PLAN DE ÎNCETARE A ACTIVITĂȚII

(Termination Plan)

în conformitate cu cerințele art. 12 alin. (2) lit. g) din Legea nr. 214/2024 și art. 5 alin. (2) lit. h) din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026

aplicabil exclusiv serviciilor de încredere necalificate prestate de QSIGN S.R.L. (semnături electronice avansate cu certificat)

Subscrisa QSIGN S.R.L., cu sediul social în București, str. Drumea Rădulescu, nr. 26, sector 4, înregistrată la Oficiul Registrului Comerțului sub nr. J2024010825402, având cod unic de înregistrare fiscală 34633481, reprezentată legal prin Trandafirescu Alexandru Florin, identificat prin C.I. seria RX, nr. 955913, CNP 1870821420049, în calitate de prestator de servicii de încredere, adoptă prezentul Plan de încetare a activității ca document de referință pentru asigurarea continuității operaționale și a protecției utilizatorilor în orice scenariu de încetare a activității de prestare a serviciilor de încredere.

1. Domeniul de aplicare

Prezentul Plan acoperă exclusiv serviciile de încredere necalificate prestate de QSIGN S.R.L., respectiv:

Servicii de încredere necalificate (înscrise în Registrul prestatorilor necalificați conform Anexei nr. 2 la Ordinul MEDAT nr. 102/2026):

emiterea de certificate pentru semnătura electronică avansată (X.509 v3, conform ETSI EN 319 412 și art. 26 din Reg. (UE) nr. 910/2014).

Planul se aplică tuturor componentelor infrastructurii de chei publice (PKI) operate de QSIGN — Root CA, Issuing CA, Time Stamping Authority (TSA), modul OCSP, repository CRL, modulul de înregistrare/identitate și modulele criptografice hardware (HSM), precum și tuturor utilizatorilor finali (subscriberi) și părților care se bazează pe servicii (relying parties).

2. Cadrul legal și de reglementare aplicabil

Planul respectă următoarele cerințe normative și standarde tehnice:

Regulamentul (UE) nr. 910/2014 (eIDAS) — art. 17 (rolul organismului de supraveghere), art. 19 (cerințe de securitate și notificarea incidentelor) — aplicabile tuturor prestatorilor de servicii de încredere, inclusiv celor necalificați; art. 26 (cerințe pentru semnătura electronică avansată).

Regulamentul (UE) 2024/1183 (eIDAS 2.0) — modificări aplicabile prestatorilor de servicii de încredere calificate, inclusiv obligațiile suplimentare privind portofelul european de identitate digitală (în măsura în care devin incidente activităților QSIGN).

Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea — în special art. 12 (obligațiile prestatorilor) și art. 19–21 (notificare/registru).

Legea nr. 58/2024 privind securitatea și apărarea cibernetică (transpunerea Directivei (UE) 2022/2555 — NIS2) — pentru obligația de cooperare cu DNSC și de notificare a incidentelor de securitate cibernetică.

Legea nr. 85/2014 privind procedurile de prevenire a insolvenței și de insolvență — pentru tratamentul prioritar al obligațiilor de încetare ordonată în relația cu administratorul judiciar/lichidatorul.

Ordinul MEDAT nr. 102/29.01.2026 — Anexa nr. 2 (servicii necalificate).

ETSI EN 319 401 V3.1.1 — General Policy Requirements for Trust Service Providers (clauza 7.12 — Termination of TSP and TSP service).

ETSI EN 319 411-1 V1.4.1 — Policy and security requirements for TSPs issuing certificates (clauza 6.4.9 — CA termination).

ETSI EN 319 411-2 V2.5.1 — cerințe pentru certificate calificate (semnătură/sigiliu).

ETSI EN 319 421 V1.2.1 — TSA Policy and Security Requirements (clauza 7.12 — TSA termination).

ETSI TS 119 461 V2.1.1 — Identity Proofing.

EN 419 221-5 — Protection profiles for TSP cryptographic modules — Cryptographic module for trust services (cerință pentru HSM-urile utilizate în prestarea serviciilor calificate, conform listei publicate la art. 31 din Reg. UE 910/2014).

Decizia de implementare (UE) 2016/650 — standarde pentru evaluarea de securitate a dispozitivelor calificate de creare a semnăturii și sigiliului electronic (QSCD).

ISO/IEC 27001:2022 — Sistemul de management al securității informației (controale A.5.30 ICT readiness for business continuity și A.5.29 Information security during disruption).

Regulamentul (UE) 2016/679 (GDPR) — pentru prelucrarea datelor cu caracter personal pe parcursul și după încetare.

Legea nr. 135/2007 privind arhivarea documentelor în formă electronică, republicată — pentru transferul arhivei.

3. Evenimente declanșatoare ale planului

Planul se activează la apariția oricăruia dintre următoarele evenimente, calificate în două categorii principale:

3.1. Încetare planificată (Planned Termination)

decizia voluntară a Adunării Generale / Administratorului unic de a înceta prestarea unuia, mai multor sau a tuturor serviciilor de încredere;

dizolvarea voluntară a societății sau încetarea obiectului de activitate prevăzut în actul constitutiv referitor la servicii de încredere;

expirarea ciclului de viață planificat al unei autorități de certificare (CA) sau al unei perechi de chei criptografice de top, fără reînnoire;

schimbarea modelului de afaceri (transferul activității către un prestator succesor printr-o operațiune de fuziune, divizare, cesiune sau achiziție).

3.2. Încetare neplanificată / forțată (Unplanned or Forced Termination)

radierea din Registrul prestatorilor necalificați conform Procedurii ADR;

intrarea în procedura de insolvență, faliment, lichidare judiciară sau orice altă procedură echivalentă care împiedică continuarea activității;

compromiterea ireversibilă a unei chei private de CA sau TSA și imposibilitatea recuperării în condiții de încredere;

incident major de securitate, dezastru sau forță majoră care face imposibilă reluarea operațiunilor în termenele prevăzute de Planul de continuitate (BCP/DRP);

decizia unei autorități judecătorești sau a unei autorități competente care impune încetarea.

4. Roluri și responsabilități

Pe durata procesului de încetare, responsabilitățile sunt distribuite după cum urmează:

Administratorul (Trandafirescu Alexandru Florin) — autoritatea decizională exclusivă privind activarea Planului, alegerea succesorului, calendarul efectiv și alocarea resurselor; semnarea notificărilor către ADR, DNSC, ANSPDCP și subscribers; reprezentarea QSIGN în relațiile cu autoritățile, lichidatorul (dacă este cazul) și succesorul.

Responsabilul cu securitatea (CISO / TSP Security Officer) — execută operațional revocarea certificatelor, distrugerea controlată a cheilor private de CA și TSA și predarea evidențelor, conform deciziilor și calendarului stabilit de Administrator. Decizia operațională asupra ceremoniilor, ordinii de revocare și nivelului de detaliu al jurnalelor predate aparține CISO, în limita prevederilor legale aplicabile.

Responsabilul cu protecția datelor (DPO) — asigură conformitatea GDPR pe parcursul transferului sau distrugerii datelor cu caracter personal; se pronunță asupra cererilor de exercitare a drepturilor titularilor în limitele permise de legislația specială (păstrarea obligatorie a evidențelor în interes public conform art. 17 alin. (3) lit. b) GDPR și art. 12 din Legea 214/2024).

Responsabilul de arhivă electronică — coordonează predarea evidențelor către administratorul de arhivă electronică acreditat în baza contractului-cadru încheiat de QSIGN; selecția administratorului de arhivă și conținutul efectiv al fondului transferat se stabilesc la discreția QSIGN, cu respectarea cerințelor minime din Legea nr. 135/2007.

Auditor extern (înscris în Lista auditorilor de securitate cibernetică LASC, valabil atestat de DNSC, pentru servicii de încredere necalificate) — participă la auditul final de încetare și la verificarea distrugerii cheilor.

5. Faza de pregătire continuă (în timpul activității)

Pentru a asigura aplicabilitatea efectivă a planului în orice moment, QSIGN menține în permanență:

un acord-cadru de transfer încheiat cu cel puțin un prestator succesor (calificat și/sau necalificat, după caz), revizuit cel puțin anual; selecția succesorului și a oricărei părți alternative aparține în mod exclusiv QSIGN și nu poate fi contestată de subscribers, relying parties sau alte terțe părți;

contractul cu administratorul de arhivă electronică acreditat, prin care se asigură preluarea, conservarea și accesul la dovezile relevante pe perioada legală;

rezerve financiare alocate fazei de încetare (asigurare de răspundere civilă profesională, scrisoare de garanție bancară sau cont blocat/escrow), în cuantumurile MINIME prevăzute de reglementările aplicabile: minim 100.000 EUR per eveniment, conform art. 5 alin. (2) lit. b) din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026. Fondurile se utilizează în ordinea de prioritate stabilită la Secțiunea 13;

un registru actualizat în timp real al subscriberilor activi, certificatelor emise, cheilor private de CA/TSA, modulelor HSM, jurnalelor de audit și serializărilor CRL/OCSP, cu replicare off-site și revizie de integritate cel puțin lunară;

declarația publică privind politicile (CP / CPS / TSP) care include prezentul Plan ca anexă publică, comunicată subscriberilor prin Termenii și Condițiile semnate;

scrisoare de garanție bancară sau poliță de asigurare de răspundere civilă profesională cesionată în favoarea ADR, în cuantumul minim prevăzut de art. 5 alin. (2) lit. b) din Anexa nr. 2 (necalificat) la Ordinul MEDAT nr. 102/2026; QSIGN nu este obligată să mențină garanții peste minimele legale.

6. Procedura de încetare planificată

Termenele de mai jos sunt orientative pentru serviciile necalificate prestate de QSIGN, conforme cu cerința art. 12 alin. (2) lit. g) din Legea nr. 214/2024 și cu standardele europene ETSI EN 319 401 §7.12. În absența unei prevederi legale exprese contrare în Anexa nr. 2 la Ordinul MEDAT 102/2026, QSIGN își rezervă dreptul de a aplica termene mai scurte (minim D-30 zile pentru notificare ADR, D-15 zile pentru subscribers individual, D-7 zile pentru oprirea emiterii) cu respectarea cerinței minime de informare oportună prevăzute de standardele tehnice. D = data efectivă a încetării, exprimată în zile calendaristice.

6.1. D-90 zile — Decizia formală și notificarea ADR

hotărârea Administratorului / Adunării Generale de încetare a serviciului;

notificarea Autorității pentru Digitalizarea României (ADR) în formă scrisă și prin semnătură electronică calificată, cu indicarea: serviciilor afectate, datei efective, succesorului propus (dacă există), modului de gestionare a certificatelor active, modalității de păstrare a dovezilor;

notificarea Direcției Naționale de Securitate Cibernetică (DNSC) conform obligațiilor de cooperare aplicabile;

notificarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) dacă încetarea implică transfer/distrugere de date personale ce necesită evaluare DPIA suplimentară.

6.2. D-60 zile — Notificarea utilizatorilor

notificare individuală a fiecărui subscriber, prin e-mail la adresa din certificate și scrisoare recomandată, cu confirmare de primire pentru subscriberii instituționali;

publicarea unui anunț pe pagina www.qsign.ro, în secțiunea Repository și pe pagina principală — forma, conținutul, gradul de detaliu și perioada de afișare se stabilesc la discreția QSIGN, cu respectarea cerinței minime de informare reală și non-înșelătoare a publicului;

publicarea unui anunț pe pagina www.qsign.ro, în secțiunea Repository, conform cerințelor art. 12 alin. (2) lit. g) Legea nr. 214/2024;

comunicarea conține: serviciile afectate, data efectivă, succesorul (dacă este desemnat), instrucțiunile pentru migrare, drepturile subscriberului și calea de contact pentru sprijin.

6.3. D-30 zile — Oprirea emiterii și transfer

oprirea emiterii de certificate noi pentru semnătura electronică avansată; cererile primite după această dată sunt respinse în mod uniform;

realizarea transferului efectiv către succesor (dacă există): export de jurnale, transfer de evidențe ale subscriberilor, predarea instalațiilor și a dovezilor de identificare conform ETSI TS 119 461;

emiterea CRL-urilor finale și planificarea programului de OCSP după încetare;

audit final efectuat de un auditor LASC tip General, înscris în Lista auditorilor de securitate cibernetică valabil atestați de DNSC, conform art. 8 alin. (3) lit. f) din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026; selecția și instructajul auditorului aparțin QSIGN, în condițiile în care raportul auditorului este transmis ADR conform obligațiilor legale.

6.4. Data D — Încetarea efectivă

revocarea în masă a tuturor certificatelor neexpirate emise pe lanțul afectat (motiv: cessationOfOperation, OID 1.3.6.1.5.5.7.1.1 — RFC 5280, reasonCode = 5);

emiterea ultimului CRL semnat de CA, cu nextUpdate fixat conform politicilor de continuitate (minim până la expirarea ultimului certificat valid);

oprirea emiterii de mărci temporale și emiterea unei declarații finale a TSA;

transferul controlului către succesor sau către modulul de menținere a CRL/OCSP operat post-încetare;

notificarea ADR cu privire la încheierea operațiunilor și transmiterea raportului final.

6.5. D+1 până la expirarea ultimului certificat — Operare reziduală

menținerea repository-ului public (CRL/OCSP, lista certificatelor revocate, declarațiile publicate) pe site-ul oficial sau pe site-ul succesorului, în mod gratuit;

menținerea unui canal de contact (e-mail support@qsign.ro și/sau succesor) pentru subscriberi și relying parties;

conservarea jurnalelor de audit și a dovezilor conform Secțiunii 11.

7. Procedura de încetare neplanificată / forțată

În scenariile prevăzute la Secțiunea 3.2, termenele se comprimă la nivelul minim legal aplicabil, iar Planul se aplică sub coordonarea exclusivă a Administratorului și a CISO. QSIGN nu are obligația de a prelungi termenele cu acordul subscribers sau al relying parties; deciziile operaționale necesare pentru limitarea daunelor (revocare, distrugerea cheilor compromise, oprirea OCSP, izolarea sistemelor afectate) sunt executive.

7.1. Compromitere de chei (key compromise)

declanșare imediată în mai puțin de 4 ore de la confirmarea compromiterii;

revocarea tuturor certificatelor emise pe lanțul afectat (motiv: keyCompromise — reasonCode 1 conform RFC 5280; pentru CA: cACompromise — reasonCode 2);

publicarea unui CRL extraordinar și actualizarea răspunsurilor OCSP — obiectiv operațional intern de maxim 60 minute de la decizia de revocare; obligație legală de cel mult 24 ore conform art. 17 alin. (2) din Legea nr. 214/2024;

notificarea ADR în maxim 24 ore conform art. 19 alin. (2) din Reg. (UE) nr. 910/2014;

notificarea DNSC în paralel pentru incidentele cu impact semnificativ asupra securității rețelelor și sistemelor informatice (Legea nr. 58/2024);

notificarea subscriberilor și a publicului prin canalele uzuale și canale de urgență;

declanșarea analizei de impact și a procedurii de tratare a incidentelor de securitate.

7.2. Insolvență / faliment / lichidare

activarea acordului-cadru cu prestatorul succesor și a contractului de arhivare;

transferul prioritar al evidențelor către administratorul de arhivă electronică acreditat;

cooperarea cu lichidatorul / administratorul judiciar pentru execuția planului — operațiunile de încetare ordonată au prioritate față de orice altă creanță în temeiul art. 12 alin. (3) din Legea 214/2024 și al regimului special al fondurilor cesionate ADR; subscribers și relying parties nu au statut de creditori privilegiați față de cheltuielile esențiale ale fazei de încetare;

utilizarea fondurilor de garanție/asigurare cesionate ADR pentru acoperirea costurilor minimale de încetare ordonată.

7.3. Radierea din Registrul prestatorilor necalificați

oprirea imediată a emiterii la data primirii deciziei ADR;

aplicarea procedurii planificate (Secțiunea 6) de la pasul D-30, cu termenele recalculate;

publicarea deciziei pe site-ul propriu și anunțarea utilizatorilor în maxim 7 zile.

8. Notificarea părților interesate

Notificările sunt structurate pe canale și destinatari, cu termene minime aplicabile fiecărui regim de servicii. Comunicările sunt considerate primite la data confirmării livrării (de exemplu

confirmarea SMTP de livrare către serverul destinatarului, confirmarea de primire prin operatorul poștal sau confirmarea de citire) sau, în absența unei erori de livrare comunicate către QSIGN în termen de 48 de ore de la trimitere, la expirarea acestui termen de 48 de ore (în acord cu art. 1326–1330 C.civ. privind ajungerea ofertei/comunicării în sfera destinatarului). Notificările respinse din motive imputabile destinatarului (adresă invalidă, mailbox plin, refuz expres, lipsa colectării corespondenței) sunt considerate efectuate la data primei trimiteri, fără ca QSIGN să fie obligată să le retransmită.

ADR — notificare scrisă semnată electronic calificat, transmisă la adresa oficială înregistrată; ≥ 30 zile înainte (planificat) sau în maxim 24 ore de la incidentul declanșator (forțat), conform art. 12 alin. (2) lit. g) din Legea nr. 214/2024;

DNSC — notificare în paralel cu ADR pentru servicii care fac obiectul cooperării de securitate cibernetică.

ANSPDCP — notificare în maxim 72 ore pentru orice incident sau transfer ce ar avea impact asupra protecției datelor.

Subscribers (utilizatori finali) — notificare individuală prin e-mail (semnat electronic) la adresa de contact declarată în certificat sau în dosarul de înrolare, însoțită de publicare pe site; transmiterea pe e-mail este suficientă conform art. 12 alin. (1) lit. d) Legea nr. 214/2024 — scrisoarea recomandată este opțională, la discreția QSIGN; minim 15 zile pentru subscribers;

Relying parties — notificare publică pe www.qsign.ro și actualizarea Registrului electronic al prestatorilor necalificați gestionat de ADR.

Public larg — anunț pe site-ul oficial www.qsign.ro.

Browser/OS root programs (dacă este cazul) — notificare prin canalele oficiale Mozilla, Microsoft, Apple, Google, Adobe pentru rădăcini incluse în magazinele de încredere.

9. Transferul activității către un prestator succesor

QSIGN va depune eforturi rezonabile pentru a desemna și transfera activitatea către un prestator de servicii de încredere succesor (calificat sau necalificat) înscris în Registrul ADR. Identificarea succesorului, negocierea condițiilor și momentul transferului efectiv aparțin discreției exclusive a QSIGN; subscribers și relying parties NU au drept de veto, drept de consultare prealabilă sau drept de a pretinde compensații pentru schimbarea succesorului. Transferul cuprinde STRICT următoarele evidențe — minimul cerut de standardele tehnice și de lege:

predarea evidenței complete a subscriberilor activi (date de identificare, contracte, dovezi de identity proofing — minim Baseline LoIP conform ETSI TS 119 461);

predarea evidenței certificatelor emise (active, expirate, revocate), inclusiv numerele de serie și fingerprint-urile;

predarea jurnalelor de audit (audit logs) ale CA, RA, TSA, OCSP responder, conform ETSI EN 319 411-1 clauza 6.4.5;

predarea politicilor de certificare (CP), declarațiilor de practici (CPS), politicilor TSA în versiunile aplicabile la momentul încetării;

predarea CRL-urilor istorice și a configurațiilor OCSP (pentru continuarea răspunsurilor post-termination);

predarea cheilor publice ale CA și a lanțurilor de încredere — cu lista certificatelor rădăcină incluse în Trusted Lists naționale și în programele de root browser;

notificarea comună ADR–QSIGN–succesor cu privire la statutul transferului.

În cazul în care succesorul nu poate fi identificat în termen rezonabil, predarea evidențelor și obligația de menținere a CRL/OCSP se efectuează către administratorul de arhivă electronică acreditat și/sau, după caz, către ADR, conform contractelor în vigoare. Subscribers afectați de imposibilitatea identificării unui succesor nu au drept la rambursarea integrală a tarifelor, ci doar la o rambursare PRO-RATA temporis a perioadei neprestate, condiționată de existența disponibilului în fondurile de încetare după acoperirea costurilor operaționale (Secțiunea 13).

10. Revocarea certificatelor

Procedura de revocare este structurată conform RFC 5280, ETSI EN 319 411-1 și politicii de certificare aplicabile, după cum urmează:

Determinarea perimetrului — identificarea tuturor certificatelor neexpirate care urmează a fi revocate, grupate pe lanțuri de încredere și politici de certificat (OID-uri de politici).

Motivul revocării — conform RFC 5280, codurile sunt valori INTEGER incluse în extensia CRLReason: cessationOfOperation (5) pentru încetare planificată, keyCompromise (1) sau cACompromise (2) pentru compromitere, privilegeWithdrawn (9) pentru retragerea statutului, superseded (4) pentru migrare către lanț succesor.

Prezervarea validării pe termen lung — pentru semnăturile, sigiliile și mărcile temporale aplicate înainte de revocare, validitatea juridică se menține prin long-term validation (LTV/LTA) — profilurile B-LT și B-LTA conforme ETSI EN 319 122 (CAdES), ETSI EN 319 132 (XAdES), ETSI EN 319 142 (PAdES) și ETSI EN 319 102-1 (procedurile de validare); marcaje temporale calificate (RFC 3161 + ETSI EN 319 421) emise anterior revocării rămân probatorii.

Publicarea — CRL emis cu thisUpdate la momentul revocării, semnat de CA-ul emitent; OCSP responder configurat pentru a răspunde revoked cu motivul corespunzător; semnături OCSP păstrate până la expirarea ultimului certificat.

Continuitate post-termination — CRL și OCSP continuă să fie disponibile (operate de QSIGN, succesor sau ADR) cel puțin până la expirarea ultimului certificat emis pe lanțul respectiv, în temeiul art. 12 alin. (2) lit. d) și (g) din Legea nr. 214/2024 și al cerințelor ETSI EN 319 411-1 clauza 6.4.9 (CA termination).

11. Conservarea evidențelor și transferul arhivei

Toate informațiile relevante pentru funcționarea ulterioară a verificării semnăturilor și pentru investigațiile legale sunt conservate astfel:

Durata — 10 ani de la expirarea/revocarea ultimului certificat emis, conform art. 12 alin. (2) lit. f) din Legea nr. 214/2024 și ETSI EN 319 411-1 §6.4. La expirarea termenului, evidențele sunt distruse irevocabil dacă nu există o cerere legală de prelungire (decizie ADR, ordin instanță, anchetă DNSC); QSIGN nu este obligată să mențină evidențele peste această durată din proprie inițiativă.

Categorii de evidențe — (i) cereri și dovezi de identity proofing; (ii) contracte cu subscriberii și termeni acceptați; (iii) jurnale de audit ale CA/TSA/RA/OCSP; (iv) configurații și politici versionate; (v) CRL-uri istorice; (vi) rapoarte de audit; (vii) corespondența cu organismele de supraveghere; (viii) registrul operațiunilor criptografice executate de HSM-uri.

Modul de păstrare — preluare integrală de către administratorul de arhivă electronică acreditat conform Legii nr. 135/2007 (contract activ — pct. 20 din OPIS-ul cererilor depuse la ADR), cu integritate asigurată prin sigilare electronică și marcare temporală calificată.

Confidențialitate — respectarea GDPR; ștergerea datelor cu caracter personal după expirarea termenelor legale; access logs controlat strict.

Acces ulterior — autoritățile competente (ADR, ANSPDCP, instanțe judecătorești, organe de urmărire penală) pot solicita extrase pe baza unei cereri scrise întemeiate legal. Subscribers pot solicita extrase ce îi privesc, contra cost (taxă administrativă publicată în Lista de tarife). Răspunsul se transmite în termen de 30 de zile lucrătoare. Cererile excesive, repetitive sau vădit nefondate pot fi respinse sau tarifate suplimentar conform art. 12 alin. (5) GDPR.

12. Distrugerea cheilor private

După încetarea activității și emiterea ultimului CRL semnat, cheile private de CA și TSA care nu sunt necesare pentru semnarea CRL-urilor reziduale se distrug în mod controlat, cu respectarea următoarelor reguli:

distrugerea se realizează în interiorul HSM-urilor (zeroize) cu suportul mecanismelor criptografice native ale modulului — HSM minim FIPS 140-2/3 Nivel 3 sau Common Criteria EAL 4+, conform cerințelor art. 5 alin. (2) lit. e) din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026;

ceremonia de distrugere este înregistrată video, supervizată de Administrator și Responsabilul cu securitatea, cu participarea auditorului extern;

se întocmește un proces-verbal de distrugere care include: identificatorii cheilor, numerele de serie HSM, data și ora, semnăturile participanților; distrugerea este IREVOCABILĂ — orice cerere ulterioară de re-emitere a unui certificat semnat cu cheile distruse, sau de regenerare a CRL-urilor istorice, nu poate fi onorată tehnic și nu naște răspunderea QSIGN, indiferent de natura interesului invocat;

procesul-verbal este transmis ADR și inclus în arhiva de încheiere;

cheile de semnare CRL post-termination, dacă sunt necesare, sunt conservate în HSM până la data expirării ultimului certificat și apoi distruse după aceeași procedură;

cheile private ale subscriberilor finali rămân în controlul exclusiv al acestora — QSIGN nu are obligația și nici posibilitatea de a le distruge, întrucât pentru semnătura electronică avansată

cheile sunt generate și protejate de utilizator (definiția art. 26 din Reg. UE 910/2014); subscriberii sunt informați să distrugă/șteargă cheile pe canalul propriu.

13. Resurse financiare alocate încetării

Pentru garantarea aplicabilității efective a Planului în orice scenariu, inclusiv în caz de insolvență, QSIGN menține resurse financiare alocate, utilizate strict în următoarea ordine de prioritate, la decizia exclusivă a Administratorului (sau a lichidatorului, dacă este numit, dar cu respectarea Planului):

(i) costurile operaționale ale încetării ordonate — notificări, audit final, retenție personal-cheie pe perioada minimă necesară (3-6 luni), operare CRL/OCSP rezidual, predare evidențe către administratorul de arhivă;

(ii) plățile către succesor desemnat (cu titlu de migrare) și obligațiile minime contractuale față de furnizorii critici (HSM, conectivitate, găzduire, asigurări);

(iii) eventuale rambursări pro-rata temporis către subscribers, în limita disponibilului rămas după acoperirea cheltuielilor de la (i) și (ii); subscribers nu au statut de creditori privilegiați pentru aceste rambursări și nu au drept la dobânzi de întârziere; rambursările se calculează exclusiv pentru perioada neprestată efectiv, în baza tarifului plătit la emitere, fără actualizări pentru inflație;

14. Plan de comunicare publică

Pe lângă notificările formale prevăzute la Secțiunea 8, QSIGN întreține un plan de comunicare publică pe parcursul încetării; conținutul, frecvența și forma sunt la discreția QSIGN, cu respectarea cerinței de informare reală și non-înșelătoare:

pagină dedicată pe www.qsign.ro cu cronologie, calendar, FAQ pentru subscriberi și relying parties — actualizată la fiecare etapă a planului;

instrucțiuni clare de migrare către prestatorul succesor (dacă este desemnat) cu detalii tehnice, identificatori OID, lanț de încredere nou;

ghid de validare retroactivă a semnăturilor existente după încetare (long-term validation), cu trimitere la procedurile ETSI EN 319 102-1;

punct unic de contact: e-mail termination@qsign.ro, operațional pe toată durata fazei active. QSIGN nu este obligată să mențină acest canal după expirarea ultimului certificat sau după transferul integral către succesor; în această fază, reclamațiile și solicitările se adresează succesorului sau ADR.

15. Testarea, revizia și aprobarea planului

Planul este revizuit anual sau la apariția unei modificări semnificative (adăugare sau retragere de servicii, schimbarea succesorului-cadru, modificări de reglementare, lecții învățate dintr-o simulare sau dintr-un incident). Modificările intră în vigoare la data aprobării de către

Administrator și a publicării unui extras în repository-ul public; subscribers și relying parties recunosc dreptul QSIGN de a actualiza Planul fără consimțământul lor, în condițiile transparenței.

Cel puțin o dată pe an se efectuează o simulare (tabletop exercise) a unui scenariu de încetare — planificată și forțată — cu participarea conducerii și a echipei tehnice.

Rezultatele simulării sunt consemnate într-un raport intern și utilizate pentru îmbunătățirea planului.

Versiunea curentă a planului este aprobată de Administrator și păstrată în repository-ul intern de documente, cu istoric al versiunilor.

Un extras public al planului este disponibil pe www.qsign.ro/repository, conform principiului transparenței față de subscriberi și relying parties (ETSI EN 319 401, clauza 6.1).

16. Limitarea răspunderii și exonerări

Răspunderea QSIGN în cadrul executării Planului și în legătură cu evenimentul de încetare este limitată conform următoarelor reguli:

16.1 Pentru servicii necalificate, NU se aplică prezumția de eroare imputabilă din art. 13 alin. (1) eIDAS. Răspunderea QSIGN se stabilește conform regulilor generale de drept civil român (Codul civil), în baza probei daunei și a culpei dovedite de partea reclamantă; răspunderea este limitată la valoarea poliței de asigurare (minim 100.000 EUR per eveniment) și la reliance limits din PDS-AC.

16.2 În toate situațiile, QSIGN NU răspunde pentru:

- daunele indirecte, pierderea de profit, pierderea de oportunități comerciale, pierderea de reputație sau alte daune consecutive, indiferent de previzibilitatea acestora;
- daunele rezultate din utilizarea unui certificat în condiții ce încalcă acordurile aplicabile (Subscriber Agreement, Relying Party Agreement, PDS, CP/CPS), în special: utilizare după expirare/revocare, utilizare peste keyUsage/extKeyUsage, utilizare peste reliance limits;
- daunele rezultate din erori, omisiuni sau falsuri în datele furnizate de subscribers la cerere — sub rezerva că QSIGN a aplicat procedurile de identity proofing prevăzute la nivelul LoIP corespunzător politicii;
- daunele cauzate de un eveniment de forță majoră (Secțiunea 18);
- daunele rezultate din ne-cooperarea subscribers/relying parties cu obligațiile lor stabilite la Secțiunea 17 — în special, ignorarea notificărilor de încetare publicate prin canalele uzuale;
- daunele rezultate din imposibilitatea tehnică de a emite o nouă marcă temporală sau un nou certificat după distrugerea cheilor de CA/TSA (Secțiunea 12) — distrugerea cheilor este irevocabilă și obligatorie.

16.3 QSIGN își rezervă dreptul de regres împotriva oricărei persoane care a contribuit la cauzarea daunei (subscriber neglijent, atacator extern, furnizor de servicii defectuos), inclusiv pentru recuperarea sumelor plătite cu titlu de despăgubire.

17. Obligațiile subscribers și relying parties pe parcursul încetării

Prin acceptarea Subscriber Agreement / Relying Party Agreement, fiecare subscriber și relying party recunoaște și acceptă următoarele obligații, aplicabile pe parcursul fazei de încetare:

17.1 Cooperare în maxim 30 zile calendaristice de la data primirii notificării — pentru migrare la succesor, eliberarea dispozitivelor de creare a semnăturii (token, smart card) către succesor sau distrugerea acestora conform instrucțiunilor QSIGN, predarea evidențelor proprii cerute pentru transfer.

17.2 Recunoașterea revocării prin cessationOfOperation (RFC 5280, reasonCode 5) ca eveniment legitim de încetare, FĂRĂ ca aceasta să nască drept la compensație suplimentară peste rambursarea pro-rata temporis prevăzută la Secțiunea 13 punctul (iii).

17.3 Suportarea costurilor proprii de migrare (configurări tehnice, modificări procedurale, eventuala emitere a unui nou certificat la succesor); aceste costuri NU pot fi reclamate de la QSIGN.

17.4 Continuarea respectării obligațiilor de confidențialitate asupra informațiilor primite în executarea acordurilor (datele de identificare, datele tehnice ale infrastructurii QSIGN, conținutul documentelor interne primite, etc.) pentru o perioadă de 5 ani după data încetării; obligația supraviețuiește încetării.

17.5 Renunțarea la dreptul de a iniția acțiuni colective (class action) împotriva QSIGN în legătură cu evenimentul de încetare, în limita permisă de dreptul român aplicabil; subscribers și relying parties pot exercita drepturile lor numai individual.

17.6 Acceptarea că publicarea notificării pe canalele uzuale (e-mail la adresa declarată, anunț pe www.qsign.ro/repository) constituie comunicare validă; lipsa monitorizării acestor canale nu se opune valabilității notificării.

17.7 Validarea retroactivă a semnăturilor și sigiliilor aplicate înainte de revocare/încetare se efectuează pe baza CRL-urilor istorice și OCSP-ului post-termination publicate de QSIGN, succesor sau administratorul de arhivă; subscribers și relying parties au obligația de a aplica tehnicile de long-term validation prevăzute de ETSI EN 319 102-1 (LTV).

18. Forța majoră

Niciuna dintre părți nu este răspunzătoare pentru neexecutarea totală sau parțială a obligațiilor sale dacă neexecutarea este cauzată de un eveniment de forță majoră, definit în sensul cel mai larg permis de art. 1351 Cod civil și de practica judiciară internațională, incluzând:

- calamități naturale (cutremure, inundații, incendii devastatoare, condiții meteorologice extreme);
- războaie, conflicte armate, acte de terorism, revolte, insurecții;
- pandemii sau epidemii cu restricții oficiale care afectează capacitatea de operare;
- atacuri cibernetice masive de natură statală sau organizată (Advanced Persistent Threats sponsorizate, atacuri pe lanțul de aprovizionare criptografică, vulnerabilități zero-day exploatate la scară), inclusiv compromiteri de algoritmi criptografici sau de surse de entropie neanticipate de standardele tehnice în vigoare;
- schimbări legislative sau de reglementare bruște care fac imposibilă sau ilegală continuarea serviciului în condițiile acceptate;
- retragerea autorizării de către autoritatea competentă (ADR, DNSC, alte autorități) fără culpa demonstrată a QSIGN, inclusiv ca urmare a unei interpretări nou apărute a legii;
- întreruperi prelungite ale serviciilor furnizorilor critici (HSM, conectivitate, găzduire, distribuție de software), atunci când nu există alternative comerciale rezonabile;
- hotărâri judecătorești sau ordine administrative care impun încetarea sau modificarea esențială a serviciului.

Partea afectată de forță majoră notifică cealaltă parte (sau publicul, în cazul QSIGN) în maxim 7 zile de la luarea la cunoștință și depune eforturi rezonabile de a relua executarea sau de a tranziționa ordonat. Pe durata forței majore, obligațiile contractuale sunt suspendate; dacă forța majoră durează mai mult de 90 zile, oricare parte poate solicita încetarea acordurilor fără despăgubiri.

19. Drepturi de proprietate intelectuală

QSIGN își rezervă, pe parcursul Planului și după încetare, toate drepturile de proprietate intelectuală asupra: software-ului propriu (inclusiv configurațiile PKI personalizate, scripturile de operare, instrumentele de RA/CA/TSA, integrările cu surse de date publice), procedurilor interne, jurnalelor interne (cu excepția extraselor cerute de lege), modelelor de risc, brand-ului, mărcilor, logo-urilor și siglelor.

Transferul către succesor cuprinde STRICT documentele și evidențele cerute de lege și de standardele tehnice (cereri și dovezi de identity proofing, contracte cu subscribers, jurnale de audit, CRL-uri istorice, configurații OCSP, lanțuri de încredere); transferul NU include o licență asupra software-ului propriu QSIGN sau asupra documentației interne, decât dacă QSIGN agreează contractual o asemenea licențiere.

Marca, logo-ul și denumirea „QSIGN” și derivatele acestora rămân proprietatea exclusivă a QSIGN S.R.L. și nu pot fi utilizate de succesor, subscribers sau terțe părți după încetare, fără consimțământul scris al QSIGN.

20. Diverse — divizibilitate, lipsă drepturi terți, legea aplicabilă, jurisdicție

20.1 Divizibilitate. Dacă o clauză a Planului este declarată nulă sau inaplicabilă de către o instanță sau autoritate competentă, celelalte clauze rămân în vigoare în măsura permisă de economia documentului; părțile vor înlocui clauza afectată cu o prevedere validă, cât mai apropiată de intenția inițială.

20.2 Lipsă drepturi pentru terțe părți. Planul nu conferă drepturi sau cauze de acțiune pentru persoane care nu sunt parte la acordurile relevante (Subscriber Agreement, Relying Party Agreement) cu QSIGN — cu excepția drepturilor expres recunoscute de lege (autoritățile de supraveghere, persoanele vizate prin GDPR în limitele art. 12-22 GDPR, succesorul desemnat în limitele acordului-cadru).

20.3 Renunțarea. Neexercitarea sau exercitarea cu întârziere de către QSIGN a unui drept sau remediu nu constituie renunțare la acel drept sau remediu pentru viitor.

20.4 Cesiunea. QSIGN are dreptul să cesioneze drepturile și obligațiile sale rezultate din Plan către un succesor desemnat, fără consimțământul subscribers și al relying parties, în limita reglementărilor aplicabile. Subscribers nu pot cesiona drepturile lor fără acordul scris al QSIGN.

20.5 Comunicările formale. Notificările între QSIGN și autorități/succesor se transmit la adresele oficiale înregistrate, prin e-mail semnat electronic calificat sau scrisoare cu confirmare de primire. Comunicările cu subscribers se efectuează la adresa declarată în certificat sau în dosarul de înrolare.

20.6 Legea aplicabilă. Planul este guvernat de legea română, completată cu dreptul Uniunii Europene direct aplicabil (Reg. (UE) 910/2014, Reg. (UE) 2024/1183, Reg. (UE) 2016/679 — GDPR).

20.7 Jurisdicția. Litigiile rezultate din executarea sau interpretarea Planului — care nu sunt soluționate amiabil în 30 zile de la notificare — sunt de competența exclusivă a instanțelor judecătorești de la sediul QSIGN (București), cu respectarea regulilor speciale de competență imperativă (consumator, autoritate publică, GDPR).

20.8 Limba autentică. Versiunea în limba română este autentică; orice traducere are caracter informativ.

21. Aprobarea și intrarea în vigoare

Prezentul Plan de încetare a activității constituie document obligatoriu pentru întreaga structură organizațională a QSIGN S.R.L., devine parte integrantă a documentației depuse la ADR (art. 5 alin. (2) lit. r) din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026), și intră în vigoare la data semnării de către Administrator.

Anexa A — Calendar sintetic al încetării planificate

Tabelul de mai jos sintetizează etapele și termenele cheie. D = data efectivă a încetării serviciului. Toate termenele sunt zile calendaristice, dacă nu se specifică altfel.

A.1. Etape cheie

D-90 zile — decizia formală a Administratorului; notificare scrisă semnată calificat către ADR, DNSC și (după caz) ANSPDCP; activarea acordului-cadru cu succesorul desemnat.

D-60 zile — notificare individuală a subscriberilor (e-mail + recomandată); publicare anunț pe www.qsign.ro și în secțiunea Repository; (pentru calificat) publicare în Monitorul Oficial Partea a IV-a.

D-30 zile — oprirea emiterii certificatelor noi; transfer efectiv al evidențelor către succesor; audit final extern (organism de evaluare a conformității pentru calificat / auditor LASC pentru necalificat).

D — revocare în masă a certificatelor neexpirate (cessationOfOperation = 5); CRL final semnat; oprirea TSA; transfer control către succesor; raport final către ADR.

D+1 până la expirarea ultimului certificat — operare reziduală a CRL/OCSP (gratuit, pe canale publice); canal de contact deschis; conservare jurnale de audit.

D + 10 ani de la expirarea ultimului certificat — expirarea termenului minim de conservare a evidențelor în arhiva electronică acreditată (Legea nr. 135/2007); ștergere controlată a datelor cu caracter personal sub coordonarea DPO.

A.2. Termene scurte pentru încetare neplanificată

≤ 4 ore de la confirmarea unei compromiteri de chei — declanșarea procedurii de revocare.

≤ 60 minute (obiectiv intern) de la decizia de revocare — publicare CRL extraordinar și actualizare OCSP.

≤ 24 ore (obligație legală art. 17 alin. (2) Legea nr. 214/2024) — publicare oficială a statusului de revocare.

≤ 24 ore (obligație legală art. 19 alin. (2) eIDAS) — notificare ADR despre orice incident cu impact semnificativ asupra serviciului de încredere.

≤ 72 ore (obligație legală art. 33 GDPR) — notificare ANSPDCP, dacă incidentul implică încălcarea securității datelor cu caracter personal.

Anexa B — Matricea contactelor instituționale

Lista canalelor oficiale de comunicare utilizate la activarea Planului. Datele de contact ale succesorului desemnat sunt menținute într-o anexă confidențială separată și actualizate cel puțin anual.

Autoritatea pentru Digitalizarea României (ADR) — organism de supraveghere conform art. 17 din Reg. (UE) nr. 910/2014; CUI 42283735; contact@adr.gov.ro; site oficial www.adr.gov.ro.

Direcția Națională de Securitate Cibernetică (DNSC) — autoritate competentă conform Legii nr. 58/2024; alerts@dnsc.ro / contact@dnsc.ro; CSIRT național.

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) — autoritate competentă conform GDPR (art. 33–34); anspdcp@dataprotection.ro; site oficial www.dataprotection.ro.

Punct unic de contact intern QSIGN — e-mail: termination@qsign.ro (operațional pe toată durata fazei active); telefon: 0724.167.333; reprezentant legal: Trandafirescu Alexandru Florin.

Administrator de arhivă electronică acreditat — conform contractului în vigoare (referință OPIS pct. 20 din cererile depuse la ADR), datele de contact se mențin actualizate în anexa contractuală; transferul efectiv se realizează la activarea Planului.

Auditor extern — organism de evaluare a conformității acreditat (pentru servicii calificate) sau auditor înscris în Lista auditorilor de securitate cibernetică LASC a DNSC, deținător al atestatului de tip General (pentru serviciul necalificat); selectat la momentul activării Planului din lista de auditori cu acord-cadru.

Programe root browser/OS — Mozilla CA Program (ca-program@mozilla.com), Microsoft Trusted Root Program, Apple Root Program, Google Chrome Root Program, Adobe Approved Trust List — notificate prin canalele oficiale de incident reporting în cazul în care rădăcinile QSIGN au fost incluse în magazinele de încredere respective.

Întocmit și certificat,

QSIGN S.R.L. — prin Administrator

Trandafirescu Alexandru Florin

Data: 06.05.2026

Semnătura electronică calificată:

Versiune document: 01 Cod: TP-AC Clasificare: Public