

Termini e Condizioni Generali di Utilizzo di APP-ARE

(Validi per Utenti Privati / B2C, Aziende e Professionisti / B2B e Pubbliche Amministrazioni / P.A.)

Edizione: 3.0 – Produzione, Trasparenza Tariffaria e Asseverazione Forense

Piattaforme autorizzate: Apple App Store (iOS) & Google Play Store (Android)

Portale web di verifica indipendente: app-are-web.com

Articolo 1 – Premesse, Definizioni e Ambito Soggettivo (B2C, B2B e P.A.)

1.1. I presenti Termini e Condizioni Generali di Utilizzo (di seguito, "Termini") disciplinano l'accesso, l'installazione e l'utilizzo dell'applicazione denominata **APP-ARE** (di seguito, l'"Applicazione" o la "Piattaforma") e delle connesse infrastrutture telematiche di calcolo crittografico, validazione temporale e verifica pubblica, fornite dalla società titolare del servizio (di seguito, il "Fornitore" o "Titolare"), i cui dati societari, legali e di contatto sono consultabili all'interno dell'Applicazione e sul portale web ufficiale.

1.2. L'Applicazione è destinata all'utilizzo da parte di una pluralità di categorie soggettive, nello specifico:

- a) **Utenti Privati / Consumatori (B2C):** Persone fisiche che utilizzano il servizio per finalità personali, private ed estranee a qualsiasi attività commerciale, imprenditoriale o professionale, ai sensi del D.Lgs. 206/2005 (Codice del Consumo);
- b) **Utenti Aziende e Professionisti (B2B):** Persone giuridiche, società di persone o di capitali, ditte individuali, periti, tecnici e liberi professionisti che integrano il servizio nei propri processi d'impresa, peritali o di audit;
- c) **Pubbliche Amministrazioni ed Enti Pubblici (P.A.):** Amministrazioni statali, enti locali, corpi di polizia locale, organi di vigilanza edilizia e ambientale, stazioni appaltanti ed enti pubblici che impiegano l'Applicazione per la verbalizzazione di sopralluoghi, verifiche dello stato dei luoghi, accertamento dello stato di avanzamento lavori (SAL), gestione di beni demaniali o constatazione di infrazioni.

1.3. L'installazione, la registrazione e l'uso di APP-ARE comportano l'accettazione integrale, consapevole e senza riserve dei presenti Termini da parte dell'Utente o del soggetto che legalmente rappresenta l'Ente o l'Azienda contraente.

1.4. Ai fini dei presenti Termini, si assumono le seguenti definizioni:

- a) **Report Tecnico:** Il documento informatico in formato PDF generato dall'Applicazione, contenente la riproduzione fotografica acquisita alla fonte, i relativi parametri spazio-temporali, i dati telemetrici del dispositivo, la marca temporale qualificata e l'impronta di notarizzazione su registro distribuito;
- b) **Impronta Crittografica (Digest / Hash SHA-256):** La sequenza alfanumerica univoca generata mediante l'algoritmo standard SHA-256 che fotografa matematicamente il flusso ottico e il documento, garantendo che qualsiasi modifica successiva, anche di un singolo bit, alteri irrimediabilmente l'impronta;
- c) **Marca Temporale Qualificata:** La validazione temporale elettronica rilasciata da un Prestatore di Servizi Fiduciari Qualificato (QTSP) ai sensi del Regolamento UE n. 910/2014 (eIDAS);
- d) **Registro Distribuito (Blockchain):** Il registro informatico pubblico e decentralizzato su cui viene depositato l'hash del Report ai sensi dell'art. 8-ter del D.L. 135/2018 (conv. in L. 12/2019);
- e) **Controparte:** Il terzo invitato dall'Utente a controfirmare il Report mediante l'inserimento di una One-Time Password (OTP) ricevuta via posta elettronica;
- f) **Pacchetto di Certificati:** Il quantitativo predefinito e a consumo di crediti/certificazioni acquistato una tantum dall'Utente, senza vincoli di abbonamento o addebiti periodici automatici.

Articolo 2 – Finalità dello Strumento, Qualificazione Probatoria e Distinzione Dogmatica

2.1. Si informa espressamente l'Utente che l'Applicazione e i relativi Report non intendono e non possono fornire di per sé "prove legali" precostituite nel senso tecnico-formale del diritto processuale (ossia prove che vincolano

tassativamente il giudice nella decisione, come l'atto pubblico redatto da pubblico ufficiale fino a querela di falso ex art. 2700 c.c.).

2.2. Lo scopo esclusivo di APP-ARE è dotare la riproduzione fotografica e documentale di tutti i crismi tecnici, crittografici, temporali e procedurali previsti dalla scienza informatico-forense (standard ISO/IEC 27037) e dalle normative europee e nazionali (Regolamento eIDAS e Codice dell'Amministrazione Digitale). Tale apparato di presidi è specificamente concepito per:

- a) Fornire elementi oggettivi di integrità, immutabilità e certezza temporale;
- b) Consentire alla rappresentazione informatica di resistere efficacemente al disconoscimento generico di controparte ai sensi dell'art. 2712 c.c.;
- c) Fornire all'autorità giudiziaria o peritale un corredo di evidenze verificabili idoneo a consentire la transizione del reperto da mera prova semplice (liberamente contestabile) a prova dotata di piena efficacia probatoria e asseverativa, valutabile ai sensi dell'art. 20, comma 1-bis del CAD e dell'art. 116 c.p.c.

2.3. Il Fornitore non garantisce e non può garantire l'esito dei contenziosi giudiziari, amministrativi o assicurativi in cui il Report viene prodotto, rimanendo la decisione finale sull'efficacia probatoria devoluta al prudente apprezzamento dell'autorità giudiziaria competente.

Articolo 3 – Requisiti Funzionali, Piattaforme Store e Permessi di Sistema

3.1. L'Applicazione è reperibile unicamente sui canali ufficiali Apple App Store (per sistemi operativi iOS) e Google Play Store (per sistemi operativi Android).

3.2. L'elaborazione del Report richiede obbligatoriamente che l'Utente mantenga attivi sul proprio terminale:

- Il modulo fotocamera;
- Il modulo di geolocalizzazione satellitare (GNSS/GPS) e di rete;
- L'identificativo tecnico del dispositivo (fingerprint hardware);
- Una connessione dati Internet funzionante durante la generazione della certificazione.

3.3. L'assenza o la disattivazione anche parziale di tali autorizzazioni impedisce tecnicamente il congelamento dello scatto e la chiusura della procedura fiduciaria.

Articolo 4 – Modalità DEMO ed Espressa Assenza di Valore Certificativo

4.1. L'Applicazione mette a disposizione degli Utenti una specifica "**Modalità DEMO**", utilizzabile prima o indipendentemente dall'acquisto dei pacchetti a pagamento, con lo scopo esclusivo di testare le inquadrature, verificare l'interfaccia e comprendere il funzionamento dell'app.

4.2. L'Utente prende atto ed accetta espressamente che il documento PDF rilasciato all'esito di una sessione in Modalità DEMO:

- a) È totalmente privo di valore certificativo, asseverativo o probatorio, sia sostanziale che processuale;
- b) Viene generato mediante marche temporali simulate/fittizie e non subisce alcun effettivo ancoraggio su registri blockchain;
- c) Non effettua controlli bloccanti sull'accuratezza dei sensori, della geolocalizzazione o della rete;
- d) Reca impresso un contrassegno indelebile e una filigrana visibile a schermo e sul documento: "*PDF marcato DEMO – nessun valore certificativo*".

4.3. È fatto espresso e perentorio divieto all'Utente di depositare, notificare, trasmettere o spendere il PDF ottenuto in Modalità DEMO in sede processuale, dinanzi a pubbliche amministrazioni, enti assicurativi o controparti private per attestare alcunché. Il Fornitore declina ogni responsabilità per l'indebito utilizzo o per l'affidamento che terzi dovessero erroneamente riporre in elaborati dimostrativi.

Articolo 5 – Flusso di Acquisizione: Inibizione della Galleria e Blocco dello Scatto

5.1. Al fine di garantire la rigorosa catena di custodia digitale ed escludere il rischio di manomissioni preventive, l'Applicazione acquisisce le immagini esclusivamente mediante scatto in tempo reale operato attraverso la fotocamera comandata dal software (*capture-at-source*). L'Applicazione inibisce in modo assoluto il prelievo, il caricamento o l'importazione di fotografie, screenshot o filmati presenti nella galleria multimediale, nella memoria interna del dispositivo o su spazi cloud esterni. L'Applicazione inibisce altresì lo zoom e altre operazioni da effettuarsi in fase di scatto così come specificato nel successivo articolo 6.

5.2. Nell'istante esatto della cattura, l'Applicazione blocca la sequenza di fotogrammi ricevuta dal sensore ottico, estrae i dati telemetrici ambientali e genera localmente il digest crittografico SHA-256 prima di qualsiasi archiviazione temporanea, rendendo impossibile l'intercalazione di software manipolatori.

Articolo 6 – Assoluta Esclusione di Modelli di Intelligenza Artificiale

6.1. Il Fornitore garantisce che la catena di elaborazione di APP-ARE preserva il flusso ottico nella sua configurazione originaria.

6.2. È tassativamente escluso l'utilizzo di algoritmi di miglioramento semantico, filtri di fotoritocco, motori predittivi o modelli di intelligenza artificiale (generativa, additiva o sottrattiva). La Piattaforma non effettua alcuna ricostruzione o correzione dei pixel, attestando unicamente la corrispondenza oggettiva della rappresentazione visiva con quanto intercettato dal sensore ottico.

Articolo 7 – Conformità Fiduciaria eIDAS, Blockchain e Portale di Verifica

7.1. Al Report generato in sessione effettiva viene applicata una Marca Temporale Qualificata rilasciata da un Prestatore di Servizi Fiduciari Qualificato (QTSP) ai sensi degli artt. 41 e 42 del Regolamento UE n. 910/2014, la quale gode della presunzione legale di esattezza della data e dell'ora e di integrità dei dati in tutti gli Stati membri dell'Unione Europea.

7.2. L'impronta crittografica del Report viene memorizzata su un registro distribuito pubblico in conformità all'art. 8-ter della Legge n. 12/2019, attribuendo certezza decentralizzata, immutabile e non retrodatabile all'avvenuta asseverazione.

7.3. Qualsiasi interessato, perito, magistrato o terza parte può accertare in ogni tempo l'autenticità e la non alterazione del documento collegandosi al portale web **app-are-web.com**, mediante inserimento del codice hash SHA-256 o scansione del QR-Code presente sul PDF, ottenendo conferma immediata della corrispondenza dell'impronta e dell'ora di notarizzazione.

Articolo 8 – Oggetto dell'Asseverazione: Cose, Documenti e Rilievi Misti

8.1. L'Applicazione consente di asseverare:

- **Cose materiali, luoghi e manufatti:** Stato di immobili, cantieri edili, sinistri stradali, impianti industriali, merci, inventari o beni mobili;
- **Documenti:** Contratti, scritture private cartacee, testamenti, lettere, bolle di consegna o notifiche;
- **Ambiti congiunti e misti:** La contestuale e correlata presenza di cose e documenti (ad esempio, un macchinario diforme ritratto unitamente al relativo manuale di istruzioni o alla bolla di trasporto).

8.2. L'attestazione riguarda esclusivamente la conformità fenomenica e spazio-temporale di quanto inquadrato dal sensore al momento dello scatto; l'Applicazione non certifica né accerta la validità intrinseca, l'autenticità sostanziale o la legittimità giuridica dei documenti o delle cose riprodotte.

Articolo 9 – Asseverazione Unilaterale o Bilaterale con OTP Controparte

9.1. L'Utente esegue l'acquisizione a proprio beneficio o per gli scopi della propria organizzazione/amministrazione.

9.2. **Modalità Bilaterale con Controparte (Firma Elettronica):**

- a) L'Utente immette nell'interfaccia i dati anagrafici essenziali e l'indirizzo di posta elettronica della Controparte;

- b) Il sistema genera e trasmette automaticamente a tale indirizzo email un codice monouso (OTP) temporizzato, unitamente alla sintesi dell'asseverazione;
- c) L'inserimento del codice OTP da parte della Controparte realizza la controfirma del documento;
- d) La procedura si qualifica tecnicamente e giuridicamente come **Firma Elettronica** ai sensi dell'art. 3, n. 10 del Regolamento eIDAS e dell'art. 20, co. 1-bis del Codice dell'Amministrazione Digitale, il cui valore probatorio è liberamente valutabile in giudizio tenendo conto dei requisiti oggettivi di integrità e tracciabilità informatica.

9.3. L'onere di accertare che l'indirizzo email immesso appartenga effettivamente alla persona o all'ente controinteressato ricade interamente ed esclusivamente sull'Utente.

Articolo 10 – Divieto Assoluto di "Foto su Foto", Frodi Probatorie e Usi Illeciti

10.1. È fatto espresso e tassativo divieto all'Utente di puntare l'obiettivo della fotocamera verso display elettronici (monitor di computer, televisori, schermi di smartphone o tablet), fotografie cartacee, stampe o qualsiasi supporto bidimensionale che riproduca un'immagine scattata in precedenza o creata artificialmente, al fine di simulare l'acquisizione in tempo reale o alterare artatamente la collocazione spazio-temporale dello scatto.

10.2. La violazione del divieto di "foto su foto" costituisce gravissima violazione contrattuale e integra comportamenti suscettibili di integrare reati perseguiti dalla legge penale (tra cui frode processuale, truffa, tentata estorsione o falsità ideologica). Il Fornitore si riserva la facoltà di revocare immediatamente l'accesso al servizio e di segnalare l'accaduto alle competenti autorità giudiziarie o agli ordini professionali di appartenenza.

10.3. È vietato l'utilizzo dell'Applicazione per:

- a) Violare la riservatezza altrui (inclusa la ripresa non autorizzata in luoghi di privata dimora ex art. 615-bis c.p.);
- b) Riprendere materiale pedopornografico, diffamatorio, minatorio o contrario a norme imperative;
- c) Riprendere materiale contraffatto, illegale, illecito;
- d) Costruire elementi probatori fraudolenti finalizzati a trarre in inganno magistrati, periti o organi di controllo.

Articolo 11 – Integrità del Dispositivo e Divieto di Spoofing, Root e Jailbreak

11.1. L'Applicazione deve essere installata su dispositivi con sistema operativo integro. È tassativamente vietato l'impiego su dispositivi sottoposti a modifiche di sistema quali rooting (Android) o jailbreak (iOS), nonché l'uso all'interno di emulatori o macchine virtuali.

11.2. È vietato l'utilizzo di applicativi terzi deputati a falsificare la geolocalizzazione (GPS spoofing o mock location) o ad alterare l'orario di sistema. Il rilevamento di tali anomalie comporta l'annullamento della sessione di asseverazione.

Articolo 12 – Modello Economico a Pacchetti, Prezzi sull'App ed Esclusione di Abbonamenti

12.1. Il servizio APP-ARE non prevede contratti di abbonamento periodico né meccanismi di rinnovo automatico.

12.2. L'accesso alle funzionalità di certificazione effettiva avviene unicamente tramite l'acquisto di Pacchetti di Certificati a consumo (crediti predefiniti). Ciascun pacchetto attribuisce all'Utente il diritto di generare il numero corrispondente di Report Tecnici Forensi reali.

12.3. I prezzi applicabili, i tagli dei pacchetti disponibili e le condizioni economiche sono indicati in modo chiaro, analitico e aggiornato direttamente all'interno dell'interfaccia dell'Applicazione nella schermata di acquisto, prima della conferma della transazione.

12.4. L'acquisto dei pacchetti su dispositivi mobili si perfeziona tramite i canali di pagamento In-App autorizzati (Apple In-App Purchase e Google Play Billing). Esauriti i certificati inclusi nel pacchetto, l'Applicazione cessa la facoltà di scatto reale fino all'acquisto di un nuovo pacchetto, senza che intervenga alcun addebito ricorrente.

Articolo 13 – Pacchetti Personalizzati per Aziende (B2B) e Pubbliche Amministrazioni (P.A.)

13.1. Per le esigenze strutturate di Aziende, Ordini Professionali e Pubbliche Amministrazioni, il Fornitore predispone pacchetti personalizzati su misura con quantitativi elevati di crediti, opzioni multi-utenza per operatori sul territorio, cruscotti web dedicati e interfacce API per l'integrazione con i sistemi gestionali o di protocollo dell'Ente.

13.2. L'approvvigionamento dei pacchetti da parte delle Pubbliche Amministrazioni può avvenire mediante affidamento diretto o procedure telematiche nel rispetto del Codice dei Contratti Pubblici (anche tramite piattaforma MePA / Consip), con emissione di determina a contrarre, rilascio di CIG/CUP ove previsto e liquidazione su presentazione di Fattura Elettronica PA (con codice IPA e split payment).

Articolo 14 – Conservazione dei Dati, Privacy e Backup a Carico dell'Utente

14.1. Per preservare la riservatezza commerciale, personale e istituzionale dell'Utente, i server del Fornitore non conservano in modo permanente copia dei file fotografici originali o dei Report PDF definitivi, limitandosi a mantenere i metadati telemetrici, i log di trasmissione e l'impronta hash SHA-256 necessari al funzionamento del portale di verifica app-are-web.com.

14.2. Il Report PDF generato viene trasmesso all'Utente o salvato nella memoria del suo dispositivo. Una copia può restare temporaneamente sui server del Fornitore solo per il tempo tecnico di consegna al dispositivo e, se prevista, della finestra OTP controparte; tale copia viene eliminata al termine di tali operazioni e, in ogni caso, entro al massimo ventiquattro (24) ore. E' onere esclusivo e inderogabile dell'Utente (e dell'Amministrazione o Impresa contraente) provvedere al tempestivo download, alla duplicazione di sicurezza, alla conservazione a norma e al backup permanente del file PDF originale. Lo smarrimento del documento da parte dell'Utente rende impossibile per il Fornitore procedere a un recupero del contenuto visivo, restando archiviata unicamente l'impronta crittografica pubblica.

Articolo 15 – Responsabilità Esclusiva dell'Utente e Manleva Totale

15.1. L'Utente assume in via totale ed esclusiva ogni responsabilità civile, penale, amministrativa e disciplinare connessa all'impiego dell'Applicazione, alla legittimità dell'accesso ai luoghi inquadrati, alla liceità della riproduzione dei documenti e all'utilizzo giudiziale o stragiudiziale del Report.

15.2. Il Fornitore si limita a fornire l'infrastruttura tecnologica e non assume alcuna qualifica di pubblico ufficiale, perito asseveratore o certificatore della veridicità intrinseca del contenuto materiale inquadrato.

15.3. L'Utente (ivi compresi l'Azienda o l'Ente per conto del quale l'operatore agisce) si obbliga a tenere integralmente indenne, manlevare e difendere il Fornitore, i suoi soci, legali rappresentanti, dipendenti e fornitori di servizi fiduciari da qualsivoglia richiesta risarcitoria, danno, perdita, pregiudizio economico, sanzione comminata da autorità garanti (incluso il Garante per la Protezione dei Dati Personali) e spesa legale (incluse spese stragiudiziali e peritali) cagionati da:

- a) Uso illecito, doloso o negligente dell'Applicazione o dei Report generati;
- b) Violazione del divieto perentorio di "foto su foto" o manipolazione dei dati di acquisizione;
- c) Lesione di diritti di terzi (violazione della privacy altrui, violazione di segreti industriali o brevetti);
- d) Erronea o fraudolenta digitazione dell'indirizzo email della Controparte nelle procedure OTP;
- e) Indebita spendita verso terzi del documento rilasciato in Modalità DEMO.

Articolo 16 – Diritto di Recesso per l'Utente Consumatore (B2C)

16.1. Qualora l'Utente rivesta la qualifica di Consumatore, ha diritto di recedere dall'acquisto del pacchetto di certificati entro 14 (quattordici) giorni dalla data di transazione, a condizione che i certificati acquistati non siano stati utilizzati, inoltrando istanza secondo le procedure di rimborso previste da Apple o Google Play.

16.2. Ai sensi dell'art. 59, comma 1, lett. a) del Codice del Consumo, l'Utente riconosce e accetta espressamente che, avviando la generazione e la marcatura di un Report reale prima della scadenza del termine di 14 giorni, richiede l'esecuzione immediata della prestazione tecnologica; per l'effetto, per i singoli certificati già erogati e consumati il diritto di recesso si intende definitivamente perso.

Articolo 17 – Dipendenze Tecnologiche e Limiti di Responsabilità del Fornitore

17.1. L'Applicazione interagisce con infrastrutture di terze parti indipendenti (reti di telecomunicazione, store di Apple e Google, Prestatori Fiduciari Qualificati e reti blockchain pubbliche). Il Fornitore non risponde di eventuali ritardi, disservizi o mancate marcature derivanti da guasti o congestioni di tali nodi esterni.

17.2. Fatti salvi i limiti inderogabili posti dall'art. 1229 c.c. per i casi di dolo o colpa grave, la responsabilità economica complessiva del Fornitore nei confronti degli Utenti professionali (B2B) o delle Pubbliche Amministrazioni non potrà in alcun caso eccedere l'importo complessivamente corrisposto dall'Ente o dall'Azienda per l'acquisto del pacchetto di certificati all'interno del quale si è verificato l'evento contestato.

Articolo 18 – Proprietà Intellettuale

18.1. Il marchio APP-ARE, l'infrastruttura software, il codice sorgente, l'architettura dei sigilli crittografici, le interfacce grafiche e la composizione strutturale del report PDF costituiscono proprietà industriale e intellettuale esclusiva del Fornitore.

18.2. All'Utente viene concessa una licenza d'uso non esclusiva, a tempo determinato (fino al consumo dei crediti), revocabile e non cedibile a terzi, con divieto categorico di compiere attività di decompilazione, reverse engineering o estrazione sistematica delle logiche di funzionamento.

Articolo 19 – Sospensione del Servizio e Risoluzione Espressa

19.1. Il Fornitore ha facoltà di bloccare l'accesso al profilo e risolvere di diritto il rapporto contrattuale ai sensi dell'art. 1456 c.c. qualora riscontri:

- a) L'effettuazione di "foto su foto" o tentativi di generazione di prove fittizie;
- b) L'esecuzione dell'app su terminali con jailbreak, root o software di spoofing delle coordinate;
- c) L'impiego della Piattaforma per attività contrarie all'ordine pubblico o alla legge penale.

19.2. Nelle suddette fattispecie, i crediti residui presenti sul pacchetto saranno incamerati a titolo di penale risarcitoria, fatto salvo il risarcimento del maggior danno.

Articolo 20 – Legge Applicabile e Foro Competente

20.1. I presenti Termini sono regolati e interpretati in conformità alla legge italiana.

20.2. Per le controversie che vedano parte un Utente Consumatore, la competenza territoriale spetta inderogabilmente al Tribunale del luogo di residenza o domicilio elettivo del Consumatore, ai sensi del Codice del Consumo.

20.3. Per qualsiasi controversia promossa da o contro Utenti Imprese o Professionisti, è stabilita la competenza territoriale esclusiva ed inderogabile del Foro della sede legale del Fornitore. Per i contratti conclusi con Pubbliche Amministrazioni, restano salve le eventuali norme inderogabili di competenza territoriale previste dall'ordinamento processuale per le controversie con lo Stato o gli enti pubblici.

Articolo 21 – Disposizioni Finali e Rinvio ai Contratti Specifici

21.1. I presenti Termini disciplinano in via generale le condizioni d'uso dell'applicativo e i requisiti di funzionamento tecnologico dello scatto certificato.

21.2. Tra le parti saranno predisposti e sottoscritti separati schemi contrattuali dedicati:

- a) Uno schema contrattuale per i Privati Consumatori (B2C);
- b) Uno schema contrattuale per le Imprese e i Professionisti (B2B);
- c) Uno schema contrattuale e amministrativo per le Pubbliche Amministrazioni (P.A.).

21.3. L'eventuale nullità o inefficacia di una clausola dei presenti Termini non inficia la validità delle restanti previsioni, che manterranno piena efficacia e cogenza tra le parti.

INTEGRAZIONE ? VINCOLO DISPOSITIVI (device binding)

Edizione allineata a Termini 3.1 / Privacy 1.1 / Contratti B2C-B2B 1.1.

Ai fini di sicurezza, antifrode e corretta esecuzione del servizio APP-ARE:

- 1) Un medesimo fingerprint tecnico di dispositivo (non IDFA/AAID) può essere associato a un solo account APP-ARE: non è consentito condividere lo stesso telefono o tablet tra utenze diverse.
- 2) Account B2C e account Admin (titolare azienda / Admin di team / admin P.A.): massimo 1 (uno) telefono e 1 (uno) tablet contemporaneamente collegati.
- 3) Account Operatore (sotto-account B2B o P.A.): massimo 1 (uno) solo dispositivo (telefono oppure tablet).
- 4) L'accesso da PC o browser web non occupa gli slot e non consente di certificare; resta disponibile, ove previsto, la console organizzativa da PC.
- 5) Se lo slot è pieno, l'Utente può sostituire in autonomia, tramite l'Applicazione, il dispositivo precedente della stessa classe (o l'unico dispositivo per l'Operatore).
- 6) La generazione di un Report richiede che il dispositivo in uso risulti collegato all'account. Le misure sono proporzionate: nessuna garanzia di impossibilità assoluta di elusione tecnica.

Base privacy (ove applicabile): fingerprint e binding trattati per contratto (art. 6.1.b GDPR), legittimo interesse antifrode/sicurezza (art. 6.1.f) e, per la rilevazione del fingerprint in onboarding, consenso (art. 6.1.a). Conservazione dell'associazione: durata del rapporto fino a sostituzione, revoca del consenso fingerprint o chiusura account.

Riferimenti: Termini Art. 3.4; Contratto B2C Art. 3.5; Contratto B2B Art. 3.5; Privacy sez. 2.B.7 / finalità binding; testi autorizzativi fingerprint.