Certification and Electronic Seal Policy, Time-Stamping Policy, etc.), without reproducing them in full, but indicating how they are reflected in operational practices.

Note: The TSPS is a publicly available document, published and updated periodically, accessible to users and interested parties, and remains in force until a new approved version is issued. Any new version of the TSPS will be subject to internal approval and notified to the supervisory body (the Romanian Authority for Digitalization – ADR), after which it will be published to inform all

interested parties (details on review and updating are provided in the *Review and Update* section of this document).

2. SCOPE OF APPLICATION

This Trust Service Practice Statement (TSPS) applies to all trust services provided by AlfaTrust Certification S.A., as well as to all participants in the company's public key infrastructure (PKI). The scope covers: AlfaTrust personnel and structures (including the **Certification Authority – CA**, the **Registration Authority – RA**, the **Time Stamping Authority – TSA**, and, where applicable, the **Validation Authority – VA**), contractual partners (e.g., distributors, delegated external registration authorities), end-users (holders of qualified certificates, whether natural or legal persons), as well as relying parties that depend on the certificates issued (partner entities/relying parties).

The TSPS establishes the rules and practices governing the use of AlfaTrust certificates and trust services, in particular qualified certificates, ensuring that they can be used under maximum security conditions in any legally permitted context.

The TSPS covers the qualified trust services provided by AlfaTrust (listed in the following section), including "advanced" variants of these services, where applicable. The document also describes the applicability of certificates issued by AlfaTrust in different usage scenarios. Qualified digital certificates issued under the authority of AlfaTrust are of general use and may be applied anywhere within the European Union and internationally, without being limited to a specific sector or business environment.

According to the applicable legislation, an electronic signature created with a qualified certificate issued by AlfaTrust is recognized as valid regardless of the country in which the certificate was issued or where the user is located, provided that both the certificate and the signature comply with the relevant legal requirements. Qualified certificates issued by AlfaTrust may also be used to generate advanced (non-qualified) electronic signatures or seals; however, in this case, the legal value will correspond to the "advanced" level of the signature/seal (not qualified).

By default, qualified certificates issued by AlfaTrust have a general scope of use (purposes: electronic signature, electronic seal, authentication, encryption) and are not restricted to a single application. Any specific limitations of use will be explicitly communicated in the terms and conditions or in the certificate itself (through its extensions). In the absence of such limitations,

relying parties may use AlfaTrust certificates to verify electronic signatures/seals in any legal context where such signatures or seals are accepted.

3. TRUST SERVICES PROVIDED

AlfaTrust Certification S.A. is qualified as a Qualified Trust Service Provider (QTSP) and offers the following trust services, in accordance with the eIDAS Regulation and national legislation:

- Qualified electronic signature creation service – consisting of the issuance of qualified certificates for electronic signatures intended for natural persons (including authorized representatives of legal entities). This service enables the generation of qualified electronic signatures with the same legal effect as handwritten signatures, as well as advanced electronic signatures when the issued certificates are used without a qualified device. Certificates for electronic signatures may be stored on secure signature creation devices (e.g., qualified USB tokens, smart cards) or, in the case of the remote signing solution (AlfaSign Cloud), they may be centrally hosted on an HSM module administered by AlfaTrust (subject to activation conditions by the certificate holder).
- Qualified electronic seal creation service – consisting of the issuance of qualified certificates for electronic seals intended for legal entities (organizations). These certificates may be used by entities to apply qualified electronic seals to documents or data, thereby ensuring their origin and integrity. Similar to electronic signatures, seal certificates may be deployed on cryptographic devices held by the client or hosted remotely within AlfaTrust's infrastructure, allowing the application of either advanced or qualified electronic seals, depending on the mode of use.
- Qualified electronic time-stamping service – consisting of the generation and provision of qualified electronic timestamps through the AlfaTrust Time Stamping Authority (TSA). This service provides reliable dating and timing of electronic documents or transactions, using a synchronized and secured time source. The issued timestamp includes the TSA's electronic signature and complies with the applicable standards (e.g., RFC 3161 and ETSI

EN 319 421 for timestamping policies), ensuring that at the indicated moment the document content had not been altered.

Note: AlfaTrust also provides supporting technical services required for the operation of the above-mentioned services, such as certificate status validation services (OCSP – Online Certificate Status Protocol and CRLs – Certificate Revocation Lists), as well as user support and consultancy regarding the integration of electronic signatures. The certificate validation service (Validation Authority, if offered separately) complies with eIDAS requirements for qualified electronic signature validation. However, in practice, the status of certificates issued by AlfaTrust is automatically, freely, and in real time verified through the OCSP/CRL services made available by the provider.

All services provided are subject to the present practices and security policies described in this TSPS.

4. TECHNICAL AND ORGANISATIONAL INFRASTRUCTURE

PKI (Public Key Infrastructure) architecture: AlfaTrust's technical system is structured on a multi-level hierarchy of certificate authorities (**CAs**) to ensure both cryptographic security and scalability of services. At the top of the hierarchy is a **root CA** (**AlfaTrust Root CA),** maintained in a strictly secure environment and operated *offline* (isolated from the network), whose private key is used exclusively to sign the certificates of subordinate CAs and their revocation lists. At the next level (level 1) there are **internal subordinate CAs (on-site SubCAs),** which directly issue qualified certificates to end-users (natural and legal persons) and timestamp certificates. There are distinct CAs for different types of certificates (e.g., a CA dedicated to qualified electronic signatures, a CA for qualified electronic seals, a CA for non-qualified certificates used for advanced electronic signatures or authentication, etc.), depending on the related certification policies. A possible level 2 (off-site CAs) may exist for special implementations (e.g.: sub-CAs hosted at certain large customers, for the issuance of advanced certificates not qualified in their

environment); such Level 2 CAs are signed by AlfaTrust's internal CAs and operate under the control of AlfaTrust policies.

Key components and equipment: All sensitive infrastructure operations (key generation, signing certificates and revocation lists, issuing timestamps) are performed on highly secure hardware cryptographic modules (**HSMs**). The HSMs used comply with at least the requirements of the *FIPS PUB 140-2 Level 3* standard (or equivalent Common Criteria EAL4+), ensuring the protection of private keys against unauthorized access. CAs' private keys never leave the HSM in unencrypted form; Dual control and secret sharing mechanisms (K-of-N schemes) are also implemented for key operations such as HSM activation or key backup, so that no individual person can access or activate critical components on their own. HSMs are installed in secure data centers, being physically and logically protected.

IT systems and software: AlfaTrust uses redundant IT systems and specialized **PKI software** for certificate lifecycle management (certificate requests, issuance, revocation, revocation list and OCSP server management, timestamp issuance, etc.). The servers that host these services run hardened operating systems and security applications that comply with industry standards. There is strict separation between production and test environments, as well as network segmentation to isolate critical components (e.g., AC servers and HSMs are in a separate secure network with restricted access). Critical data (e.g. audit logs, certificate database) is replicated in real time on backup systems.

Primary and secondary data center: AlfaTrust's infrastructure is hosted in a **main data center**, with adequate physical and environmental security conditions (biometric access control, video surveillance, uninterrupted power supply – UPS and generators, air conditioning systems and fire detection/extinguishing, etc.). In addition, to ensure continuity of services, there is a **secondary data center** located at an alternative location, at a sufficient distance from the primary center not to be affected simultaneously by the same regional disaster. It functions as a disaster recovery site and takes over critical operations in the event of the unavailability of the primary center. Critical data (including encrypted backups of keys and databases) is kept synchronized

or through periodic replication to the secondary location. Backup **and restore** procedures provide for full weekly and daily incremental backups, stored both on-site and off-site (in the secondary location), in secure containers, in order to be able to fully restore the systems in case of need.

Distribution and Registration Network: AlfaTrust has designated one or more **Registration Authorities (IAs)** responsible for validating the identity of certificate applicants. AI can even be AlfaTrust's internal staff (for applications processed at AlfaTrust's premises) and/or authorized partners (distributors, registry officers) contractually empowered to perform end-user registration on behalf of AlfaTrust. Regardless of the formula, all registration authorities follow the same identification policies and procedures established by AlfaTrust (verifying identity documents, registering the necessary information, obtaining user consent, etc.). The information and documents collected by the AI are securely transmitted to the relevant issuing CA.

Certificate database and status services: As part of its infrastructure, AlfaTrust maintains an **up-to-date database of** issued certificates, which includes information about the status of each certificate (valid, revoked, expired, etc.). This database is the basis of the status validation services offered (revocation lists – CRLs, and real-time CPVO responses). Any revoked certificate is immediately entered in the database and communicated through the public revocation lists and the CPVO server, within a maximum of 24 hours from the revocation request (in practice, usually much faster). AlfaTrust's OCSP server is permanently available, allowing third parties to obtain information about the validity of any issued certificate free of charge, throughout its lifetime and for a period after expiration.

Additional information: The technical infrastructure is designed and operated in accordance with the security requirements of ETSI EN 319 401 and ETSI EN 319 411-1 standards (including infrastructure and key management requirements), respectively ETSI EN 319 421 for the timestamp service. All critical equipment is subject to regular maintenance, security updates, and 24/7 monitoring for prompt detection of any incidents or anomalies.

5. INTERNAL POLICIES AND SECURITY CONTROLS

AlfaTrust Certification S.A. has a solid framework of **internal security policies and procedures** that govern all aspects of the provision of trust services, in accordance with an implemented Information Security Management System (**ISMS).** Internal policies are aligned with international standards (such as ISO/IEC 27001) and the specific requirements of the ETSI Standards for Trust Service Providers. Among the relevant internal documents, we mention: **Information Security Policy - ATC-PS-18 "Information Security Management"** (which defines the objectives and general security measures), AlfaTrust'**s Code of Practice and Procedures (CPP)** (internal document detailing the operational and security processes for all services), **Certification** Policy for issued certificates (specifying the conditions and criteria for the issuance/use of certificates, including the certificate profile and the OIDs of certification policies) and **the Timestamping Policy** (which sets out the specific rules for the timestamp service). These policies are maintained and approved by AlfaTrust's management, and are the basis for compliance with legal requirements. The following is a summary of AlfaTrust's approach to security and organizational controls:

- **Cryptographic measures:** The generation of cryptographic key pairs for CAs and TSAs is performed in a controlled environment, using algorithms and parameters considered secure at the moment (e.g.: RSA 2048/3072 or ECC curve P-256/P-384 or SHA-256 hash functions). Private keys of authorities and seal/signature devices are protected on FIPS 140-2 Level 3 compliant HSMs. Key lifetime procedures (generation, distribution, backup, end-of-life destruction) documented in the CPP are applied. The signature keys of the certificate authorities have a limited validity, being renewed periodically according to the policy (e.g. every 5 years), and the change of keys is planned in such a way as not to affect the continuity of the validation of the issued certificates (there are validity overlaps and prior notifications to users, as appropriate).

- **Physical security:** Critical equipment (AC servers, HSMs, database servers) are located in secure spaces with strict physical access control. Only authorized personnel have access to the secure area, based on an access card. The spaces are monitored by video and guarded. There are fire detection and extinguishing systems (e.g.: smoke sensors, inert extinguishing gas) and redundant air conditioning systems to maintain optimal environmental parameters. Protection against floods or other environmental factors is also provided (critical equipment is mounted in racks raised from the ground, etc.). Storage media containing sensitive information (e.g., backup drives, discarded hard drives) are handled and destroyed according to procedures to prevent information leakage.
- **Procedural and personnel controls:** AlfaTrust has defined clear trust functions within the organization, avoiding excessive concentration of access to critical operations in the hands of a single person. The principles *of segregation of duties* and *need-to-know* are implemented. Certain important operations (e.g.: generation of AC keys, activation of HSM, approval of certification requests) require the simultaneous presence of two or more authorized persons, each with a distinct role (dual control). Personnel in critical roles (registry officers, system administrators, security officers, internal auditors, etc.) undergo pre-employment checks (background checks, experience and qualifications) and sign confidentiality agreements. Also, all employees and collaborators involved in trust services periodically follow training and awareness programs in the field of information security, data protection and eIDAS regulations. Any violation of security policies by staff entails disciplinary sanctions, according to internal policies.
- **Security of IT and network systems:** All of AlfaTrust's IT systems are configured with appropriate cybersecurity measures. This includes the use of network border **firewalls**, internal network segmentation, intrusion detection/prevention systems (IDS/IPS), as well as continuous monitoring of security logs. Critical systems run only essential services, minimizing the attack surface, and security updates (patches) are

applied in a controlled, timely manner. Logical **access control** mechanisms are used based on strong password authentication and, where possible, two-factor authentication for administrators. Administrator access to servers and HSMs is logged and restricted to a secure console.

- **Event logging and auditing:** AlfaTrust maintains detailed logs for all relevant events in the system: certificate issuances, revocation requests, issuance of CRL lists and OCSP responses, administrator access, security alarms, etc. The logs are protected against modification and are kept for an appropriate duration (minimum 10 years for events related to qualified certificates, according to legal requirements). These records can serve as evidence in the investigation of security incidents or in possible legal proceedings. Regular **internal audits** are also carried out to verify compliance with security procedures. According to Art. 20 of eIDAS and national legislation, AlfaTrust is also subject to an **external compliance audit** every 24 months or whenever necessary (e.g. in case of major changes or expansion of services). The external audit is carried out by an accredited conformity assessment body, which verifies compliance with all eIDAS requirements (including those related to security, processes, personnel, data protection, etc.) and applicable ETSI standards. Audit reports are submitted to the supervisory body (ADR) and non-compliances, if they occur, are remedied promptly.

Continuity and disaster recovery: AlfaTrust has implemented a **Business Continuity Plan (BCP)** and a **Disaster Recovery Plan (DRP),** which cover scenarios of major unavailability of key systems or personnel (e.g., natural disasters, serious cybersecurity incidents, extended power outage, etc.). These plans provide for procedures for moving to the secondary location, restoring backup systems and resuming operations in the shortest possible time, with priority on essential services such as certificate validation and timestamping. Disaster *recovery exercises* are carried out periodically to test the effectiveness of the plans and the preparation of the team. There is also a specific plan for the controlled termination of the business in the unlikely event of permanent termination of AlfaTrust's services (see section *Termination of services*).

- **Confidentiality and integrity:** Any sensitive information held by AlfaTrust (including customer personal data, public keys, audit logs) is treated confidentially and in accordance with the principle of integrity. Employees have access to data according to their roles and only for the purpose of performing their job duties. Data transmission is done through secure channels (TLS encryption for external communications, VPN virtual private networks for links between locations). The Security Policy expressly prohibits unauthorized disclosure of customer data or the security configuration of systems. The integrity of the certificates and signatures/marks issued is protected by robust cryptographic mechanisms and strict adherence to operating procedures.

Through all these controls and policies, AlfaTrust ensures that the level of security is proportionate to the associated risks and that the trust services are provided in a safe, reliable manner and in compliance with the applicable legal and standard requirements.

6. RESPONSIBILITIES OF THE PARTIES INVOLVED

In order to ensure the proper functioning of the certification ecosystem, the DPSI defines the main obligations and responsibilities of each category of actors involved in the provision and use of AlfaTrust trust services. These responsibilities are assumed by contracts, terms and conditions or applicable policies, so that each party understands its role and expectations:

Trust Service Provider (Certification Authority – CA): AlfaTrust Certification S.A., as a qualified CA, has the obligation to comply with all legal requirements in force and commitments to users. The main responsibilities include: (1) proper verification of the identity of the applicants for certificates before issuance (directly or remotely by using video means according to the Procedure adopted by the Decision of the President of ADR no. 564/2021 or other subsequent normative act); (2) issuing certificates in accordance with stated policies, (3) ensuring the availability of certificate status check mechanisms (CRL/CPVO) throughout their validity, (4) immediately applying revocations upon request or when good reasons arise; (5) maintaining the security of CA and TSA private keys, recording and retaining relevant service information (logs) for the necessary period;

(6) as well as the protection of users' personal data. The CA must notify the supervisory authority (ADR) in advance of any significant change in the qualified services provided or of the intention to cease operations. It also undertakes to promptly remedy any non-compliance identified as a result of the compliance audit.

- **Registration Authority (IA):** IA (internal or authorized external partner) is responsible for identifying and validating potential certificate holders in accordance with AlfaTrust's procedures. This involves verifying the original identity documents of natural persons and/or the incorporation and power of attorney documents for legal entities, collecting the necessary data (full name, CNP or equivalent identifier, address, legal representative, etc.), informing the data subject about the processing of his or her personal data (in accordance with art. 13 of EU Regulation 679/2016 – GDRP) and for the terms and conditions of the service. AI must ensure the accuracy of the information entered in the certification application and the secure transmission of this data to the CA. The Registration Authority has the obligation of confidentiality towards the processed data and compliance with AlfaTrust's security policies. In addition, AI provides support to applicants by explaining their rights and obligations as certificate holders. In the case of remote identification (if used), AI must follow the special procedures approved (see section *Remote identification*).

Timestamping Authority (TSA): TSA AlfaTrust is responsible for issuing accurate and secure timestamps. The TSA is required to maintain the synchronization of the internal time source with the Universal Time Standard (UTC) by means of precisely calibrated clocks (e.g. NTP servers linked to standard time sources). The TSA must ensure that each timestamp issued correctly reflects the time of issuance and is signed with the corresponding TSA's private key, which is under the sole control of AlfaTrust. The TSA is also responsible for keeping a log of all timestamps issued, in order to demonstrate, if necessary, the exact time of their issuance and the integrity of the service. In case of compromise or suspicion of compromise of the TSA key, it has the

obligation to immediately cease issuing timestamps with that key and to inform users and the supervisory authority, generating if necessary a new pair of keys and a new TSA certificate.

- **Validation Authority (certificate status verification service)** *(if offered separately as a qualified service):* The Validation Authority (AV) is responsible for providing third parties with validation reports of electronic signatures or certificates, according to the eIDAS Regulation. In the context of AlfaTrust, the validation functionality is mainly carried out through OCSP/CRL (automated); and involves verifying the specific elements provided by law (validity of the certificate, integrity of the signature, non-revocation at the time of signing, identity of the signatory, etc.) and providing a binary answer, **true or false,** regarding the validity of a signature, accompanied by a proof (qualified electronic seal of the validation report). The VA has the obligation of objectivity and accuracy, as well as of keeping validation logs.
- **End User (Certificate Holder): Each certificate holder** *(natural or legal person)* has a series of obligations assumed by the contract/terms of use signed with AlfaTrust. These responsibilities include, but are not limited to: (1) providing accurate and complete information during registration (any relevant changes, such as name changes, must be communicated in a timely manner for re-issuance or updating if applicable); (2) knowing, understanding and complying with the terms and conditions of use of the certificate and the secure device (token) provided; (3) the use of the certificate only for permitted purposes (e.g. a qualified signature certificate is used only by the natural person holder for signing, not by other people); (4) maintaining the security of the private key associated with the certificate – which involves keeping the qualified device and the PIN/password safe; (5) not sharing them with third parties and immediately reporting to AlfaTrust any suspicion of compromise (loss/theft of the token, disclosure of the password, etc.). The end user is responsible for requesting the revocation of the certificate without delay if the entered identity data becomes inaccurate or if the security of the private key is compromised. The end-user must also check the validity and status of their certificate

before using it for signing, especially if they know that there would have been grounds for revocation. In relation to third parties, the holder consents that the information in his certificate (e.g. name, public key) is public and available for signature verification.

- **Partner entities and third parties that trust certificates (*Relying Parties*):** This category includes any third party that receives a signature or electronic seal generated with an AlfaTrust certificate and decides to rely on it. Partner entities (e.g. institutions that validate the signatures of their employees, platforms that integrate AlfaTrust services, etc.) and in general all end users of signed documents have the following responsibilities: to **verify the authenticity and status** of any AlfaTrust certificate on which they rely (by consulting the revocation list or querying the OCSP at the time of signature validation) – this obligation is essential, as trusting a expired or revoked certificate can invalidate the signature; take into account any limitations of the certificates, specified in the IPPD or in the certificate itself (e.g. if a certificate has restricted use mentions or a certain limit on the value of the transaction – although generally qualified certificates do not have such limitations imposed by the provider, third parties must pay attention to any clauses); use standard-compliant software to verify signatures. Third parties (as defined in the context of this section) are also responsible for informing themselves about the terms and conditions of AlfaTrust's services (a document that is public and available on the AlfaTrust website), where the provider's obligations and possible limitations of liability are detailed. By using signatures based on AlfaTrust certificates, third parties implicitly accept their terms of use.

All of the above-mentioned parties must cooperate and act in good faith for the purpose of maintaining an environment of trust. AlfaTrust publishes in an accessible way **the obligations of each party** (in the public documentation – DPSI, certification policy, terms and conditions, etc.), so that each participant knows their responsibilities before using the service.

7. COMMITMENTS MADE BY ALFATRUST (THE PROVIDER)

AlfaTrust Certification S.A., as a qualified provider of trust services, formally assumes a series of commitments and guarantees towards the users of the services and towards the authorities, in order to ensure the quality and legality of the services provided. These commitments stem from legal requirements (eIDAS Regulation, national law) and AlfaTrust's own internal policies. The main commitments made are:

- **Legal compliance and standardization:** AlfaTrust is committed to fully comply with Regulation (EU) No. 910/2014 (eIDAS) and the relevant Romanian legislation, such as Law 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them (including the requirements of the Supervisory Authority – ADR). The provider maintains the certification as a **qualified provider** and demonstrates compliance through the periodic audits required by law. Also, the services are offered in accordance with the applicable European ETSI standards (EN 319 401, 319 411, 319 421, etc.), so that there is interoperability and recognition at European level.
- **Quality of services and continuity:** The Provider guarantees that the reliable services will be provided in a reliable and uninterrupted manner, except for announced maintenance periods or cases of force majeure. The infrastructure is designed with redundancy to maximize availability. There is a commitment that, in the unlikely event of a major interruption of services, AlfaTrust will make every effort to restore the services as soon as possible and minimize the impact on users. In addition, AlfaTrust maintains an up-to-date termination plan that ensures continuity or controlled closure of services, in accordance with the requirements of eIDAS (details in the *Termination of Services* section).
- **Transparency and information:** AlfaTrust undertakes to clearly and completely inform any person who intends to use a trust service about the terms and conditions of use of that service, including any limitations on use. This commitment corresponds to Article 24(2)(d) of the eIDAS. In practice, before the issuance of a qualified certificate, the end user receives and accepts the Terms and Conditions of Use, which specify the rights

and obligations, limitations of liability, security policies, etc. The Terms and Conditions, as well as the DPSI and certification policies, are published on the AlfaTrust website and are easily accessible. AlfaTrust is also committed to promptly notifying users of any relevant and significant changes to the terms of service or policies (e.g., legislative changes affecting the service, changes in supported cryptographic algorithms, etc.).

- **Security of technical solutions:** The Service Provider guarantees that it uses reliable systems and products, protected against unauthorized modifications, and that it takes appropriate measures to ensure the technical security and reliability of the supported processes. This involves keeping security solutions up to date, using certified HSMs, patching, reviewing architecture to deal with new threats, etc. AlfaTrust assumes the obligation to prevent and combat fraud, forgery of certificates or theft of data, through the controls described in the DPSI. In the event of a security incident, AlfaTrust undertakes to manage it according to procedures and to communicate it to the affected parties, as detailed in the Risk *and Incident Management section*.
- **Data protection and privacy:** A major commitment is to ensure **the lawful and secure processing of customers' personal data** , in accordance with the General Data Protection Regulation (GDPR) and art. 24(2) letter j of EU Regulation 910/2014 - eIDAS 1. AlfaTrust processes only the data strictly necessary for the provision of services (e.g. identification data for the issuance of certificates) and keeps them for the necessary period of time according to legal requirements (ex. log and identification documents for 10 years, in accordance with the obligations of EU Regulation 910/2014 - eIDAS and tax legislation, if applicable). The provider ensures the confidentiality of these data and does not use them for purposes other than those declared, nor does it disclose them to unauthorized third parties. Users are informed about AlfaTrust's Privacy and Personal Data Processing Policy, which details their rights (right of access, rectification, deletion, etc.) and the protection measures implemented. AlfaTrust staff are trained and contractually obligated to maintain the confidentiality of customer data.

- **Liability and financial resources:** AlfaTrust assumes legal liability for damages caused intentionally or negligently in the provision of its services, within the limits provided by art. 13 of EU Regulation 910/2014 - eIDAS. In order to cover the risk of civil liability, AlfaTrust maintains sufficient financial resources and/or adequate liability insurance, as required by law. This means that users harmed as a result of AlfaTrust's failure to fulfil their obligations may receive compensation, subject to contractual terms and legal provisions. (For example, if a qualified certificate is issued without proper identity verification and causes harm to a third party, AlfaTrust may be held liable.) At the same time, AlfaTrust specifies in the terms and conditions of service any exclusions or limitations of liability allowed by law (for example, failure to cover damages resulting from incorrect use of the certificate by the holder, or from the unjustified reliance of a third party without verifying the status of the certificate).
- **Support and cooperation:** The provider undertakes to provide reasonable assistance to users and third parties regarding the use of the services. There are support channels (phone, email) through which users can request information or report problems, and AlfaTrust undertakes to respond promptly to these requests. At the same time, AlfaTrust actively cooperates with **the supervisory bodies** and **with the competent authorities** (e.g.: ADR, CERT-RO, ANSPDCP in the field of personal data) regarding any checks, incident reports or investigations, providing the necessary information to them.
- **Continuous improvement:** AlfaTrust is committed to continuously reviewing and improving its practices, taking into account technological developments, regulatory changes and feedback received from stakeholders. This includes regularly updating the DPSI, security policies and internal procedures to reflect best practices and address any identified deficiencies. The provider maintains an open dialogue with the community of users and partners, encouraging responsible reporting of any vulnerabilities or problems identified within its services, and treats these reports seriously in order to solve them.

In conclusion, through these commitments, AlfaTrust Certification S.A. demonstrates its commitment to providing high-quality, secure trust services aligned with the legal framework, so that users can have full confidence in the signatures, seals and timestamps they use.

8. REMOTE IDENTIFICATION OF APPLICANTS

Identifying applicants is an essential step in the process of issuing digital certificates. According to the eIDAS Regulation, the initial identification of the persons to whom qualified certificates are issued must be carried out **either by physical presence or by remote means equivalent in terms of safety level**. Traditionally, AlfaTrust performs identification by the physical presence of the applicant in front of an operator (registration authority) who verifies the original identity document and, if applicable, the documents of the legal entity and the mandate of the representative of that entity. However, given the technological developments and customer needs, AlfaTrust also offers the option **of remote identification**, under the conditions allowed by the national legal framework, for the issuance of qualified certificates.

If the applicant cannot be physically present and wishes to use remote identification video means, AlfaTrust implements the following approved methods:

- **Identification by existing qualified certificates:** Another accepted method is to identify the person on the basis **of a qualified electronic signature** already held by the person (previously issued by AlfaTrust or another qualified trust service provider). For example, if the applicant holds a valid qualified certificate, they can electronically sign a request/statement confirming their identity and agreement, and AlfaTrust can verify the validity of that qualified signature. This approach is equivalent to face-to-face identification, as the qualified signature is already based on a previous identification. Of course, the scope of the existing certificate must allow such use and the applicant must agree.
- **Identification by video-identification (online video KYC):** In accordance with national regulations (e.g. procedures approved by ADR - **2021 Rule on the regulation,**

recognition, approval or acceptance of the procedure for remote identification of the person using video means approved by the Decision of the President of ADR no. 564/2021), AlfaTrust may use a secure video-identification process. This process involves a live video session with the applicant, in which an authorized operator verifies the identity by comparing the face with the photo on the ID presented to the camera and through security questions. The video session is recorded and stored as evidence. At the same time, additional anti-fraud mechanisms can be used (e.g.: capturing images of the identity document in various positions, automatic checks of the security elements of the document, calling an official database for validating the CNP, etc.). This method is carried out according to **the Procedure for remote identification of the person using video means** approved by the regulatory authority and ensures a level of trust equivalent to physical presence based on the aforementioned legal provisions, or possibly those that replace them.

Regardless of the remote method used, AlfaTrust requires that:

- The process must be secure (encrypted communication, measures to prevent manipulation or *spoofing*).
- The identity must be verified with at least the same degree of rigor as in person. If there is the slightest doubt as to the identity or integrity of the process, the applicant will be asked to complete the identification in the traditional way (physical presence).
- The entire process and the associated evidence (video recording, logs, copies of documents) should be securely archived, in order to demonstrate the compliance of the identification to a possible audit.

Note: Currently, remote identification is offered as a facility especially for customers from other localities or abroad, where physical presence would be difficult. AlfaTrust fully complies with the provisions of the ADR Order and other rules on remote identification. Any limitations or

additional conditions (such as the need to use only approved video identification methods) will be communicated to applicants prior to initiating the online identification process.

In conclusion, **remote identification**, where used, is carried out only by methods that provide a level of assurance equivalent to in-person identification, AlfaTrust having as a priority the prevention of the issuance of certificates to false or unverified identities.

9. MANAGEMENT OF SECURITY RISKS AND INCIDENTS

Risk management: AlfaTrust has established a **continuous process of assessing and managing security risks** related to the provision of trust services, in accordance with Article 19 para. (1) of EU Regulation 910/2014 eIDAS and with the ISO 27005 standard (information security risk management) adapted to the specific context. This process involves regularly identifying potential threats (from cyberattacks, to human error, or natural disasters) and assessing system vulnerabilities. Each risk is estimated for its potential impact and likelihood of materialisation and a level of risk is established. AlfaTrust implements control measures to reduce the assessed risks to an acceptable level – these measures include those described in the security section (technical, procedural, political controls).

The residual risks (those remaining after the application of the controls) are monitored and reviewed by AlfaTrust's management during periodic risk analysis meetings (e.g.: at least annually or whenever a significant change occurs – the appearance of a new major vulnerability, legislative changes, expansion of services, etc.). Risk treatment plans are approved by management and implemented by designated technical staff.

In addition to deliberate risks (attacks), attention is also paid to accidental or error risks: for example, the risk of unavailability due to a prolonged power outage is mitigated by the UPS power supply and generator; the risk of human error in data entry is mitigated by double-checking procedures; the risk of compromise of an HSM is mitigated by physical protection and monitoring mechanisms, etc. Thus, it is intended that the level of security is proportional to the identified risks, updated to the technological stage and to the emerging attack vectors.

Security incident management: Despite all preventive measures, security incidents can occur. AlfaTrust has defined a **Security Incident Handling Procedure**, but also a **Security Risk Management Procedure**, which covers the detection, analysis, resolution and reporting of incidents. Any suspicious event (e.g.: unauthorized access, malware detected, major equipment failures, data compromise, or loss of integrity) is logged and escalated to the security team for evaluation.

For minor incidents (with no impact on trust services or customer data), the resolution is done internally, with documentation of the cause and remediation to prevent recurrence. For major incidents – defined as those that have or may have a significant impact on the trust services provided or the personal data handled, AlfaTrust follows the legal notification requirements. According to art. 19 para. (2) of EU Regulation 910/2014 - eIDAS, the provider shall notify the supervisory body (ADR) **without undue delay, but no later than 24 hours after the finding**, of any security breach or loss of integrity with significant impact. The notification will specify the nature of the incident, the affected services, the measures taken or planned and possibly the estimated impact. If the incident is also likely to affect users (the persons to whom the services have been provided) – for example the compromise of a private CA key that invalidates the certificate, or the disclosure of customers' personal data – AlfaTrust will **also inform the affected users**, also without undue delay.

Examples of situations that would trigger notification include: obvious compromise of a certificate authority's private key (situation of maximum severity, involving immediate revocation of the compromised authority's certificate and informing all parties), a successful cyberattack leading to unauthorized modification of data in the certificate database (loss of integrity), prolonged unavailability of validation services affecting signature verification, or unauthorized access to the database containing customers' personal information.

AlfaTrust cooperates closely with the authorities in investigating incidents. If a security incident or loss of integrity affects more than one Member State (e.g. certificates issued by AlfaTrust used cross-border), ADR (as a notified supervisory body) will inform the supervisory authorities of

those States, as well as ENISA, if applicable. Also, if the incident involves a personal data breach, AlfaTrust will also notify the National Supervisory Authority for Personal Data Processing (ANSPDCP), according to the obligations of the GDPR (generally within the same 72-hour period, which is covered by the notification within 24 hours to the ADR).

Post-incident measures: After the immediate management of an incident, AlfaTrust conducts an *a posteriori* analysis to identify root causes and implement corrective/preventive actions. For example, if an incident was caused by a system vulnerability, the configuration will be updated and patch management procedures will *be* reviewed; if human error has been involved, re-training sessions will be provided to staff and it will be assessed whether procedures need to be improved. The results and lessons learned from incidents are documented and used to avoid similar situations in the future.

Operational continuity in the event of an incident: The above-mentioned continuity plans (BCPs/DRPs) are an integral part of risk and incident management. In the event of a major incident that leads to the unavailability of the primary infrastructure, the secondary center will be activated, ensuring that critical services (such as the CPVO, the CRL publication site) remain functional or come back online in the shortest possible time (in the order of hours). The priority is to protect the integrity of the certificates issued and to maintain public trust in the services, even if technical difficulties arise.

In conclusion, AlfaTrust treats both **proactively and reactively** the security of its services with the utmost seriousness. Through rigorous risk management and a robust incident response plan, users can trust that any incidents are prevented as much as possible, and if they do occur, they are managed promptly, transparently and efficiently, with minimizing the consequences on them.

10. PROTECTION OF PERSONAL DATA

As a personal data controller, AlfaTrust Certification S.A. fully complies with the applicable legislation in the field, mainly EU Regulation 679/2016 – General Data Protection Regulation

(GDPR), as well as the special provisions of the eIDAS Regulation regarding data protection (art. 5 and art. 24(2) letter j). The protection of personal data of applicants and users of trust services is integrated into all AlfaTrust processes.

Data collected and purposes: AlfaTrust collects only the personal data necessary for the provision of each trust service (principle of data minimization – art. 5 para. (1) letter c) of EU Regulation 679/2016 - GDPR. In the case of signature certificates, they usually include: the full name of the person, and in the case of certificates issued to a legal person – the name of the organisation and the assignment of the certificate to it, the address or registered office (if relevant), contact details (email, telephone) for communications regarding the service, and elements related to identity verification (type and series of identity document, supporting documents). All this data is used exclusively for the purposes of: validating identity and issuing certificates, maintaining operational records (including the issuance and revocation log), contacting users about the service (expiration notifications, security announcements, terms updates) and fulfilling legal obligations (e.g., keeping audit trails for possible fraud investigations or legal disputes).

Legal basis and when consent is used as a legal basis: The processing of personal data by AlfaTrust is based either on the **fulfillment of a legal obligation** (the provider's duty to verify identity before issuing a qualified certificate, according to eIDAS), or on **the performance of the contract** to which the data subject is a party (provision of the requested trust service), or on **explicit** consent of the data subject, where required (for example, if there will be processing of personal data for marketing purposes, separate from the provision of the service, this will only be done with separate consent, but AlfaTrust does not currently use customer data for direct marketing purposes). Users are informed about the data processing policy at the time of collection; in particular, upon registration they are presented with a Privacy and Personal Data Processing Policy in order to ensure the information requirements provided by art. 13 of EU Regulation 679/2016 – GDPR, which describes the categories of data collected, purposes, legal bases, storage period and their rights.

Storage and retention period: Customers' personal data (including copies of identity documents, application forms, verification logs) is stored in secure environments (encrypted databases, locked physical document vaults, etc.). AlfaTrust retains this data **for the period necessary according** to the regulations: as a rule, the information related to the issuance of qualified certificates and the identification of the holders is kept **for at least 10 years** from the end of the validity of the certificate, because both eIDAS and commercial requirements (e.g. legal, accounting, tax, civil provisions regarding possible limitation periods or those related to cybersecurity) require the maintenance of long-term records. After the expiration of the retention period, the data is irreversibly deleted or anonymized according to internal procedures.

Security of personal data: The technical and organizational measures detailed in the security section of the DPSI (access control, encryption, personal privacy, etc.) apply directly to the protection of personal data. In addition, AlfaTrust limits access to personal data only to those employees who need to process it for the stated purposes (*need-to-know* principle). All persons who have access to such data (including any trusted subcontractors – e.g. external auditors, technical or legal consultants if they need access) are subject to confidentiality obligations. The systems that process personal data are monitored for unauthorized access, and the transfer of data (including between the

Registration and AC) is encrypted. AlfaTrust conducts regular security testing (including vulnerability assessments and, if necessary, penetration testing) to ensure that customer data remains protected from unauthorized access or unauthorized disclosure.

Data Subject Rights: AlfaTrust guarantees the exercise of all rights provided by the GDPR: the right to information and access to their own data (the user may request a copy of his/her processed data – e.g. information in the registration form, issuance logs, etc.), the right to rectification (any incorrect or incomplete data may be corrected upon request, although, the data in the certificates cannot be changed after issuance, but only the old certificate is revoked and a new one is issued with the correct/updated data), the right to erasure (can be exercised after the expiry of the validity period of the certificate and the legal obligations of retention/retention of

personal data – before this term, some data cannot be deleted for legal reasons), the right to restriction of processing, the right to data portability (to the extent applicable – e.g. the identification data provided may be made available to the user in a structured format, if he/she wishes to use them with another provider), the right to object (e.g. opposition to the processing of data for marketing purposes, which AlfaTrust does not do anyway without consent). Also, the data subjects have the right to file a complaint with the ANSPDCP if they consider that their rights have been violated.

Transfers and Disclosures: AlfaTrust does not normally transfer customers' personal data outside of the European Economic Area. Any possible transfer (e.g. outsourced cloud storage) would only be made to entities in countries with an adequacy decision or with adequate guarantees (standard protection clauses) and would be notified in the privacy policy. The disclosure of data to third parties is limited to the necessary situations: for example, the provision of data to conformity assessment bodies during audits (which are also bound by confidentiality), the response to legal requests from the authorities (e.g. criminal prosecution bodies, based on an official request under the law), or the sharing of the minimum data with authorized partners involved in the registration process. Otherwise, the data on the issued certificates that become public are only those strictly necessary for the functioning of the public key infrastructure – namely **the certificates themselves** (which contain the name of the holder, the organization if applicable, and the public key – this information is inherently public so that third parties can verify the signatures) and status information (revoked or expired certificates, published in the CRL/CPVO). These are not considered unauthorized disclosures, but are part of the certification service.

Data Protection Officer (DPO): Given the significant volume of personal data processed (and its nature, including identity documents, CNP, etc.), AlfaTrust has appointed a **Data Protection Officer** (DPO) in accordance with Art. 37 GDPR. The contact details of the DPO are published on the AlfaTrust website and in the privacy policy. Users can contact the DPO for any aspect related

to the processing of their data, and the DPO ensures internal compliance with the GDPR requirements and provides advice on the design of new services (to ensure confidentiality).

In conclusion, AlfaTrust treats the protection of personal data as an essential component of trust services. Through strict policies, technical security measures and transparency towards users, it is ensured that their personal data is safe and processed legally, strengthening trust in the services offered.

11. TERMINATION OF SERVICES AND BUSINESS CONTINUITY

Cessation of activity plan: AlfaTrust maintains an updated plan for the cessation of the provision of trust services, according to the requirements of eIDAS (art. 24 para. (2) letter i) and national regulations. This plan sets out the measures to be taken in the event that AlfaTrust decides, or is obliged to, cease to provide one or more qualified trust services. The main purpose is to protect the interests of users and third parties and to ensure the continuity of the validation of existing signatures or the orderly transfer of obligations to a successor.

Prior Notice: In the event of an intention to cease to operate as a Qualified Provider (or to cease a specific Qualified Service, e.g. to cease the Qualified Timestamping Service), AlfaTrust will notify:

- **Supervisory Authority (ADR):** at least 3 months (90 days) before the proposed termination date, according to legal and contractual requirements. The notification will include the reasons for the termination, the planned date and the mitigation plan.
- **All users with active certificates:** At least 30 days before termination. AlfaTrust will provide each certificate holder (and possibly the relevant partners) with written notice (by email and/or post) announcing the termination of service, the exact date and instructions on the actions they need to take (e.g. to complete their signatures before that date, to obtain certificates from another provider, etc.).

Revocation of certificates and cessation of issuance: On the effective date of termination, or immediately before, AlfaTrust will **revoke all active qualified certificates** that it has issued that

were not expired prior to the termination date. This is to avoid the existence of valid certificates without the support of a provider (which would create confusion about their status). The mass revocation will be communicated through the final revocation lists and will be proactively notified to users. AlfaTrust will also **cease issuing** any new certificates with a certain period prior to the termination date (to avoid issuing certificates of very short duration and to discourage new customers from relying on a service that is to be discontinued).

Transfer of responsibilities to a successor: The termination plan states that AlfaTrust will take steps to identify another **qualified trust service provider** willing to take over the records and possibly its customers. This may include:

- Transfer of databases (issued certificates, logs, identity records) to another qualified trust service provider, subject to GDPR compliance and with the consent of the supervisory authority, to ensure continuous access to validation information.
- Conclusion of a transfer agreement with the successor, guaranteeing the retention and protection of data and the further provision of status information (e.g. the new provider could take over the publication of revocation lists for certificates historically revoked by AlfaTrust, thus maintaining the possibility of long-term verification of signatures created during the period of AlfaTrust's activity).
- Offering the equivalent certificate from the successor at no significant additional cost (to the extent that the successor and the user agree).

If a complete transfer is not possible, AlfaTrust will hand over to the supervisory authority or another neutral entity (e.g. a national repository) the necessary archives (lists of certificates, journals) to ensure that, for the necessary period, third parties can verify the signatures made with the former AlfaTrust certificates.

Public information: AlfaTrust will publish on its website and through public communication channels (e.g. press release, announcements on specialized portals) the information about the termination of services, so that all interested parties (including those who are not direct

customers, but may use intermediary services based on AlfaTrust certificates) can become aware. This public information will be made sufficiently in advance (30-90 days in advance, depending on the channel).

Minimizing the impact on users: AlfaTrust will make all reasonable efforts to reduce the negative effects on users caused by the cessation of activity. For example, if a user has a certificate that would have been valid for a significant period of time (and therefore paid the equivalent for that period), AlfaTrust may offer proportional financial **compensation** (at most the equivalent of unused issuance fees) or other agreed forms of compensation. Such details will be clarified in the notifications sent to users. Also, AlfaTrust's support staff will assist users in migrating to other solutions (providing, upon request, proof and identification documents they have, in order to facilitate re-enrollment with another provider, within the limits of the law).

Partial termination (of a specific service): If AlfaTrust decides to terminate one of its services but continues others (e.g., discontinues the qualified timestamping service but retains the services of creating, validating, and verifying electronic signatures), the above procedures will apply specifically for that service. Users of that service will be notified and offered alternatives (e.g., another qualified trust service provider) or compensation, as appropriate. The partial cessation will be announced to the supervisory authority and the public similar to the total cessation.

Force majeure and exceptional revocation of qualification: In extreme situations, such as forced withdrawal of qualification by the supervisory authority (e.g. following a severely failed audit) or untimely financial incapacity (bankruptcy), AlfaTrust will work with the supervisory authority which will take the necessary measures to protect users (possibly temporary administration of the services, delegation of administration to another qualified trust service provider, etc.). Regardless of the situation, the priority will be to maintain the possibility of verifying existing signatures and to immediately inform the public about the change in the status of the provider (e.g. removal from the EU Trusted List in case of withdrawal of the status of qualified trust service provider).

Conclusion: Although AlfaTrust intends to continue its activity indefinitely and sustainably provide reliable services, there is a clear plan in place in the event of termination, to ensure that users are not left without support or in uncertainty. Through prior notice, controlled revocation of certificates and transfer of records, AlfaTrust will **responsibly manage** any interruption of services, in accordance with legal obligations and commitments to customers.

12. REVIEW AND UPDATE OF THE STATEMENT OF PRACTICES APPLICABLE TO TRUST SERVICES (DPSI)

The Statement of Practice for Trust Services (DPSI) is a dynamic document that may be updated to reflect changes in regulation, technology or internal policies. AlfaTrust has established a formal process for the management of the DPSI, which includes periodic review, approval of changes, and publication of new versions.

Version and validity: Each version of the DPSI is identified by a version number and an effective date. A version of the IPPD shall remain applicable and take effect until the next version is approved and published. When issuing a new version, it is explicitly specified whether it replaces the previous version in its entirety or whether certain parts are in force at the same time (normally, the new version replaces the old version in its entirety).

Initiation of changes: The revision of the DPSI may be initiated as a result of: legislative/regulatory changes (e.g., the appearance of new ETSI standards or ADR guidelines to be reflected), the identification of errors or uncertainties in the current text, changes in AlfaTrust's infrastructure or procedures, or feedback received from stakeholders (users, auditors, partners). Proposals for changes can be submitted by anyone with an interest in it – for example, internal staff, auditors, partners or even users – either directly to the designated managers or to the official email address of AlfaTrust. Any proposal must describe the desired change and its motivation.

Evaluation and development of the new version: The AlfaTrust Security and Compliance Management team will periodically (usually annually or more frequently if necessary) review the need for the DPSI update. If it is decided to initiate a new version, an internal working group

(including representatives of the relevant departments: legal, IT, security, operations) will draft the new version of the DPSI. Attention will be paid to ensuring continuity – i.e. new provisions do not contravene commitments made to users, unless they are required by law (e.g. if a new regulation requires stricter conditions, the IPD will be amended accordingly and users will be notified).

Stakeholder consultation: Depending on the nature of the changes, AlfaTrust may decide to consult stakeholders in advance before the new version is finalized. Changes that are substantial or that could affect users (e.g., changing the certification policy, introducing new limitations, changing the cryptographic algorithms used, etc.) are usually subject to public consultation or at least communicated to partners and large customers for feedback. On the other hand, minor or urgent changes (such as correction of typographical errors, updating of contact details, adjustments that do not affect essential rights/obligations) can be adopted without extensive consultation, so as not to delay their implementation.

Internal approval: Once the draft of the new version is finalised (also taking into account any comments received during the consultation phase), it is subject to internal approval. The responsibility for the final approval lies with AlfaTrust's management – usually a committee made up of members of the senior executive management and managers of the key departments (IT, Security, Legal, Operations). This committee examines whether the new version meets all compliance requirements and whether the changes are properly justified. Once the agreement of the committee has been obtained, the version is considered completed.

Notification to authorities and publication: Before taking effect, the new DPSI is submitted to **the supervisory body (ADR),** in accordance with the obligations of the qualified provider to inform its authority about its policies (also referred to in ADR Order 449/2017). Usually, the DPSI is submitted to the ADR for information and possible evaluation. Shortly (maximum 10 days) after sending it to the authority, AlfaTrust proceeds to **publish** the new version on the official website. The new version is marked as "*in force*" along with the date from which it applies. The previous version, if applicable, is archived and available for reference (in particular, it may be

necessary to maintain old versions on the website for historical reference, for example by courts or third parties who validate signatures from the past and want to know the practices at that time).

Change management: DPSI provides a history of versions or significant changes at the end. Changes can be grouped into two categories:

- Major changes – that significantly affect policies (e.g. introduction of a new trust service in the offer, changes in the responsibilities of the parties, major revision of security policies). These are normally communicated to users in advance and may require explicit acceptance (for example, if the Terms and Conditions change as a result of new IPD, existing users may be notified and deemed to have agreed to continue using the service).
- Minor changes – that do not substantially influence rights and obligations (e.g.: editorial corrections, text clarifications, updating some standard names to new versions with no practical impact). They may be effective as soon as the updated DPSI is published, without special notice to customers, although AlfaTrust may choose to inform in a newsletter or on the website of the existence of the new version.

Input from external parties: Any entity or user who believes that a particular provision of the IPD needs to be improved may send suggestions to AlfaTrust (by email to the official contact address). AlfaTrust undertakes to carefully consider such suggestions, and if they are pertinent and feasible, to include them in a future version. This mechanism ensures transparency and collaboration in refining practices, taking into account diverse perspectives (e.g. an external auditor might suggest clarifying a section to make it easier to verify compliance).

Availability of DPSI: The current version of DPSI, as well as any previous versions, are available free of charge on the AlfaTrust website in a printable format. The DPSI is available in Romanian (the official language), and if necessary, AlfaTrust can also provide an unofficial English translation of this document, in order to facilitate understanding by foreign partners (according

to the cross-border cooperation requirement of Order 449/2017). In case of discrepancies, the Romanian version remains the official version.

Conclusion: Through this process of reviewing and updating the DPSI, AlfaTrust ensures that the declared practices are always aligned with reality and legal requirements. Any change is made in a controlled way, avoiding confusion or lack of communication. Users and partners can trust that the DPSI reflects the current way in which AlfaTrust operates, and AlfaTrust, in turn, undertakes to operate as stated in the DPSI. The DPSI document, together with the internal policies and procedures it refers to, is subject to the compliance audit, thus ensuring that it is not a mere formality, but a real representation of the provider's actual practices.