



Declarația practicilor aplicabile serviciilor de încredere furnizate de AlfaTrust Certification S.A.

CUPRINS

CUPRINS.....	2
1. Introducere.....	3
2. Domeniu de aplicare.....	3
3. Serviciile de încredere furnizate.....	4
4. Infrastructura tehnică și organizatorică.....	5
5. Politici interne și controale de securitate.....	6
6. Responsabilități ale părților implicate.....	8
7. Angajamentele asumate de AlfaTrust (Prestatorul).....	11
8. Identificarea la distanță a solicitanților.....	13
9. Gestionarea riscurilor și a incidentelor de securitate.....	14
10. Protecția datelor cu caracter personal.....	16
11. Încetarea serviciilor și continuitatea activității.....	18
12. Revizuire și actualizarea Declarației Practicilor aplicabile Serviciilor de Încredere (DPSI).....	20

1. INTRODUCERE

Scop

Declarația practicilor aplicabile serviciilor de încredere (DPSI) descrie în mod cuprinzător practicile, politicile și procedurile utilizate de **AlfaTrust Certification S.A.** (denumită în continuare **Prestator de Servicii de Încredere** sau **PSC**) pentru furnizarea serviciilor de încredere. Documentul are rolul de a asigura transparența modului de operare al prestatorului, în conformitate cu legislația națională și europeană aplicabilă, în special Regulamentul (UE) nr. 910/2014 (Regulamentul eIDAS) și standardele europene relevante. DPSI răspunde cerințelor art. 19 și art. 24 alin. (2) din Regulamentul eIDAS, precum și cerințelor impuse de standardele ETSI (precum EN 319 401, EN 319 411-1, EN 319 421) și de legislația națională (Ordinul ADR nr. 449/2017 și alte reglementări subsecvente).

Prin intermediul acestei declarații, AlfaTrust Certification S.A. stabilește angajamentele asumate și controalele implementate pentru a oferi servicii de încredere calificate la nivel înalt de securitate și conformitate. DPSI explică rolurile și responsabilitățile tuturor părților implicate, cerințele operaționale pentru emiterea și administrarea certificatelor digitale, măsurile de securitate aplicate, precum și modul de gestionare a riscurilor, incidentelor de securitate, protecției datelor și continuității serviciilor. Documentul servește totodată ca referință pentru **politicile interne** ale AlfaTrust (ex.: Politica de securitate a informației – ATC-PS-18 “Managementul Securității Informațiilor”, Codul de Practici și Proceduri – CPP, Politica de certificare și sigilii electronice, Politica de marcare temporală ș.a.), fără a le reproduce integral, indicând însă modul în care acestea se reflectă în practicile operaționale.

Notă: DPSI este un document publicat și actualizat periodic, disponibil utilizatorilor și părților interesate, care rămâne în vigoare până la emiterea unei versiuni noi aprobate. Orice nouă versiune a DPSI va fi supusă aprobării interne și notificată către organismul de supraveghere (Autoritatea pentru Digitalizarea României – ADR), fiind apoi publicată pentru informarea tuturor celor interesați (detalii privind revizuirea și actualizarea se regăsesc în secțiunea *Revizuire și actualizare* a prezentului document).

2. DOMENIU DE APLICARE

Prezenta declarație se aplică tuturor serviciilor de încredere furnizate de AlfaTrust Certification S.A., precum și tuturor participanților la infrastructura de certificare electronică a societății. Sunt vizați: personalul și structurile AlfaTrust (inclusiv Autoritatea de Certificare – AC, Autoritatea de Înregistrare – AI, Autoritatea de Marcare Temporală – TSA și, dacă este cazul, Autoritatea de Validare – AV), partenerii contractuali (ex.: distribuitori, autorități de înregistrare externe delegate), utilizatorii finali (deținătorii certificatelor calificate) persoane fizice sau juridice, precum și terții care se bazează pe certificatele emise (entități partenere/relying parties). DPSI stabilește regulile și practicile care guvernează **utilizarea certificatelor și serviciilor de încredere AlfaTrust**, în special a certificatelor calificate, asigurând că acestea pot fi folosite în condiții de maximă siguranță, în orice context permis de lege.

DPSI acoperă serviciile de încredere calificate oferite de AlfaTrust (enumerare în secțiunea următoare), inclusiv variantele “avansate” ale acestor servicii acolo unde este cazul. Documentul descrie aplicabilitatea certificatelor emise de AlfaTrust în diferite scenarii de utilizare. **Certificatele digitale calificate** emise sub autoritatea AlfaTrust sunt de uz general și pot fi utilizate oriunde pe teritoriul Uniunii Europene și internațional, nefiind limitate la un anumit sector sau mediu de afaceri. Conform legislației în vigoare, o semnătură electronică realizată cu un certificat calificat AlfaTrust este recunoscută ca validă indiferent de

țara în care a fost emis certificatul sau unde se află utilizatorul, atâta timp cât atât certificatul cât și semnătura respectă cerințele legale aplicabile. Certificatele calificate AlfaTrust pot fi folosite și pentru a genera semnături sau sigilii electronice avansate (necalificate), însă în acest caz valoarea legală va fi dată de nivelul “avansat” al semnăturii/sigiliului (nefiind calificat).

În mod implicit, certificatele calificate emise de AlfaTrust au **domeniu de utilizare general** (utilizare: semnătură electronică, sigiliu electronic, autentificare, criptare), nefiind restricționate la un singur tip de aplicație. Orice limitări specifice ale utilizării vor fi comunicate explicit în termeni și condiții sau în certificatul propriu-zis (în extensiile certificatului). În lipsa unor asemenea limitări, terții care se încred în certificatele AlfaTrust le pot utiliza pentru a verifica semnături/sigilii electronice în orice context legal în care astfel de semnături sau sigilii sunt acceptate.

3. SERVICIILE DE ÎNCREDERE FURNIZATE

AlfaTrust Certification S.A. este calificată ca prestator de servicii de încredere calificat și oferă următoarele servicii de încredere, în conformitate cu eIDAS și legislația națională:

- **Serviciu calificat de creare a semnăturilor electronice** – constă în emiterea de certificate calificate pentru semnătură electronică destinate persoanelor fizice (inclusiv reprezentanților autorizați ai persoanelor juridice). Acest serviciu permite generarea de semnături electronice calificate cu valoare legală echivalentă semnăturii olografe, precum și de **semnături electronice avansate** atunci când certificatele emise sunt utilizate fără dispozitiv calificat. Certificatele pentru semnătură electronică pot fi stocate pe dispozitive securizate de creare a semnăturii (ex.: token USB, smart card calificat) sau, în cazul soluției de semnătură la distanță (**AlfaSign Cloud**), pot fi găzduite centralizat pe un modul HSM administrat de AlfaTrust (cu respectarea condițiilor de activare de către titular).
- **Serviciu calificat de creare a sigiliilor electronice** – constă în emiterea de certificate calificate pentru sigiliu electronic destinate persoanelor juridice (organizații). Aceste certificate pot fi folosite de entități pentru a aplica sigilii electronice calificate pe documente sau date, garantând astfel originea și integritatea acestora. Similar semnăturilor, certificatele pentru sigilii pot fi implementate pe dispozitive criptografice aflate la client sau găzduite la distanță în infrastructura AlfaTrust, permițând aplicarea de **sigilii electronice avansate** sau calificate în funcție de modul de utilizare.
- **Serviciu calificat de marcă temporală electronică** – constă în generarea și furnizarea de mărci temporale calificate, prin intermediul Autorității de Marcă Temporală (TSA) AlfaTrust. Serviciul asigură datarea și temporizarea fiabilă a documentelor sau tranzacțiilor electronice, folosind o sursă de timp sincronizată și securizată. Marca temporală emisă include semnătura electronică a TSA și este conformă cu standardele aplicabile (de ex. RFC 3161 și ETSI EN 319 421 pentru politici de timestamping), garantând că la momentul indicat conținutul documentului nu era modificat.

Mențiune: AlfaTrust asigură și servicii tehnice adiacente necesare funcționării celor de mai sus, cum ar fi servicii de validare a stării certificatelor (OCSP – Online Certificate Status Protocol și liste de revocare CRL), precum și suport pentru utilizatori și consultanță privind integrarea semnăturilor electronice. Serviciul de

validare a certificatelor (Autoritatea de Validare, dacă este oferit distinct) respectă cerințele eIDAS pentru verificarea calificată a semnăturilor electronice, însă în mod uzual verificarea statusului certificatelor emise de AlfaTrust se realizează automat, gratuit și în timp real prin serviciile OCSP/CRL puse la dispoziție de prestator. Toate serviciile furnizate se supun prezentelor practici și politici de securitate descrise în DPSI.

4. INFRASTRUCTURA TEHNICĂ ȘI ORGANIZATORICĂ

Arhitectura PKI (Public Key Infrastructure): Sistemul tehnic al AlfaTrust este structurat pe o ierarhie de autorități de certificare (AC) pe mai multe niveluri, pentru a asigura atât siguranța criptografică, cât și scalabilitatea serviciilor. La vârful ierarhiei se află o **AC rădăcină (AlfaTrust Root CA)**, menținută într-un mediu strict securizat și operată *off-line* (izolată de rețea), a cărei cheie privată este folosită exclusiv pentru a semna certificatele AC-urilor subordonate și listele de revocare ale acestora. La nivelul următor (nivel 1) funcționează **AC-uri subordonate interne (SubCA on-site)**, care emit direct certificatele calificate către utilizatorii finali (persoane fizice și juridice) și certificatele pentru marcă temporală. Există AC-uri distincte pentru diferite tipuri de certificate (ex.: o AC dedicată semnăturilor electronice calificate, o AC pentru sigilii electronice calificate, o AC pentru certificate necalificate folosite la semnături electronice avansate sau autentificare, etc.), în funcție de politicile de certificare aferente. Un eventual nivel 2 (AC-uri off-site) poate exista pentru implementări speciale (ex.: subCA găzduite la anumiți clienți mari, pentru emiterea de certificate avansate necalificate în mediul acestora); asemenea AC-uri de nivel 2 sunt semnate de AC-urile interne AlfaTrust și funcționează sub controlul politicilor AlfaTrust.

Componente și echipamente cheie: Toate operațiunile sensibile ale infrastructurii (generarea de chei, semnarea certificatelor și a listelor de revocare, emiterea mărcilor temporale) sunt realizate pe module criptografice hardware securizate (**HSM – Hardware Security Module**) de înaltă siguranță. HSM-urile utilizate sunt conforme cel puțin cu cerințele standardului *FIPS PUB 140-2 Level 3* (sau echivalent Common Criteria EAL4+), asigurând protecția cheilor private împotriva accesului neautorizat. Cheile private ale autorităților de certificare nu părăsesc niciodată modulul HSM în formă necriptată; de asemenea, sunt implementate mecanisme de control dual și secret sharing (scheme de tip *k din n*) pentru operațiunile cheie precum activarea HSM sau backup-ul cheilor, astfel încât nicio persoană individuală să nu poată accesa sau activa singură componentele critice. HSM-urile sunt instalate în centre de date securizate, fiind protejate fizic și logic.

Sisteme IT și software: AlfaTrust utilizează sisteme informatice redundante și **software PKI** specializat pentru gestionarea ciclului de viață al certificatelor (cereri de certificat, emitere, revocare, managementul listelor de revocare și al serverelor OCSP, emiterea de timestamp-uri etc.). Serverele care găzduiesc aceste servicii rulează sisteme de operare întărite (hardened) și aplicații de securitate conforme standardelor industriei. Există separare strictă între mediile de producție și cele de test, precum și segmentarea rețelei pentru a izola componentele critice (de ex., serverele AC și HSM-urile sunt într-o rețea securizată separată, cu acces restricționat). Datele critice (de ex. jurnalele de audit, baza de date a certificatelor) sunt replicate în timp real pe sisteme de backup.

Centru de date primar și secundar: Infrastructura AlfaTrust este găzduită într-un **centru de date principal**, cu condiții de securitate fizică și ambientală adecvate (control acces biometric, supraveghere video, alimentare electrică neîntreruptă – UPS și generatoare, sisteme de climatizare și detecție/stingere incendii etc.). În plus, pentru asigurarea continuității serviciilor, există un **centru de date secundar** aflat la o locație alternativă, la o distanță suficient de mare față de centrul primar pentru a nu fi afectat simultan de același dezastru regional. Acesta funcționează ca sit de recuperare în caz de dezastru și preia operațiunile critice

în situația indisponibilității centrului primar. Datele esențiale (inclusiv copiile de siguranță criptate ale cheilor și bazelor de date) sunt păstrate sincronizat sau prin replicare periodică în locația secundară. Procedurile de **backup și restaurare** prevăd realizarea de backup-uri integrale săptămânale și incrementale zilnice, stocate atât on-site cât și off-site (în locația secundară), în recipiente securizate, pentru a putea restaura integral sistemele în caz de nevoie.

Rețeaua de distribuție și înregistrare: AlfaTrust are desemnate una sau mai multe **Autorități de Înregistrare (AI)**, responsabile cu validarea identității solicitanților de certificate. AI poate fi chiar personalul intern AlfaTrust (pentru cererile procesate la sediile AlfaTrust) și/sau parteneri autorizați (distribuitori, ofițeri de registru) împuterniciți prin contract să efectueze înregistrarea utilizatorilor finali în numele AlfaTrust. Indiferent de formulă, toate autoritățile de înregistrare respectă aceleași politici și proceduri de identificare stabilite de AlfaTrust (verificarea documentelor de identitate, înregistrarea informațiilor necesare, obținerea consimțământului utilizatorului etc.). Informațiile și documentele colectate de AI sunt transmise securizat către AC-ul emitent relevant.

Baza de date a certificatelor și serviciile de status: Ca parte a infrastructurii sale, AlfaTrust menține o **bază de date actualizată a certificatelor** emise, care include informații despre starea fiecărui certificat (valid, revocat, expirat etc.). Această bază de date stă la baza serviciilor de validare a statusului oferite (liste de revocare – CRL, și răspunsuri OCSP în timp real). Orice certificat revocat este înscris imediat în baza de date și comunicat prin listele de revocare publice și serverul OCSP, în maximum 24 de ore de la solicitarea de revocare (în practică, de obicei mult mai rapid). Serverul OCSP al AlfaTrust este disponibil permanent, permițând terților să obțină gratuit informații despre valabilitatea oricărui certificat emis, pe toată durata de viață a acestuia și o perioadă după expirare.

Mențiuni suplimentare: Infrastructura tehnică este proiectată și operată în conformitate cu cerințele de securitate din standardele ETSI EN 319 401 și ETSI EN 319 411-1 (inclusiv cerințele de infrastructură și management al cheilor), respectiv ETSI EN 319 421 pentru serviciul de marcare temporală. Toate echipamentele critice sunt supuse mentenanței periodice, actualizărilor de securitate și monitorizării 24/7 pentru detectarea promptă a oricăror incidente sau anomalii.

5. POLITICI INTERNE ȘI CONTROALE DE SECURITATE

AlfaTrust Certification S.A. dispune de un cadru solid de **politici interne de securitate și proceduri** care guvernează toate aspectele furnizării serviciilor de încredere, în conformitate cu un Sistem de Management al Securității Informației (**ISMS**) implementat. Politicile interne sunt aliniate standardelor internaționale (precum ISO/IEC 27001) și cerințelor specifice din standardele ETSI pentru prestatori de servicii de încredere. Dintre documentele interne relevante, menționăm: **Politica de securitate a informației - ATC-PS-18 "Managementul Securității Informațiilor"** (care definește obiectivele și măsurile generale de securitate), **Codul de Practici și Proceduri (CPP)** al AlfaTrust (document intern ce detaliază procesele operaționale și de securitate pentru toate serviciile), **Politica de certificare** pentru certificatele emise (care precizează condițiile și criteriile de emiterie/utilizare a certificatelor, inclusiv profilul certificatelor și OID-urile politicilor de certificare) și **Politica de marcare temporală** (care stabilește regulile specifice pentru serviciul de timestamp). Aceste politici sunt ținute la zi și aprobate de managementul AlfaTrust, și stau la baza conformității cu cerințele legale. În continuare este prezentată, sumar, abordarea AlfaTrust privind controalele de securitate și organizatorice:

- **Măsuri criptografice:** Generarea perechilor de chei criptografice pentru AC-uri și TSA se efectuează într-un mediu controlat, folosind algoritmi și parametri considerați siguri la momentul

actual (ex.: RSA 2048/3072 sau ECC curba P-256/P-384 sau funcții hash SHA-256). Cheile private ale autorităților și ale dispozitivelor de sigiliu/semnătură sunt protejate pe HSM-uri conforme FIPS 140-2 nivel 3. Se aplică proceduri de viață a cheilor (generare, distribuire, backup, distrugere la sfârșitul vieții) documentate în CPP. Cheile de semnătură ale autorităților de certificare au o valabilitate limitată, fiind reînnoite periodic conform politicii (de exemplu, la fiecare 5 ani), iar schimbarea cheilor este planificată astfel încât să nu afecteze continuitatea validării certificatelor emise (există suprapuneri de valabilitate și notificări prealabile către utilizatori, după caz).

- **Securitate fizică:** Echipamentele critice (servere AC, HSM-uri, servere de baze de date) sunt amplasate în spații securizate, cu control strict al accesului fizic. Doar personalul autorizat are acces în zona securizată, pe baza de card de acces. Spațiile sunt monitorizate video și păzite. Există sisteme de detecție și stingere a incendiilor (ex.: senzori de fum, gaz inert de stingere) și sisteme de climatizare redundantă pentru menținerea parametrilor de mediu optimi. Protecția împotriva inundațiilor sau altor factori de mediu este de asemenea asigurată (echipamentele critice sunt montate în rack-uri ridicate de la sol etc.). Medii de stocare ce conțin informații sensibile (de ex. unități de backup, hard-disk-uri scoase din uz) sunt manipulate și distruse conform procedurilor, pentru a preveni scurgerile de informații.
- **Controale procedurale și de personal:** AlfaTrust a definit funcții de încredere clare în cadrul organizației, evitând concentrarea excesivă a accesului la operațiuni critice în mâna unei singure persoane. Sunt implementate principiile **separării atribuțiilor** (*segregation of duties*) și **necesității de a cunoaște** (*need-to-know*). Anumite operațiuni importante (ex.: generarea cheilor AC, activarea HSM, aprobarea cererilor de certificare) necesită prezența concomitentă a două sau mai multe persoane autorizate, fiecare cu rol distinct (control dual). Personalul care ocupă roluri critice (ofițeri de registru, administratori de sistem, ofițeri de securitate, auditori interni etc.) este supus unor verificări prealabile la angajare (verificarea antecedentelor, experienței și calificărilor) și semnează acorduri de confidențialitate. De asemenea, toți angajații și colaboratorii implicați în servicii de încredere urmează periodic programe de pregătire și conștientizare în domeniul securității informației, protecției datelor și al reglementărilor eIDAS. Orice încălcare a politicilor de securitate de către personal atrage sancțiuni disciplinare, conform politicilor interne.
- **Securitatea sistemelor IT și a rețelei:** Toate sistemele informatice ale AlfaTrust sunt configurate cu măsuri de securitate cibernetică adecvate. Aceasta include utilizarea de **firewall-uri** la frontiera rețelei, segmentarea rețelelor interne, sisteme de detecție/prevenție a intruziunilor (IDS/IPS), precum și monitorizarea continuă a jurnalelor de securitate. Sistemele critice rulează doar serviciile esențiale, minimizând suprafața de atac, iar actualizările de securitate (patch-uri) sunt aplicate în mod controlat, în timp util. Se folosesc mecanisme de **control al accesului** logic bazat pe autentificare cu parolă puternică și, acolo unde este posibil, autentificare cu doi factori pentru administratori. Accesul administratorilor la servere și HSM-uri este jurnalizat și restricționat la o consolă securizată.

- **Înregistrarea evenimentelor și audit:** AlfaTrust menține jurnale (log-uri) detaliate pentru toate evenimentele relevante din sistem: emisii de certificate, cereri de revocare, emiterea listelor CRL și a răspunsurilor OCSP, accesul administratorilor, alarme de securitate etc. Jurnalele sunt protejate împotriva modificării și sunt păstrate pe o durată adecvată (minim 10 ani pentru evenimente legate de certificate calificate, conform cerințelor legale). Aceste înregistrări pot servi ca dovezi în investigarea incidentelor de securitate sau în eventuale proceduri legale. De asemenea, se efectuează **audituri interni** periodice pentru a verifica respectarea procedurilor de securitate. Conform art. 20 din eIDAS și legislației naționale, AlfaTrust este supusă și unui **audit extern de conformitate** la fiecare 24 de luni sau ori de câte ori este necesar (de ex., în cazul unor modificări majore sau al extinderii serviciilor). Auditul extern este realizat de un organism de evaluare a conformității acreditat, care verifică respectarea tuturor cerințelor eIDAS (inclusiv cele legate de securitate, procese, personal, protecția datelor etc.) și ale standardelor ETSI aplicabile. Rapoartele de audit sunt transmise organismului de supraveghere (ADR) și neconformitățile, dacă apar, sunt remediate cu celeritate.
- **Continuitate și recuperare în caz de dezastru:** AlfaTrust a implementat un **Plan de continuitate a afacerii (BCP)** și un **Plan de recuperare în caz de dezastru (DRP)**, care acoperă scenarii de indisponibilitate majoră a sistemelor sau a personalului cheie (ex.: dezastru naturale, incidente de securitate cibernetică grave, pană extinsă de curent etc.). Aceste planuri prevăd proceduri de trecere în locația secundară, restaurarea sistemelor din backup și reluarea operațiunilor într-un interval de timp cât mai scurt, cu prioritate pe serviciile esențiale precum validarea certificatelor și emiterea de marcaje temporale. Exerciții de tip *disaster recovery* sunt efectuate periodic pentru a testa eficiența planurilor și pregătirea echipei. De asemenea, există un plan specific de încheiere controlată a activității în eventualitatea puțin probabilă a încetării definitive a serviciilor AlfaTrust (vezi secțiunea *Încetarea serviciilor*).
- **Confidențialitate și integritate:** Orice informație sensibilă deținută de AlfaTrust (inclusiv datele personale ale clienților, cheile publice, jurnalele de audit) este tratată cu confidențialitate și în conformitate cu principiul integrității. Angajații au acces la date conform rolurilor lor și doar în scopul îndeplinirii sarcinilor de serviciu. Transmiterea datelor se face prin canale securizate (criptare TLS pentru comunicările externe, rețele private virtuale VPN pentru legăturile dintre locații). Politica de securitate interzice expres divulgarea neautorizată a datelor despre clienți sau a configurației de securitate a sistemelor. Integritatea certificatelor și a semnăturilor/mărcilor emise este protejată prin mecanisme criptografice robuste și prin respectarea strictă a procedurilor de operare.

Prin ansamblul acestor controale și politici, AlfaTrust se asigură că nivelul de securitate este proporțional cu riscurile asociate și că serviciile de încredere sunt furnizate într-un mod sigur, fiabil și conform cu cerințele legale și de standard aplicabile.

6. RESPONSABILITĂȚI ALE PĂRȚILOR IMPLICATE

Pentru asigurarea funcționării corecte a ecosistemului de certificare, DPSI definește obligațiile și responsabilitățile principale ale fiecărei categorii de actori implicați în furnizarea și utilizarea serviciilor de încredere AlfaTrust. Aceste responsabilități sunt asumate prin contracte, termeni și condiții sau prin politicile aplicabile, astfel încât fiecare parte să înțeleagă rolul și așteptările ce-i revin:

- **Prestatorul de Servicii de Încredere (Autoritatea de Certificare – AC):** AlfaTrust Certification S.A., în calitate de AC calificată, are obligația de a respecta toate cerințele legale în vigoare și angajamentele față de utilizatori. Principalele responsabilități includ: (1) verificarea corespunzătoare a identității solicitanților de certificate înainte de emitere (direct sau la distanță prin utilizarea mijloacelor video conform Procedurii adoptate prin Decizia Președintelui ADR cu nr. 564/2021 sau alt act normativ ulterior); (2) emiterea certificatelor în conformitate cu politicile declarate, (3) asigurarea disponibilității mecanismelor de verificare a stării certificatelor (CRL/OCSP) pe tot parcursul valabilității acestora, (4) aplicarea imediată a revocărilor la solicitare sau când apar motive întemeiate; (5) menținerea securității cheilor private ale AC și TSA, înregistrarea și păstrarea informațiilor relevante despre servicii (jurnale) pentru perioada necesară; (6) precum și protejarea datelor cu caracter personal ale utilizatorilor. AC trebuie să notifice în prealabil autoritatea de supraveghere (ADR) despre orice schimbare semnificativă în serviciile calificate furnizate sau despre intenția de încetare a activității. De asemenea, se angajează să remedieze prompt orice neconformitate identificată în urma auditului de conformitate.
- **Autoritatea de Înregistrare (AI):** AI (internă sau partener extern autorizat) are responsabilitatea de a identifica și valida potențialii titulari de certificate în conformitate cu procedurile AlfaTrust. Aceasta implică verificarea documentelor de identitate originale ale persoanelor fizice și/sau a documentelor de înființare și împuternicire pentru persoanele juridice, colectarea datelor necesare (nume complet, CNP sau identificator echivalent, adresa, reprezentant legal etc.), informarea persoanei vizate cu privire la prelucrarea datelor sale personale (în conformitate cu art. 13 din Regulamentul UE 679/2016 – GDPR) și pentru termenii și condițiile serviciului. AI trebuie să asigure acuratețea informațiilor introduse în cererea de certificare și transmiterea securizată a acestor date către AC. Autoritatea de Înregistrare are obligația de confidențialitate față de datele procesate și de respectare a politicilor de securitate AlfaTrust. În plus, AI oferă suport solicitanților, explicându-le drepturile și obligațiile ce le revin ca deținători de certificate. În cazul identificării la distanță (dacă este utilizată), AI trebuie să urmeze procedurile speciale avizate (vezi secțiunea *Identificarea la distanță*).
- **Autoritatea de Marcare Temporală (TSA):** TSA AlfaTrust este responsabilă de emiterea de mărci temporale exacte și securizate. TSA are obligația să mențină sincronizarea sursei interne de timp cu standardul de timp universal (UTC) prin intermediul unor ceasuri precise calibrate (de ex. servere NTP legate la surse de timp etalon). TSA trebuie să se asigure că fiecare marcă temporală emisă reflectă corect momentul emiterii și este semnată cu cheia privată a TSA corespunzătoare, aflată sub controlul exclusiv al AlfaTrust. De asemenea, TSA are responsabilitatea de a păstra un jurnal al tuturor mărcilor temporale emise, pentru a putea demonstra, la nevoie, momentul exact

al emisie acestora și integritatea serviciului. În caz de compromitere sau suspiciune de compromitere a cheii TSA, aceasta are obligația de a înceta imediat emiterea mărcilor temporale cu acea cheie și de a informa utilizatorii și autoritatea de supraveghere, generând dacă este cazul o pereche de chei nouă și un nou certificat TSA.

- **Autoritatea de Validare (serviciul de verificare a stării certificatelor)** (*dacă este oferită distinct ca serviciu calificat*): Autoritatea de Validare (AV) are responsabilitatea de a furniza terților rapoarte de validare a semnăturilor electronice sau a certificatelor, conform Regulamentului eIDAS. În contextul AlfaTrust, funcționalitatea de validare se realizează în principal prin OCSP/CRL (automatizat); și implică verificarea elementelor specifice prevăzute de lege (valabilitatea certificatului, integritatea semnăturii, ne-revocarea la momentul semnării, identitatea semnatarului etc.) și să furnizeze un răspuns de binar, **adevărat sau fals**, cu privire la validitatea unei semnături, însoțit de o dovadă (sigiliu electronic calificat al raportului de validare). AV are obligația de obiectivitate și acuratețe, precum și de păstrare a jurnalelor de validare.
- **Utilizatorul final (Titularul certificatului)**: Fiecare deținător de certificat (persoană fizică sau juridică) are o serie de obligații asumate prin contractul/termenii de utilizare semnați cu AlfaTrust. Aceste responsabilități includ, dar fără a se limita la: (1) furnizarea de informații corecte și complete pe durata înregistrării (orice modificare relevantă, precum schimbarea numelui, trebuie comunicată în timp util pentru re-emitere sau actualizare dacă este cazul); (2) cunoașterea, înțelegerea și respectarea termenilor și condițiilor de utilizare a certificatului și a dispozitivului securizat (token) furnizat; (3) utilizarea certificatului numai în scopurile permise (de exemplu, un certificat calificat de semnătură este folosit doar de titularul persoană fizică pentru semnare, nu și de alte persoane); (4) menținerea securității cheii private asociate certificatului – ceea ce implică păstrarea în siguranță a dispozitivului calificat și a codului PIN/parolei; (5) neîmpărtășirea acestora cu terțe persoane și raportarea imediată către AlfaTrust a oricărei suspiciuni de compromitere (pierdere/furt al token-ului, divulgarea parolei etc.). Utilizatorul final este responsabil să solicite revocarea certificatului fără întârziere dacă datele de identitate înscrise devin inexacte sau dacă securitatea cheii private este compromisă. De asemenea, utilizatorul final trebuie să verifice la rândul său valabilitatea și statutul propriului certificat înainte de a-l folosi pentru semnare, mai ales dacă știe că ar fi existat motive de revocare. În relația cu terții, titularul consimte ca informațiile din certificatul său (ex. numele, cheia publică) să fie publice și disponibile pentru verificarea semnăturilor.
- **Entități partenere și părți terțe ce se încred în certificate (Relying Parties)**: Aceasta categorie include orice terț care primește o semnătură sau sigiliu electronic generat cu un certificat AlfaTrust și decide să se bazeze pe acesta. Entitățile partenere (ex.: instituții care validează semnăturile angajaților proprii, platforme care integrează servicii AlfaTrust etc.) și în general toți utilizatorii finali ai documentelor semnate au următoarele responsabilități: să **verifice autenticitatea și statusul** oricărui certificat AlfaTrust pe care se bazează (prin consultarea listei de revocare sau interogarea OCSP în momentul validării semnăturii) – această obligație este esențială, întrucât a se încrede într-un certificat expirat sau revocat poate invalida semnătura; să țină cont de

eventualele limitări ale certificatelor, precizate în DPSI sau în certificatul însuși (de ex., dacă un certificat are mențiuni de utilizare restrânsă sau o anumită limită de valoare a tranzacției – deși certificatele calificate general nu au astfel de limitări impuse de prestator, terții trebuie să fie atenți la orice clauze); să utilizeze mijloace software conforme standardelor pentru a verifica semnăturile. Terțele părți (astfel cum sunt definite în contextul prezentei secțiuni) au, de asemenea, responsabilitatea de a se informa asupra termenilor și condițiilor serviciilor AlfaTrust (document ce este public și disponibil pe site-ul AlfaTrust), unde sunt detaliate obligațiile prestatorului și eventualele limitări de răspundere. Prin folosirea semnăturilor bazate pe certificate AlfaTrust, terții acceptă implicit condițiile de utilizare a acestora.

Toate părțile menționate mai sus trebuie să coopereze și să acționeze cu bună-credință în scopul menținerii unui mediu de încredere. AlfaTrust publică în mod accesibil **obligațiile fiecărei părți** (în documentația publică – DPSI, politică de certificare, termenii și condiții etc.), astfel încât fiecare participant să-și cunoască responsabilitățile înainte de a folosi serviciul.

7. ANGAJAMENTELE ASUMATE DE ALFATRUST (PRESTATORUL)

AlfaTrust Certification S.A., în calitate de prestator calificat de servicii de încredere, își asumă în mod formal o serie de angajamente și garanții față de utilizatorii serviciilor și față de autorități, pentru a asigura calitatea și legalitatea serviciilor furnizate. Aceste angajamente decurg din cerințele legale (Regulamentul eIDAS, legea națională) și din propriile politici interne ale AlfaTrust. Principalele angajamente asumate sunt:

- **Conformitate legală și standardizare:** AlfaTrust se angajează să respecte în totalitate Regulamentul (UE) nr. 910/2014 (eIDAS) și legislația română incidentă, precum Legea 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea (inclusiv cerințele Autorității de Supraveghere – ADR). Prestatorul menține certificarea ca **prestator calificat** și demonstrează conformitatea prin auditurile periodice prevăzute de lege. De asemenea, serviciile sunt oferite în concordanță cu standardele europene ETSI aplicabile (EN 319 401, 319 411, 319 421 etc.), astfel încât să existe interoperabilitate și recunoaștere la nivel european.
- **Calitatea serviciilor și continuitate:** Prestatorul garantează că serviciile de încredere vor fi furnizate într-un mod fiabil și neîntrerupt, exceptând perioadele de mentenanță anunțate sau cazurile de forță majoră. Infrastructura este proiectată cu redundanță pentru a maximiza disponibilitatea. Există angajamentul că, în situația puțin probabilă a unei întreruperi majore a serviciilor, AlfaTrust va depune toate eforturile necesare pentru a restaura serviciile în cel mai scurt timp și pentru a minimiza impactul asupra utilizatorilor. În plus, AlfaTrust menține un plan de încetare a serviciilor actualizat care asigură continuitatea sau închiderea controlată a serviciilor, în conformitate cu cerințele eIDAS (detalii în secțiunea *Încetarea serviciilor*).
- **Transparență și informare:** AlfaTrust se obligă să informeze în mod clar și complet orice persoană care intenționează să utilizeze un serviciu de încredere cu privire la termenii și condițiile de

utilizare ale serviciului respectiv, inclusiv eventuale limitări ale utilizării. Acest angajament corespunde art. 24(2) lit. d din eIDAS. În practică, înainte de emiterea unui certificat calificat, utilizatorul final primește și acceptă Termenii și Condițiile de utilizare, care precizează drepturile și obligațiile, limitările de răspundere, politicile de securitate etc. Termenii și Condițiile, precum și DPSI și politicile de certificare, sunt publicate pe site-ul AlfaTrust și sunt ușor accesibile. De asemenea, AlfaTrust își ia angajamentul de a notifica prompt utilizatorii în legătură cu orice schimbare relevantă și semnificativă a condițiilor serviciului sau a politicilor (de ex., modificări legislative ce afectează serviciul, schimbarea algoritmilor criptografici suportați etc.).

- **Securitatea soluțiilor tehnice:** Prestatorul garantează că utilizează sisteme și produse de încredere, protejate împotriva modificărilor neautorizate, și că ia măsuri adecvate pentru a asigura securitatea tehnică și fiabilitatea proceselor suportate. Aceasta implică menținerea la zi a soluțiilor de securitate, utilizarea HSM certificați, aplicarea de patch-uri, revizuirea arhitecturii pentru a face față noilor amenințări etc. AlfaTrust își asumă obligația de a prevenii și de a combate fraudele, falsificarea certificatelor sau furtul de date, prin controalele descrise în DPSI. În eventualitatea apariției unui incident de securitate, AlfaTrust se angajează să îl gestioneze conform procedurilor și să comunice părților afectate, după cum se detaliază la secțiunea *Gestionarea riscurilor și incidentelor*.
- **Protejarea datelor și confidențialitate:** Un angajament major este asigurarea **prelucrării legale și sigure a datelor cu caracter personal** ale clienților, în conformitate cu Regulamentul General privind Protecția Datelor (GDPR) și art. 24(2) lit. j din Regulamentul UE 910/2014 - eIDAS 1. AlfaTrust prelucrează numai datele strict necesare furnizării serviciilor (ex.: date de identificare pentru emiterea certificatelor) și le păstrează pe durata necesară conform cerințelor legale (de ex. log-uri și documente de identificare timp de 10 ani, conform obligațiilor Regulamentul UE 910/2014- eIDAS și legislației fiscale, dacă aplicabil). Prestatorul asigură confidențialitatea acestor date și nu le utilizează în alte scopuri decât cele declarate, nici nu le divulgă către terți neautorizați. Utilizatorii sunt informați cu privire la Politica de confidențialitate și de prelucrare a datelor cu caracter personal a AlfaTrust, ce detaliază drepturile lor (dreptul de acces, rectificare, ștergere etc.) și măsurile de protecție implementate. Personalul AlfaTrust este instruit și obligat prin contract să mențină confidențialitatea datelor clienților.
- **Răspundere și resurse financiare:** AlfaTrust își asumă răspunderea legală pentru prejudiciile cauzate intenționat sau din neglijență în furnizarea serviciilor sale, în limitele prevăzute de art. 13 din Regulamentul UE 910/2014- eIDAS. Pentru a acoperi riscul de răspundere civilă, AlfaTrust menține resurse financiare suficiente și/sau o asigurare de răspundere civilă adecvată, conform cerințelor legale. Aceasta înseamnă că utilizatorii prejudiciați ca urmare a neîndeplinirii obligațiilor de către AlfaTrust pot primi compensații, sub rezerva termenilor contractuali și a prevederilor legale. (De exemplu, dacă un certificat calificat este emis fără verificarea corespunzătoare a identității și cauzează un prejudiciu unei terțe părți, AlfaTrust poate fi trasă la răspundere.) În același timp, AlfaTrust precizează în termenii și condițiile serviciului eventualele excluderi sau limitări de răspundere permise de lege (de pildă, neacoperirea prejudiciilor rezultate din utilizarea

incorectă a certificatului de către titular, sau din încrederea nejustificată a unei terțe părți fără verificarea statusului certificatului).

- **Suport și cooperare:** Prestatorul se angajează să ofere asistență rezonabilă utilizatorilor și părților terțe cu privire la utilizarea serviciilor. Există canale de suport (telefon, email) prin care utilizatorii pot solicita informații sau raporta probleme, iar AlfaTrust se obligă să răspundă prompt acestor solicitări. Totodată, AlfaTrust cooperează activ cu **organismele de supraveghere** și cu **autoritățile competente** (ex.: ADR, CERT-RO, ANSPDCP în domeniul datelor personale) în privința oricăror verificări, raportări de incidente sau investigații, furnizând informațiile necesare acestora.
- **Îmbunătățire continuă:** AlfaTrust își asumă angajamentul de a revizui și îmbunătăți continuu practicile sale, ținând cont de evoluția tehnologică, de schimbările de reglementare și de feedback-ul primit de la părțile interesate. Acest lucru include actualizarea periodică a DPSI, a politicilor de securitate și a procedurilor interne, pentru a reflecta cele mai bune practici și pentru a remedia eventualele deficiențe identificate. Prestatorul menține un dialog deschis cu comunitatea de utilizatori și parteneri, încurajând raportarea responsabilă a oricăror vulnerabilități sau probleme identificate în cadrul serviciilor sale, și tratează cu seriozitate aceste semnalări în vederea rezolvării lor.

În concluzie, prin aceste angajamente asumate, AlfaTrust Certification S.A. își demonstrează dedicarea față de furnizarea unor servicii de încredere de înaltă calitate, sigure și aliniate cadrului legal, astfel încât utilizatorii să poată avea încredere deplină în semnăturile, sigiliile și mărcile temporale pe care le utilizează.

8. IDENTIFICAREA LA DISTANȚĂ A SOLICITANȚILOR

Identificarea solicitanților reprezintă un pas esențial în procesul de emitere a certificatelor digitale. Conform Regulamentului eIDAS, identificarea inițială a persoanelor cărora li se emit certificate calificate trebuie realizată **fie prin prezență fizică, fie prin mijloace la distanță echivalente ca nivel de siguranță**. În mod tradițional, AlfaTrust efectuează identificarea prin prezența fizică a solicitantului în fața unui operator (autoritate de înregistrare) care verifică actul de identitate original și, dacă este cazul, documentele entității juridice și mandatul reprezentantului respectivei entități. Totuși, având în vedere evoluțiile tehnologice și nevoile clienților, AlfaTrust oferă și opțiunea **identificării la distanță**, în condițiile permise de cadrul legal național, pentru emiterea certificatelor calificate.

Dacă solicitantul nu poate fi prezent fizic și dorește să utilizeze mijloace video de identificare la distanță, AlfaTrust implementează următoarele metode aprobate:

- **Identificare prin certificate calificate existente:** O altă metodă acceptată este identificarea persoanei pe baza **unei semnături electronice calificate** deținute deja de aceasta (emise anterior, de către AlfaTrust sau alt prestator de servicii de încredere calificat). De exemplu, dacă solicitantul deține un certificat calificat valid, poate semna electronic o solicitare/declarație în care își confirmă identitatea și acordul, iar AlfaTrust poate verifica validitatea acelei semnături calificate. Această abordare echivalează cu identificarea față în față, întrucât semnătura calificată are deja la bază o identificare anterioară. Desigur, trebuie ca domeniul de aplicare al certificatului existent să permită o astfel de utilizare, iar solicitantul să fie de acord.

- **Identificare prin video-identificare (online video KYC):** În conformitate cu reglementările naționale (ex: proceduri aprobate de ADR - **Norma din 2021 privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video** aprobată prin Decizia Președintelui ADR cu nr. 564/2021), AlfaTrust poate folosi un proces securizat de video-identificare. Acest proces implică o sesiune video în direct cu solicitantul, în care un operator autorizat verifică identitatea prin compararea feței cu fotografia din documentul de identitate prezentat la cameră și prin întrebări de securitate. Sesiunea video este înregistrată și stocată ca dovadă. Totodată, se pot folosi mecanisme suplimentare anti-fraudă (ex.: captura de imagini ale actului de identitate în diverse poziții, verificări automate ale elementelor de siguranță ale actului, apelarea unei baze de date oficiale pentru validarea CNP-ului etc.). Această metodă se realizează conform **Procedurii de identificare a persoanei la distanță utilizând mijloace video** aprobată de autoritatea de reglementare și asigură un nivel de încredere echivalent prezenței fizice în baza dispozițiilor legale anterior citate, sau eventual, cele care le înlocuiesc.

Indiferent de metoda la distanță folosită, AlfaTrust impune ca:

- Procesul să fie securizat (comunicare criptată, măsuri de prevenire a manipulării sau *spoofing*-ului).
- Identitatea să fie verificată cu cel puțin același grad de rigurozitate ca și în persoană. Dacă există cea mai mică îndoială privind identitatea sau integritatea procesului, solicitantul i se va cere să parcurgă identificarea în mod tradițional (prezență fizică).
- Întregul proces și dovezile asociate (înregistrare video, log-uri, copii ale documentelor) să fie arhivate în siguranță, pentru a demonstra conformitatea identificării la un eventual audit.

Mențiune: În prezent, identificarea la distanță este oferită ca facilitate în special pentru clienții din alte localități sau din străinătate, unde prezența fizică ar fi dificilă. AlfaTrust respectă întocmai prevederile Ordinului ADR și ale altor norme privind identificarea la distanță. Orice limitări sau condiții suplimentare (precum necesitatea utilizării doar a unor metode de video-identificare aprobate) vor fi comunicate solicitanților înainte de inițierea procesului de identificare online.

În concluzie, **identificarea la distanță**, acolo unde este utilizată, se realizează numai prin metode care asigură un nivel de asigurare echivalent identificării în persoană, AlfaTrust având ca prioritate prevenirea emiterii de certificate către identități false sau neverificate.

9. GESTIONAREA RISCURILOR ȘI A INCIDENTELOR DE SECURITATE

Managementul riscurilor: AlfaTrust a instituit un **proces continuu de evaluare și gestionare a riscurilor de securitate** legate de furnizarea serviciilor de încredere, în conformitate cu art. 19 alin. (1) din Regulamentul UE 910/2014 eIDAS și cu standardul ISO 27005 (managementul riscului de securitate informațională) adaptat contextului specific. Acest proces implică identificarea periodică a amenințărilor potențiale (de la atacuri cibernetice, la erori umane sau calamități naturale) și evaluarea vulnerabilităților sistemului. Fiecărui risc i se estimează impactul potențial și probabilitatea de materializare, stabilindu-se un nivel de risc. AlfaTrust implementează măsuri de control pentru a reduce riscurile evaluate la un nivel acceptabil – aceste măsuri includ cele descrise în secțiunea de securitate (controale tehnice, procedurale, politice).

Riscurile reziduale (cele rămase după aplicarea controalelor) sunt monitorizate și revizuite de conducerea AlfaTrust în cadrul ședințelor periodice de analiză a riscurilor (ex.: cel puțin anual sau ori de câte ori intervine o schimbare semnificativă – apariția unei noi vulnerabilități majore, modificări legislative, extinderea serviciilor etc.). Planurile de tratament al riscurilor sunt aprobate de management și implementate de personalul tehnic desemnat.

Pe lângă riscurile deliberate (atacuri), se acordă atenție și riscurilor accidentale sau de eroare: de exemplu, riscul de indisponibilitate din cauza unei pene de curent prelungite este atenuat prin alimentare UPS și generator; riscul de eroare umană la introducerea datelor este atenuat prin proceduri de dublă verificare; riscul de compromitere a unui HSM este atenuat prin mecanisme de protecție fizică și monitorizare etc. Astfel, se urmărește ca nivelul de securitate să fie proporțional cu riscurile identificate, actualizat la stadiul tehnologic și la vectorii de atac emergenți.

Gestionarea incidentelor de securitate: În pofida tuturor măsurilor preventive, pot apărea incidente de securitate. AlfaTrust are definită o **Procedură de tratare a incidentelor de securitate**, dar și o **Procedură de gestiune a riscurilor de securitate**, care acoperă detectarea, analiza, soluționarea și raportarea incidentelor. Orice eveniment suspect (de exemplu: acces neautorizat, malware detectat, defecțiuni majore ale echipamentelor, compromiterea sau pierderea integrității datelor) este înregistrat și escaladat către echipa de securitate pentru evaluare.

Pentru incidentele minore (fără impact asupra serviciilor de încredere sau datelor clienților), rezolvarea se face intern, cu documentarea cauzei și remedierea pentru a preveni recurența. Pentru incidentele majore – definite ca acelea care au sau pot avea un impact semnificativ asupra serviciilor de încredere furnizate sau asupra datelor cu caracter personal gestionate, AlfaTrust urmează cerințele legale de notificare. Conform art. 19 alin. (2) din Regulamentul UE 910/2014 - eIDAS, prestatorul va **notifica fără întârzieri nejustificate, dar nu mai târziu de 24 de ore de la constatare**, organismul de supraveghere (ADR) cu privire la orice breșă de securitate sau pierdere a integrității cu impact semnificativ. În notificare se vor preciza natura incidentului, serviciile afectate, măsurile luate sau planificate și eventual impactul estimat. Dacă incidentul este susceptibil să afecteze și utilizatorii (persoanele cărora le-au fost furnizate serviciile) – de exemplu compromiterea unei chei private de AC care invalidează certificatul, sau divulgarea datelor personale ale clienților – AlfaTrust va **informa și utilizatorii afectați**, de asemenea fără întârzieri nejustificate.

Exemple de situații ce ar declanșa notificarea includ: compromiterea evidentă a cheii private a unei autorități de certificare (situație de gravitate maximă, ce implică revocarea imediată a certificatului autorității compromise și informarea tuturor părților), un atac cibernetic de succes care duce la modificarea neautorizată a datelor din baza de certificate (pierderea integrității), indisponibilitatea prelungită a serviciilor de validare care afectează verificarea semnăturilor, sau acces neautorizat la baza de date conținând informații personale ale clienților.

AlfaTrust cooperează strâns cu autoritățile în investigarea incidentelor. În cazul în care un incident de securitate sau pierdere a integrității afectează mai multe state membre (ex.: certificate emise de AlfaTrust folosite transfrontalier), ADR (ca organism de supraveghere notificat) va informa autoritățile de supraveghere din statele respective, precum și ENISA, dacă este cazul. De asemenea, dacă incidentul implică încălcarea securității datelor cu caracter personal, AlfaTrust va notifica și Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), conform obligațiilor din GDPR (în general în același interval de 72 de ore, ceea ce e acoperit de notificarea în 24h către ADR).

Măsurile post-incident: După gestionarea imediată a unui incident, AlfaTrust efectuează o analiză *a posteriori* pentru a identifica cauzele fundamentale și a implementa acțiuni corective/preventive. De exemplu, dacă un incident a avut drept cauză vulnerabilitatea unui sistem, se va actualiza configurația și se vor revizui procedurile de *patch management*; dacă a fost implicată o eroare umană, se vor oferi sesiuni de re-instruire personalului și se va evalua dacă procedurile trebuie îmbunătățite. Rezultatele și lecțiile învățate din incidente sunt documentate și folosite pentru a evita situații similare în viitor.

Continuitatea operațională în caz de incident: Planurile de continuitate amintite anterior (BCP/DRP) fac parte integrantă din gestionarea riscurilor și incidentelor. În cazul unui incident major care conduce la indisponibilitatea infrastructurii primare, se va activa centrul secundar, asigurându-se că serviciile critice (precum OCSP, site-ul de publicare a CRL) rămân funcționale sau revin online într-un timp cât mai scurt (de ordinul orelor). Prioritatea este protejarea integrității certificatelor emise și menținerea încrederii publice în servicii, chiar dacă apar dificultăți tehnice.

În concluzie, AlfaTrust tratează cu maximă seriozitate atât **proactiv, cât și reactiv** securitatea serviciilor sale. Printr-un management riguros al riscurilor și un plan robust de răspuns la incidente, utilizatorii pot avea încredere că eventualele incidente sunt prevenite pe cât posibil, iar dacă totuși survin, sunt gestionate prompt, transparent și eficient, cu minimizarea consecințelor asupra lor.

10. PROTECȚIA DATELOR CU CARACTER PERSONAL

În calitate de operator de date cu caracter personal, AlfaTrust Certification S.A. respectă pe deplin legislația aplicabilă în domeniu, în principal Regulamentul UE 679/2016 – Regulamentul general privind protecția datelor (GDPR), precum și prevederile speciale din Regulamentul eIDAS referitoare la protecția datelor (art. 5 și art. 24(2) lit. j). Protecția datelor personale ale solicitanților și utilizatorilor de servicii de încredere este integrată în toate procesele AlfaTrust.

Date colectate și scopuri: AlfaTrust colectează numai datele cu caracter personal necesare furnizării fiecărui serviciu de încredere (principiul reducerii la minim al datelor – art. 5 alin. (1) lit. c) din Regulamentul UE 679/2016 - GDPR. În cazul certificatelor de semnătură acestea includ de obicei: numele complet al persoanei, iar în cazul certificatelor emise către o persoană juridică – denumirea organizației și atribuirea certificatului către aceasta, adresa sau sediul (dacă este relevant), date de contact (email, telefon) pentru comunicări privind serviciul, și elemente legate de verificarea identității (tipul și seria actului de identitate, documente suport). Toate aceste date sunt folosite exclusiv în scopul: validării identității și emiterii certificatelor, menținerii evidențelor operaționale (inclusiv jurnalul de emisii și revocări), contactării utilizatorilor privind serviciul (notificări de expirare, anunțuri de securitate, actualizări de termeni) și îndeplinirii obligațiilor legale (de ex., păstrarea de audit trail pentru eventuale cercetări de fraudă sau dispute juridice).

Temei legal și când este utilizat consimțământul ca temei legal: Prelucrarea datelor personale de către AlfaTrust se bazează fie pe **îndeplinirea unei obligații legale** (datoria prestatorului de a verifica identitatea înaintea emiterii unui certificat calificat, conform eIDAS), fie pe **executarea contractului** la care persoana vizată este parte (furnizarea serviciului de încredere solicitat), fie pe **consimțământul explicit** al persoanei vizate, acolo unde acesta este cerut (de exemplu, dacă vor exista prelucrări de date cu caracter personal în scopuri de marketing, separate de furnizarea serviciului, acestea se vor face doar cu consimțământ separat, însă în mod curent AlfaTrust nu folosește datele clienților în scop de marketing direct). Utilizatorii sunt informați cu privire la politica de prelucrare a datelor la momentul colectării; în special, la înregistrare

li se prezintă o Politică de confidențialitate și de prelucrare a datelor cu caracter personal în vederea asigurării cerințelor de informare prevăzute de art. 13 din Regulamentul UE 679/2016 – GDPR, care descrie categoriile de date colectate, scopurile, temeiurile legale, durata de stocare și drepturile lor.

Stocarea și perioada de retenție: Datele personale ale clienților (inclusiv copiile de pe documentele de identitate, formularele de cerere, log-urile de verificare) sunt stocate în medii securizate (baze de date criptate, seifuri de documente fizice sub cheie etc.). AlfaTrust păstrează aceste date **pe durata necesară** conform reglementărilor: de regulă, informațiile legate de emiterea certificatelor calificate și identificarea titularilor se păstrează **minim 10 ani** de la încetarea valabilității certificatului, deoarece atât eIDAS, cât și cerințele comerciale (ex. prevederile legale contabile, fiscale, civile referitoare la eventuale termene de prescripție sau cele referitoare la securitatea cibernetică) impun menținerea evidențelor pe termen lung. După expirarea perioadei de retenție, datele sunt șterse sau anonimizate ireversibil, conform procedurilor interne.

Securitatea datelor personale: Măsurile tehnice și organizatorice detaliate în secțiunea de securitate a DPSI (control acces, criptare, confidențialitate personal etc.) se aplică în mod direct protecției datelor personale. În plus, AlfaTrust limitează accesul la datele personale doar la acei angajați care trebuie să le proceseze pentru scopurile declarate (principiul *need-to-know*). Toate persoanele care au acces la astfel de date (inclusiv eventuali subcontractori de încredere – ex. auditori externi, consultanți tehnici sau juridici dacă au nevoie de acces) sunt supuse obligațiilor de confidențialitate. Sistemele care prelucrează date personale sunt monitorizate pentru acces neautorizat, iar transferul datelor (inclusiv între Autoritatea de Înregistrare și AC) este criptat. AlfaTrust efectuează teste periodice de securitate (inclusiv evaluări de vulnerabilitate și, la nevoie, teste de penetrare) pentru a asigura că datele clienților rămân protejate împotriva accesului neautorizat sau a divulgării neautorizate.

Drepturile persoanelor vizate: AlfaTrust garantează persoanelor vizate (utilizatorilor) exercitarea tuturor drepturilor prevăzute de GDPR: dreptul de informare și acces la propriile date (utilizatorul poate solicita o copie a datelor sale prelucrate – de ex. informațiile din formularul de înregistrare, log-urile de emisie etc.), dreptul la rectificare (orice date incorecte sau incomplete pot fi corectate la cerere, deși, datele din certificate nu pot fi modificate după emisie, ci doar se revocă certificatul vechi și se emite unul nou cu datele corecte/actualizate), dreptul la ștergere (poate fi exercitat după expirarea perioadei de valabilitate a certificatului și a obligațiilor legale de retenție/păstrare a datelor cu caracter personal – înainte de acest termen, unele date nu pot fi șterse din motive legale), dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor (în măsura aplicabilității – ex. datele de identificare furnizate pot fi puse la dispoziția utilizatorului într-un format structurat, dacă acesta dorește să le folosească la alt prestator), dreptul de opoziție (de ex., opoziție la prelucrarea datelor în scop de marketing, pe care oricum AlfaTrust nu o face fără consimțământ). De asemenea, persoanele vizate au dreptul să depună plângere la ANSPDCP dacă consideră că drepturile lor au fost încălcate.

Transferuri și divulgări: AlfaTrust, de regulă, nu transferă datele personale ale clienților în afara Spațiului Economic European. Orice eventual transfer (de ex., stocare în cloud externalizată) ar fi realizat doar către entități din țări cu decizie de adecvare sau cu garanții adecvate (clauze standard de protecție) și ar fi notificat în politica de confidențialitate. Dezvăluirea datelor către terți este limitată la situațiile necesare: de exemplu, furnizarea de date către organismele de evaluare a conformității în cadrul auditurilor (aceștia fiind la rândul lor obligați la confidențialitate), răspunsul la solicitări legale din partea autorităților (ex.: organe de urmărire penală, pe baza unei solicitări oficiale în condițiile legii), sau partajarea minimului de date cu partenerii autorizați implicați în procesul de înregistrare. În rest, datele despre certificatele emise care devin publice sunt doar cele strict necesare pentru funcționarea infrastructurii de chei publice –

anume **certIFICATELE ÎN SINE** (care conțin numele titularului, organizația dacă e cazul, și cheia publică – aceste informații sunt inerent publice pentru ca terții să poată verifica semnăturile) și informațiile de status (certIFICATELE REVOCATE SAU EXPIRATE, publicate în CRL/OCSP). Acestea nu sunt considerate divulgări neautorizate, ci fac parte din serviciul de certificare.

Responsabilul cu protecția datelor (DPO): Dat fiind volumul semnificativ de date personale prelucrate (și natura lor, incluzând acte de identitate, CNP etc.), AlfaTrust a numit un **Responsabil cu Protecția Datelor (DPO)** în conformitate cu art. 37 GDPR. Datele de contact ale DPO sunt publicate pe site-ul AlfaTrust și în politica de confidențialitate. Utilizatorii pot contacta DPO pentru orice aspect legat de prelucrarea datelor lor, iar DPO asigură conformitatea internă cu cerințele GDPR și oferă consultanță la proiectarea noilor servicii (pentru a asigura confidențialitatea).

În concluzie, AlfaTrust tratează protecția datelor cu caracter personal ca pe o componentă esențială a serviciilor de încredere. Prin politici stricte, măsuri tehnice de securitate și transparență față de utilizatori, se asigură că datele personale ale acestora sunt în siguranță și prelucrate legal, consolidând încrederea în serviciile oferite.

11. ÎNCETAREA SERVICIILOR ȘI CONTINUITATEA ACTIVITĂȚII

Plan de încetare a activității: AlfaTrust menține un plan actualizat de încetare a furnizării serviciilor de încredere, conform cerințelor eIDAS (art. 24 alin. (2) lit. i) și reglementărilor naționale. Acest plan prevede măsurile ce trebuie luate în eventualitatea în care AlfaTrust decide, sau este nevoită, să înceteze furnizarea unuia sau mai multor servicii de încredere calificate. Scopul principal este protejarea intereselor utilizatorilor și a terților și asigurarea continuității validării semnăturilor existente sau a transferului ordonat al obligațiilor către un succesori.

Notificarea prealabilă: În cazul intenției de încetare a activității ca prestator calificat (sau de încetare a unui anumit serviciu calificat, de exemplu renunțarea la serviciul de marcă temporală calificată), AlfaTrust va notifica:

- **Autoritatea de Supraveghere (ADR):** cu minimum 3 luni (90 de zile) înainte de data propusă a încetării, conform cerințelor legale și contractuale. Notificarea va include motivele încetării, data planificată și planul de măsuri de atenuare.
- **Toți utilizatorii cu certificate active:** cu minimum 30 de zile înainte de încetare. AlfaTrust va transmite fiecărui deținător de certificat (și eventual partenerilor relevanți) o notificare scrisă (prin email și/sau poștă) anunțând încetarea serviciului, data exactă și instrucțiuni privind acțiunile pe care trebuie să le întreprindă (de ex., să își finalizeze semnările înainte de acea dată, să obțină certificate de la alt prestator etc.).

Revocarea certificatelor și oprirea emisiei: La data efectivă a încetării, sau imediat înainte, AlfaTrust va **revoca toate certificatele calificate active** pe care le-a emis și care nu erau expirate anterior datei de încetare. Aceasta pentru a evita existența unor certificate valide fără suportul unui prestator (ceea ce ar crea confuzie cu privire la statusul lor). Revocarea în masă va fi comunicată prin listele de revocare finale și va fi notificată în mod proactiv utilizatorilor. De asemenea, AlfaTrust va **înceta emiterea** oricăror certificate noi cu o anumită perioadă înainte de data încetării (pentru a evita emiterea de certificate cu

durată foarte scurtă și pentru a descuraja noi clienți să se bazeze pe un serviciu care urmează să nu mai fie furnizat).

Transferul responsabilităților către un succesor: Planul de încetare prevede că AlfaTrust va face demersuri pentru a identifica un alt **prestator de servicii de încredere calificat** dispus să preia evidențele și eventual clienții săi. Acest lucru poate include:

- Transferul bazelor de date (certIFICATE emise, jurnale, evidențe de identitate) către un alt prestator de servicii de încredere calificat, sub rezerva respectării GDPR și cu acordul autorității de supraveghere, pentru a asigura accesul continuu la informații de validare.
- Încheierea unui contract de transfer cu succesorul, care să garanteze păstrarea și protecția datelor și furnizarea în continuare a informațiilor de status (de ex. noul prestator ar putea prelua publicarea listelor de revocare pentru certificatele revocate istoric de AlfaTrust, menținând astfel posibilitatea verificării pe termen lung a semnăturilor create în perioada activității AlfaTrust).
- Oferirea certificat echivalent de la succesor fără costuri suplimentare semnificative (în măsura în care succesorul și utilizatorul agreează).

Dacă un transfer complet nu este posibil, AlfaTrust va preda către autoritatea de supraveghere sau o altă entitate neutră (de ex. un depozit național) arhivele necesare (liste de certificate, jurnale) pentru a asigura că, pe durata necesară, terții pot verifica semnăturile realizate cu fostele certificate AlfaTrust.

Informarea publică: AlfaTrust va publica pe website-ul său și prin canale de comunicare publice (ex: comunicat de presă, anunțuri pe portalurile de specialitate) informația despre încetarea serviciilor, astfel încât toți cei interesați (inclusiv cei care nu sunt clienți direcți, dar poate folosesc servicii intermediare bazate pe certificatele AlfaTrust) să poată lua la cunoștință. Această informare publică se va face cu o anticipație suficientă (30-90 de zile înainte, în funcție de canal).

Minimizarea impactului asupra utilizatorilor: AlfaTrust va depune toate eforturile rezonabile pentru a reduce efectele negative asupra utilizatorilor cauzate de încetarea activității. De exemplu, dacă un utilizator are un certificat care ar mai fi fost valabil o perioadă semnificativă (și deci a achitat contravaloarea pentru respectiva perioadă), AlfaTrust poate oferi o **compensație** financiară proporțională (cel mult echivalentul taxelor de emisie nefructificate) sau alte forme de despăgubire convenite. Astfel de detalii vor fi clarificate în notificările trimise utilizatorilor. De asemenea, personalul de suport AlfaTrust va asista utilizatorii în migrarea către alte soluții (furnizând, la cerere, dovezi și documente de identificare pe care le deține, pentru a facilita reînrolarea la alt prestator, în limitele legii).

Încetarea parțială (a unui serviciu specific): Dacă AlfaTrust decide încetarea unuia dintre serviciile sale, dar continuă altele (de ex., renunță la serviciul de marcă temporală calificată dar păstrează serviciile de creare, validare și verificare a semnăturilor electronice), se vor aplica procedurile de mai sus în mod specific pentru acel serviciu. Utilizatorii serviciului respectiv vor fi notificați și li se vor oferi alternative (de ex., un alt prestator de servicii de încredere calificat) sau compensații, după caz. Încetarea parțială va fi anunțată autorității de supraveghere și publicului similar încetării totale.

Forță majoră și revocare excepțională a calificării: În situații extreme, cum ar fi retragerea forțată a calificării de către autoritatea de supraveghere (de exemplu în urma unui audit eșuat grav) sau incapacitate financiară intempestivă (faliment), AlfaTrust va colabora cu autoritatea de supraveghere care va dispune măsurile necesare pentru protejarea utilizatorilor (posibil punerea sub administrare temporară a serviciilor, delegarea administrării către un alt prestator calificat de servicii de încredere etc.). Indiferent

de situație, prioritatea va fi menținerea posibilității de verificare a semnăturilor existente și informarea imediată a publicului despre schimbarea statutului prestatorului (ex.: eliminarea din Trusted List-ul UE în cazul retragerii statului de prestator calificat de servicii de încredere).

Concluzie: Deși AlfaTrust intenționează să își continue activitatea pe termen nedefinit și să ofere în mod sustenabil servicii de încredere, există un plan clar pentru cazul încetării, pentru a se asigura că utilizatorii nu rămân fără suport sau în incertitudine. Prin notificare prealabilă, revocare controlată a certificatelor și transferul evidențelor, AlfaTrust va gestiona **responsabil** orice oprire a serviciilor, conform obligațiilor legale și angajamentelor față de clienți.

12.REVIZUIRE ȘI ACTUALIZAREA DECLARAȚIEI PRACTICILOR APLICABILE SERVICIILOR DE ÎNCREDERE (DPSI)

Declarația practicilor aplicabile serviciilor de încredere (DPSI) este un document dinamic, care poate suferi actualizări pentru a reflecta schimbările de reglementare, de tehnologie sau de politici interne. AlfaTrust a stabilit un proces formal pentru managementul DPSI, care include revizuirea periodică, aprobarea modificărilor și publicarea noilor versiuni.

Versiunea și valabilitatea: Fiecare versiune a DPSI este identificată printr-un număr de versiune și o dată a intrării în vigoare. O versiune a DPSI rămâne aplicabilă și produce efecte până la momentul aprobării și publicării versiunii următoare. La emiterea unei noi versiuni, se specifică explicit dacă aceasta înlocuiește integral versiunea anterioară sau dacă sunt în vigoare concomitent anumite părți (în mod normal, noua versiune o înlocuiește pe cea veche în totalitate).

Inițierea modificărilor: Revizuirea DPSI poate fi inițiată ca urmare a: modificărilor legislative/reglementărilor (e.g., apariția unor noi standarde ETSI sau ghiduri ADR ce trebuie reflectate), a identificării unor erori sau neclarități în textul curent, a schimbărilor în infrastructura sau procedurile AlfaTrust, ori a feedback-ului primit de la părțile interesate (utilizatori, auditori, parteneri). Propunerile de modificare pot fi transmise de oricine are un interes în aceasta – de exemplu, personal intern, auditori, parteneri sau chiar utilizatori – fie direct către responsabilii desemnați, fie la adresa de email oficială a AlfaTrust. Orice propunere trebuie să descrie schimbarea dorită și motivarea acesteia.

Evaluarea și elaborarea noii versiuni: Echipa de management a securității și conformității din AlfaTrust va analiza periodic (de regulă anual sau mai des dacă e nevoie) necesitatea actualizării DPSI. În cazul în care se decide inițierea unei noi versiuni, un grup de lucru intern (care include reprezentanți ai departamentelor relevante: juridic, IT, securitate, operațiuni) va elabora draftul noii versiuni a DPSI. Se va acorda atenție asigurării continuității – adică noile prevederi să nu contravină angajamentelor luate față de utilizatori, decât dacă sunt impuse de lege (de exemplu, dacă o nouă reglementare cere condiții mai stricte, DPSI va fi modificată în consecință și utilizatorii vor fiificați).

Consultarea părților interesate: În funcție de natura modificărilor, AlfaTrust poate decide consultarea prealabilă a părților interesate înainte de finalizarea noii versiuni. Modificările substanțiale sau care ar putea afecta utilizatorii (de exemplu, schimbarea politicii de certificare, introducerea de noi limitări, schimbarea algoritmilor criptografici folosiți etc.) sunt de obicei supuse unei consultări publice sau cel puțin comunicate partenerilor și marilor clienți pentru feedback. În schimb, modificările minore sau urgente (cum ar fi corectarea unor erori tipografice, actualizarea unor date de contact, ajustări care nu afectează drepturile/obligațiile esențiale) pot fi adoptate fără consultare extinsă, pentru a nu întârzia implementarea lor.

Aprobarea internă: După ce proiectul noii versiuni este finalizat (ținând cont și de eventualele comentarii primite în faza de consultare), acesta este supus aprobării interne. Responsabilitatea aprobării finale revine conducerii AlfaTrust – de regulă, un comitet format din membrii ai conducerii superioare executive și managerii departamentelor cheie (IT, Securitate, Juridic, Operațiuni). Acest comitet analizează dacă noua versiune îndeplinește toate cerințele de conformitate și dacă modificările sunt corect justificate. Odată obținut acordul comitetului, versiunea este considerată finalizată.

Notificarea autorităților și publicarea: Înainte de a produce efecte, noua DPSI este transmisă către **organismul de supraveghere (ADR)**, în conformitate cu obligațiile prestatorului calificat de a-și informa autoritatea privind politicile sale (menționat și în Ordinul ADR 449/2017). De obicei, DPSI se transmite ADR pentru informare și eventuală evaluare. La scurt timp (maxim 10 zile) după trimiterea către autoritate, AlfaTrust procedează la **publicarea** noii versiuni pe site-ul web oficial. Noua versiune este marcată ca “*în vigoare*” împreună cu data de la care se aplică. Versiunea anterioară, dacă este cazul, este arhivată și disponibilă pentru referință (în special, poate fi necesară menținerea pe site a versiunilor vechi pentru consultare istorică, de exemplu de către instanțe sau terți care validează semnături din trecut și vor să știe practicile de la acel moment).

Gestionarea modificărilor: DPSI precizează la final un istoricul al versiunilor sau modificărilor semnificative. Modificările pot fi grupate în două categorii:

- Modificări **majore** – care afectează semnificativ politicile (de exemplu, introducerea unui nou serviciu de încredere în ofertă, schimbări în responsabilitățile părților, revizuirea majoră a politicilor de securitate). Acestea sunt în mod normal comunicate utilizatorilor în avans și pot necesita acceptarea explicită (de exemplu, dacă se modifică Termenii și Condițiile ca urmare a DPSI noi, utilizatorii existenți pot fi notificați și considerați de acord continuând să folosească serviciul).
- Modificări **minore** – care nu influențează substanțial drepturile și obligațiile (ex.: corecții editoriale, clarificări de text, actualizarea unor denumiri de standarde la versiuni noi fără impact practic). Acestea pot intra în vigoare imediat ce DPSI actualizat e publicat, fără o notificare specială către clienți, deși AlfaTrust poate alege să informeze într-un buletin de știri sau pe site despre existența noii versiuni.

Contribuția părților externe: Orice entitate sau utilizator care consideră că o anumită prevedere din DPSI trebuie îmbunătățită poate trimite sugestii către AlfaTrust (prin email la adresa oficială de contact). AlfaTrust se angajează să analizeze cu atenție asemenea sugestii, iar dacă ele sunt pertinente și fezabile, să le includă într-o versiune viitoare. Acest mecanism asigură transparență și colaborare în rafinarea practicilor, ținând cont de perspective diverse (de exemplu, un auditor extern ar putea sugera clarificarea unei secțiuni pentru a fi mai ușor de verificat conformitatea).

Disponibilitatea DPSI: Versiunea curentă a DPSI, precum și eventualele versiuni anterioare, sunt disponibile gratuit pe site-ul AlfaTrust, în format care permite tipărirea. DPSI este disponibilă în limba română (limba oficială), iar la nevoie AlfaTrust poate furniza și o traducere neoficială în limba engleză a acestui document, pentru a facilita înțelegerea de către parteneri străini (conform cerinței de cooperare transfrontalieră din Ordinul 449/2017). În caz de discrepanțe, versiunea în limba română rămâne versiunea oficială.

Încheiere: Prin acest proces de revizuire și actualizare a DPSI, AlfaTrust asigură că practicile declarate sunt întotdeauna aliniate realității și cerințelor legale. Orice schimbare este realizată într-un mod controlat,



evitând confuzii sau lipsă de comunicare. Utilizatorii și partenerii pot avea încredere că DPSI reflectă la zi modul în care AlfaTrust operează, iar AlfaTrust, la rândul său, se obligă să opereze conform celor declarate în DPSI. Documentul DPSI, împreună cu politicile și procedurile interne pe care le referă, este supus auditului de conformitate, asigurând astfel că nu este o simplă formalitate, ci o reprezentare reală a practicilor efective ale prestatorului.