General personal data protection policy

1. Introduction

This policy sets out the activities and measures adopted by AlfaTrust Certification S.A., as a trust service provider, to guarantee and protect the fundamental rights and freedoms of individuals in relation to the processing of personal data, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation – "GDPR"), as well as Law no. 190/2018 on GDPR implementation measures.

This policy is general in nature and reflects AlfaTrust Certification S.A.'s commitment to data protection, applicable in relation to customers, employees, contractual partners, authorities and other relevant third parties. It is not intended for the direct information of the data subjects, but for documenting the organizational and technical measures applied by the company for compliance purposes.

2. Purpose and grounds for the processing of personal data

2.1. Purposes of personal data processing

AlfaTrust Certification S.A. processes personal data in a lawful, fair and transparent manner, exclusively for determined, explicit and legitimate purposes, in accordance with Regulation (EU) 2016/679 ("GDPR") and Law no. 190/2018 on its implementing measures.

The processing takes place by automated and/or manual means, under conditions that ensure the security, confidentiality, integrity and availability of the data, as well as the observance of the rights of the data subjects.

Personal data is collected and used, mainly, for the following purposes:

- provision of qualified and unqualified trust services (e.g. electronic signature, timestamping);
- performance of a contract or to take steps at the request of the data subject before the conclusion of the contract (letter b);
- fulfilling the legal obligations incumbent on the operator (including those of the eIDAS Regulation, tax, accounting or electronic services legislation);
- providing technical support and customer relationship management;
- fraud prevention and ensuring the security of systems and data;
- auditing, archiving, reporting to supervisory authorities and bodies;

- other purposes justified by the legitimate interest of the controller, insofar as they do not override the fundamental rights and freedoms of the data subjects.

2.2. Grounds for processing personal data

The processing is based on one or more of the legal bases provided by art. 6 para. (1) of the GDPR, as follows:

- performance of a contract or to take steps at the request of the data subject before the conclusion of the contract (letter b);
- the fulfillment of a legal obligation incumbent on the operator (letter c);
- the legitimate interest of the operator (letter f), assessed proportionally and justified in relation to the activity carried out.

If special categories of data (e.g. biometric data) are processed, the controller shall ensure that there is a valid basis in accordance with Art. 9 para. (2) of the GDPR, such as the processing necessary for the fulfilment of legal obligations or for the establishment, exercise or defence of a right in court.

The data is not used for purposes other than those declared, unless the controller has a distinct legal basis that allows the extension of the processing.

3. Applicable principles regarding the processing of personal data

In accordance with Article 5 of Regulation (EU) 2016/679 (GDPR), AlfaTrust Certification S.A. undertakes to comply with the following fundamental principles in all personal data processing activities:

a. Legality, fairness and transparency

The data is processed in a lawful, fair and transparent manner towards the data subject, based on a valid legal basis.

b. Purpose limitation

The data is collected for specific, explicit and legitimate purposes and is not further processed in a way that is incompatible with these purposes.

c. Data minimization

The data collected is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

d. **Accuracy**

The data shall be accurate and, where necessary, updated. Reasonable steps are taken to ensure that inaccurate data is rectified or deleted without delay.

is. **Storage limitation**

The data is kept in a form that allows the identification of data subjects only for as long as it is necessary for the fulfillment of the purposes for which they are processed.

f. **Integrity and confidentiality (security)**

The data is processed in a way that ensures their security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by applying appropriate technical and organisational measures.

g. **Accountability**

AlfaTrust Certification S.A., as the controller, is responsible for complying with these principles and may demonstrate compliance with them at any time.

4. Types of data collected and recipients

4.1. Types of data collected

Depending on the nature and specificity of the services provided, AlfaTrust Certification S.A., as a personal data controller, collects and processes the following categories of personal data belonging to customers, employees, contractual partners or other data subjects:

- Identification data: name, surname, personal identification number, series and number of the identity document, citizenship, signature;
- Contact data: mailing address, e-mail address, telephone number;
- Contractual and financial data: bank data (e.g. IBAN, bank), tax data (e.g. CUI, NIF), information necessary for the conclusion and execution of contracts;
- Data regarding representation: position, quality of legal or conventional representative;
- Technical data: IP addresses, electronic identifiers and access logs, when the interaction is made through computer means;
- Other data strictly necessary to comply with legal obligations or to ensure the provision of trust services, including in relation to supervisory authorities.

The data is collected directly from data subjects or, in certain cases, from authorities or other partners involved in the execution of contracts or the provision of services.

4.2. Data recipients

Personal data may be disclosed, under conditions of legality and necessity, to the following categories of recipients:

- public authorities and regulatory bodies, including the Authority for the Digitization of Romania, ANAF, ANSPDCP, courts, at their request or based on legal obligations;
- service providers (processors) acting in the name and on behalf of AlfaTrust Certification S.A., such as: IT infrastructure, accounting, auditing, archiving, technical support providers;
- banking institutions or payment service providers, for the purpose of carrying out the necessary financial operations;
- external consultants (legal, tax, cybersecurity), for the purpose of establishing, exercising or defending a right in court.

All recipients to whom the data is transmitted are obliged, by contract or by law, to maintain the confidentiality of the data and to ensure its protection according to the requirements of the GDPR.

5. Rights of data subjects

AlfaTrust Certification S.A. ensures compliance with the rights conferred on data subjects by Regulation (EU) 2016/679 ("GDPR"), in relation to the processing of personal data. Thus, the data subjects benefit from the following rights:

- **Right to information** (Art. 13 and 14 GDPR): the data subject has the right to receive clear and detailed information regarding the identity of the controller, the purposes of the processing, the legal bases, the recipients of the data, the storage period, as well as his or her rights, both if the data are collected directly and indirectly;
- **Right of access** (Art. 15): the right to obtain confirmation that his/her data is being processed, as well as access to this data and related information;
- **Right to rectification** (art. 16): the right to request the correction of inaccurate data or the completion of incomplete data;
- **Right to erasure of data ("right to be forgotten")** (art. 17): the right to request the deletion of data, under the conditions provided by law;
- **Right to restriction of processing** (Art. 18): in certain situations, the data subject may request the limitation of the processing of his or her data;

- **Right to data portability** (art. 20): if the processing is based on consent or a contract and is carried out by automated means, the data subject may request the transfer of data to another controller;
- **Right to object** (Art. 21): the data subject may, on grounds relating to his or her particular situation, object to the processing of data on the basis of legitimate interest or for direct marketing;
- **The right not to be subject to automated decision-making (** Art. 22): including profiling, which produces legal effects on the data subject;
- **Right to withdraw consent** (Art. 7 para. 3): at any time, if the processing is based on consent;
- **The right to lodge a complaint** with the National Supervisory Authority for Personal Data Processing, as well as to address the competent courts.

Personal data is kept only for the period necessary to fulfill the purposes for which it was collected, in accordance with the principles provided by the GDPR and in full compliance with the rights of data subjects.

Requests regarding the exercise of rights can be sent to the e-mail address: **dpo@alfatrust.ro**
The Controller will respond to the request **within 30 calendar days** from the date of receipt of the request, in compliance with the provisions of art. 12 GDPR.

6. Obligations of AlfaTrust Certification S.A. as a personal data controller

As a personal data controller, AlfaTrust Certification S.A. has the obligation to comply with the provisions of Regulation (EU) 2016/679 ("GDPR"), Law no. 190/2018, as well as the regulations applicable to the activities of providing trust and electronic archiving services.

The main obligations of the operator include:

- Compliance with GDPR principles, including legality, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability;
- Data processing for specific, explicit and legitimate purposes, clearly communicated to data subjects;
- Applying appropriate technical and organizational measures to protect data against unauthorized access, loss, destruction, unauthorized disclosure or modification;
- Appointment of a Data Protection Officer (DPO), under the conditions of Article 37 of the GDPR, and collaboration with the supervisory authority (ANSPDCP);
- Managing requests regarding the exercise of data subjects' rights (e.g. access, rectification, deletion, opposition, restriction, portability), within the term provided by law;

- Notification of security breaches, within a maximum of 72 hours from the finding, to the ANSPDCP and, if applicable, to the data subjects (art. 33–34 GDPR);
- Concluding written contracts with processors, who process data on behalf of the controller, in compliance with the requirements of art. 28 GDPR;
- Keeping a register of processing activities, according to art. 30 of the GDPR, with periodic updating;
- Appropriate training of personnel, including legal obligations, risks associated with processing and protective measures;
- Adopting internal policies and procedures, including for the prevention and management of security incidents, for access control and for auditing processing processes;
- Periodic review of data protection policies and their adaptation according to legislative, technological or organizational changes.

AlfaTrust Certification S.A. treats with responsibility and rigor every aspect related to data protection, integrating the principles of GDPR in all activities and services carried out.

7. Technical and organizational security measures

AlfaTrust Certification S.A. implements appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with the processing of personal data, in accordance with Article 32 of Regulation (EU) 2016/679 ("GDPR").

These measures aim to protect data against:

- accidental or unlawful destruction;
- loss, alteration, unauthorized disclosure;
- unauthorized access or any form of unlawful processing.

The level of security applied is adapted according to the nature of the data processed, the risks identified, the volume of data, technological progress and implementation costs.

The measures implemented include, but are not limited to:

- control of physical and logical access to equipment, applications and databases;
- secure user authentication and strict password policies;
- encryption and/or pseudonymisation of data, where applicable;
- regular and regularly tested backups;
- monitoring access and auditing of processing activities;
- restricting access to data to authorized personnel only;

- regular training of employees on data protection and security incident management;
- internal policies and procedures relating to change control, classification of information, incident management and business continuity.

The equipment used in the current activity is housed in secure technical spaces, protected against unauthorized physical access, provided with measures to maintain business continuity and recover data in case of unforeseen events.

The data processing is carried out exclusively by authorized personnel of AlfaTrust Certification S.A. or by contractual processors, who undertake to comply with the same high standards of security and confidentiality.

8. Privacy by Design and Privacy by Default

AlfaTrust Certification S.A. complies with the principles of data protection from the design phase (privacy by design) and implicit (privacy by default), according to art. 25 of Regulation (EU) 2016/679 (GDPR), within all processes involving the processing of personal data.

Privacy by Design implies that, from the planning and development stage of the services, applications and IT systems used, data protection requirements are integrated, such as:

- minimizing data collection;
- limiting access to data;
- selection of appropriate legal grounds;
- establishing the storage period;
- appropriate technical and organizational measures for security (e.g. encryption, access control, activity logging, auditing);
- clear and complete information of data subjects;
- involvement, where appropriate, of the data protection officer in the decision-making process.

Privacy by Default means that, by default, only the personal data strictly necessary for each specific purpose is processed. This involves:

- limiting the volume of data collected;
- restricting the data retention period;
- limiting access only to authorised staff on the basis of the 'need-to-know' principle;
- exclusion of any unjustified or excessive processing.

Therefore, AlfaTrust Certification S.A. ensures that data protection is a fundamental and priority component in the architecture and implementation of all its internal processes, complying with the highest standards of compliance, security and transparency.

9. Notification of security incidents

As a qualified trust service provider and personal data controller, AlfaTrust Certification S.A. complies with the legal obligations regarding the notification of security incidents, according to:

- Regulation (EU) 910/2014 (eIDAS) – for incidents affecting the integrity or reliability of the trust services provided;
- Regulation (EU) 2016/679 (GDPR) – for security breaches involving personal data.

9.1. Notification to the authorities:

- The Authority for the Digitization of Romania (ADR) is notified within 24 hours of becoming aware of a significant security incident regarding trust services, according to art. 19 of eIDAS.
- The National Supervisory Authority for Personal Data Processing (ANSPDCP) is notified within 72 hours, according to art. 33 GDPR, if the incident may generate a risk to the rights and freedoms of the data subjects.

9.2. Notification to data subjects:

If the incident is likely to generate a high risk to the rights and freedoms of natural persons, AlfaTrust Certification S.A. shall notify the data subjects without undue delay, in accordance with Article 34 of the GDPR.

9.3. Content of the notification:

Notifications sent to authorities and, where applicable, to data subjects, shall include, to the extent that the information is available at the time of transmission:

- The date and time of the incident;
- Description of the nature of the incident (e.g. loss, unauthorized access, copying, modification);
- The categories and approximate number of data subjects affected and the volumes of data involved;
- The context of the incident and the relevant technical/legal circumstances;
- Contact details of the Data Protection Officer (DPO) or a designated person;

- The potential consequences for data subjects or the services provided;
- Corrective measures adopted or planned to limit the impact and prevent similar incidents.

If all this information cannot be submitted in a single step, AlfaTrust Certification S.A. will provide it in successive installments, as soon as it becomes available, without undue delay.

9.4. Collaboration with the authorities:

The company undertakes to cooperate fully with the competent authorities (ADR, ANSPDCP) and to provide any additional information necessary in the context of subsequent investigations or inspections.

10. International data transfers

Currently, AlfaTrust Certification S.A. does not transfer personal data to third countries (outside the European Economic Area – EEA) or to international organizations.

If, in the future, such transfers become necessary for the performance of the activity, they will be carried out only in accordance with the provisions of Regulation (EU) 2016/679 (art. 44–49 GDPR), and only under the following conditions:

- to states for which the European Commission has issued an adequacy decision;
- based on appropriate safeguards, such as standard contractual clauses approved by the European Commission;
- under the limiting exceptions provided for in Art. 49 GDPR, if applicable.

AlfaTrust Certification S.A. will ensure, in any case, an adequate level of protection of the personal data transferred, in accordance with European standards in terms of privacy and security.

11. Revision and entry into force

This General Data Protection Policy is reviewed annually or whenever necessary, depending on legislative changes, recommendations of supervisory authorities or relevant internal changes regarding data processing activities.

The review is carried out by the Data Protection Officer (DPO) and the updated version is subject to the approval of the management of AlfaTrust Certification S.A.

Any material changes will be duly communicated to data subjects and interested parties.