

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI (PRIVACY POLICY) E COOKIE POLICY DELLA PIATTAFORMA "APP-ARE"

(Ai sensi degli articoli 13 e 14 del Regolamento UE 2016/679 – GDPR, del D.Lgs. 196/2003 e s.m.i., delle Linee Guida del Garante per la Protezione dei Dati Personali del 10 giugno 2021 e del Regolamento UE 910/2014 "eIDAS")

Applicativi di riferimento: Applicazione Mobile APP-ARE (iOS / Android) e Portale Web di Verifica (app-are-web.com)

SEZIONE I – INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI (PRIVACY POLICY)

1. Titolare del Trattamento e Canali di Contatto

Il Titolare del Trattamento dei dati personali è la società proprietaria e gestrice della piattaforma tecnologica APP-ARE (di seguito indicata come il "**Titolare**" o "**APP-ARE**"), con sede legale e recapiti indicati nella sezione "Account" dell'Applicazione e sulla pagina principale del portale web app-are-web.com.

Per qualsiasi richiesta relativa all'esercizio dei diritti garantiti dal GDPR o per comunicazioni urgenti in merito alla sicurezza dei dati:

- ? Indirizzo PEC: re-seller@pec.it
- ? Email ordinaria per l'esercizio dei diritti privacy: privacy@app-are-web.com
- ? Canale dedicato alla gestione e notifica di incidenti di sicurezza / Data Breach: dpo@app-are-web.com

2. Categorie di Dati Personali Trattati

APP-ARE tratta esclusivamente i dati personali strettamente necessari a garantire la catena di custodia digitale, l'integrità probatoria del reperto, l'esecuzione del contratto di servizio e gli adempimenti di legge.

A. Dati Anagrafici e di Profilo (Onboarding)

- 1) **Utente Persona Fisica (B2C):** Nome, cognome, codice fiscale, indirizzo di residenza o domicilio, indirizzo email ordinario, password crittografata (hash saltato).
- 2) **Utente Azienda / Professionista (B2B):** Ragione sociale, Partita IVA, codice fiscale dell'ente, sede legale, numero di iscrizione al Registro delle Imprese (CCIAA), generalità e codice fiscale del Legale Rappresentante o procuratore delegato, indirizzo email aziendale, recapito telematico di fatturazione (Codice Destinatario SDI o casella PEC).
- 3) **Pubbliche Amministrazioni (P.A.):** Denominazione dell'Ente/Settore, Codice Fiscale, sede istituzionale, Codice Univoco Ufficio (IPA), generalità del funzionario o dell'operatore verbalizzante autorizzato, indirizzo email istituzionale, casella PEC istituzionale.

B. Dati Telemetrici, Tecnici e di Sicurezza del Dispositivo (*Device Fingerprint*)

- 1) Impronta tecnica univoca non commerciale del terminale (*device fingerprint* logico/hardware);
- 2) Marca, modello commerciale e produttore del dispositivo (es. Redmi Note 13, iPhone 18);
- 3) Tipologia e versione del sistema operativo installato (es. Android, iOS);
- 4) Stato di integrità dell'ambiente software (assenza di permessi di *root*, *jailbreak*, emulatori o strumenti di alterazione di sistema);
- 5) Indirizzo IP di connessione e parametri di rete utilizzati durante la sessione di asseverazione.
- 6) **Dichiarazione espressa di esclusione:** L'infrastruttura di APP-ARE esclude in modo assoluto e categorico la lettura, l'accesso o il trattamento di qualsiasi identificativo pubblicitario tracciante o di profilazione commerciale (quali Apple IDFA o Google AAID).

C. Dati di Geolocalizzazione Spazio-Temporale

- 1) Coordinate geospaziali fini (latitudine, longitudine, altitudine e raggio di accuratezza metrica stimata), rilevate tramite la costellazione satellitare GNSS/GPS;
- 2) Dati di triangolazione dei ponti radio di telefonia mobile (celle cellulari) e identificativi tecnici dei nodi Wi-Fi rilevati all'atto dello scatto;
- 3) La raccolta di tali dati avviene esclusivamente nel momento puntuale in cui l'Utente avvia l'acquisizione; non viene effettuato alcun tracciamento continuo, periodico o in background della posizione dell'Utente.

D. Flusso Visivo, Immagini e Documento PDF Forense (*Zero Knowledge Media Storage*)

- 1) Flusso ottico acquisito in tempo reale dal sensore della fotocamera (*capture-at-source*);
- 2) Dati grezzi dell'immagine elaborati in locale per la generazione del Report PDF e del relativo codice alfanumerico di hash SHA-256;

3) Principio Zero-Knowledge: i server di backend di APP-ARE non conservano in via definitiva né archiviano copie dei file fotografici originali né dei Report PDF definitivi. L'Applicazione elabora transitoriamente il flusso per comporre il Report PDF, lo rende disponibile all'Utente sul dispositivo e rimuove immagini e copia efilemra del PDF (subito dopo consegna/claim e comunque entro max 24 ore), trattenendo solo hash SHA-256 e metadati tecnici di audit (art. 5, par. 1, lett. c, GDPR).

E. Dati per la Certificazione Bilaterale con Controparte (OTP)

- 1) Indirizzo di posta elettronica della Controparte, immesso dall'Utente per la controfirma;
- 2) Log di generazione, trasmissione e ricezione del codice numerico monouso (One-Time Password - OTP);

- 3) Timestamp certificato del momento di immissione dell'OTP da parte della Controparte e relativo indirizzo IP di provenienza della connessione.

F. Dati Trattati sul Portale Web di Verifica (app-are-web.com)

- 1) Stringa crittografica di hash SHA-256 inserita manualmente o acquisita tramite scansione del QR-Code per l'interrogazione dello stato di validità;
- 2) Indirizzo IP e log tecnici di connessione al portale web (per sole finalità di sicurezza perimetrale e protezione da attacchi informatici).

3. Finalità del Trattamento e Basi Giuridiche (Art. 6 GDPR)

Finalità del Trattamento	Dati Trattati	Base Giuridica (Regolamento UE 2016/679)
Registrazione e Gestione Account: Creazione del profilo B2C, B2B o P.A., autenticazione, erogazione dei pacchetti acquistati.	Dati anagrafici, credenziali di accesso, recapiti di contatto.	Esecuzione di misure precontrattuali o contrattuali (Art. 6, par. 1, lett. b, GDPR).
Acquisizione Forense e Asseverazione: Blocco dello scatto in-app, georeferenziazione, rilievo fingerprint e composizione del Report Tecnico.	Flusso fotocamera, coordinate GPS/triangolazione, fingerprint dispositivo.	Consenso espresso dell'interessato prestato in fase di onboarding (Art. 6, par. 1, lett. a, GDPR) ed esecuzione del contratto (Art. 6, par. 1, lett. b, GDPR).
Validazione Temporale e Notarizzazione Fiduciaria: Trasmissione del solo hash SHA-256 al QTSP e alla blockchain.	Digest SHA-256, metadati di marcatura temporale.	Esecuzione del contratto (Art. 6, par. 1, lett. b, GDPR) e adempimento di obblighi legali derivanti da Reg. eIDAS e CAD (Art. 6, par. 1, lett. c, GDPR).
Procedura di Controfirma Bilaterale con OTP: Generazione, inoltro e verifica del codice OTP all'email della Controparte.	Email della Controparte, codice OTP, log di sessione e indirizzo IP.	Esecuzione del contratto e del servizio richiesto dalle parti (Art. 6, par. 1, lett. b, GDPR).
Amministrazione, Contabilità e Fatturazione: Gestione dei pagamenti, fatturazione elettronica (B2B e P.A.), adempimenti tributari.	Dati societari, P.IVA, CF, indirizzo, dati di pagamento, codici SDI/PEC/IPA.	Adempimento di un obbligo legale fiscale e civilistico (Art. 6, par. 1, lett. c, GDPR).
Sicurezza Informatica, Antifrode e Protezione Catena di Custodia: Rilevamento di tentativi di spoofing, emulatori, jailbreak o uso abusivo di "foto su foto".	Device fingerprint, log di accesso, indirizzo IP, telemetrie hardware.	Legittimo interesse del Titolare alla sicurezza delle reti e alla tutela della credibilità probatoria della Piattaforma (Art. 6, par. 1, lett. f, GDPR).
Tutela Giudiziaria del Titolare: Difesa dei diritti di APP-ARE in sede contenziosa o istruttoria in caso di manomissione o manleva.	Dati contrattuali, log di tracciamento, riscontri crittografici.	Legittimo interesse del Titolare all'esercizio del diritto di difesa in giudizio (Art. 6, par. 1, lett. f, GDPR).

4. Fornitori Terzi, Destinatari dei Dati e Sub-Responsabili (Art. 28 GDPR)

Per garantire i massimi livelli di resilienza informatica, conformità normativa fiduciaria, APP-ARE si avvale dei servizi tecnici di terze parti specificamente selezionate. I dati personali sono comunicati unicamente a tali soggetti nei limiti delle rispettive funzioni:

A. Google (Google Ireland Limited / Google LLC)

- 1) **Ruolo e Servizi:** Fornitore dell'infrastruttura di cloud computing, database distribuiti, bilanciamento del carico di rete, servizi di storage protetto di backend (Google Cloud Platform) e servizi applicativi di base per i terminali Android (Google Play Services).
- 2) **Dati Trattati:** Dati di profilo, log tecnici di rete, impronte hash e metadati di sessione.
- 3) **Garanzie di Protezione:** Google opera in qualità di Responsabile del Trattamento (Art. 28 GDPR). I datacenter primari sono situati all'interno dello Spazio Economico Europeo (SEE). Qualora intervengano trattamenti transfrontalieri da parte di Google LLC, essi sono regolati dalle Clausole Contrattuali Standard (SCC) della Commissione Europea e dal quadro di adeguatezza EU-U.S. Data Privacy Framework.

B. Namirial S.p.A.

- 1) **Ruolo e Servizi:** Prestatore di Servizi Fiduciari Qualificato (QTSP) accreditato a livello europeo ai sensi del Regolamento UE n. 910/2014 ("eIDAS") e vigilato dall'Agenzia per l'Italia Digitale (AgID). Namirial eroga il servizio di marcatura temporale qualificata (*Qualified Electronic Time Stamp*).

- 2) **Dati Trattati: Esclusivamente il digest crittografico (stringa di hash SHA-256) del Report e i metadati temporali di richiesta.** A Namirial S.p.A. non viene in alcun modo trasmesso il file visivo originale, né la foto scattata, né i dati personali anagrafici contenuti all'interno del report. Namirial non ha alcuna visibilità sul contenuto materiale asseverato.
- 3) **Sede del Trattamento:** Italia / Unione Europea.

C. Polygon Network (Tecnologia a Registri Distribuiti / Blockchain Pubblica)

- 1) **Ruolo e Funzione:** Protocollo e rete blockchain pubblica decentralizzata utilizzata per la notarizzazione immutabile, non retrodatabile e accessibile a terzi del digest SHA-256 del Report Tecnico Forense, ai sensi dell'art. 8-ter del D.L. 135/2018 (L. 12/2019).
- 2) **Dati Trattati e Natura Crittografica:** Sulla blockchain di Polygon viene trascritta e memorizzata pubblicamente in via definitiva unicamente ed esclusivamente l'impronta crittografica SHA-256 (hash). L'hash è un dato matematico unidirezionale, pseudonimizzato/anonimizzato alla fonte, dal quale è tecnicamente impossibile risalire all'immagine originaria o all'identità anagrafica dell'Utente senza il possesso del file originale. Nessun dato personale identificativo in chiaro (nome, cognome, email, coordinate GPS in chiaro o immagini) viene mai scritto sul registro distribuito.
- 3) **Decentralizzazione e Immutabilità:** L'Utente è consapevole che le transazioni convalidate sui nodi distribuiti della rete Polygon sono per loro natura intrinseca permanenti, imm modificabili e non cancellabili da parte di alcuna autorità centrale o dal Titolare.

D. Altri Destinatari Necessari

- 1) Fornitori dei servizi di posta elettronica transazionale (per il recapito immediato dei codici OTP alla Controparte);
- 2) Autorità Giudiziarie, Forze dell'Ordine o Autorità di Vigilanza nei soli casi in cui la comunicazione sia imposta da ordini vincolanti dell'autorità o da precisi obblighi di legge;
- 3) Istituti bancari e circuiti di pagamento degli store digitali (Apple Inc. e Google LLC) per la gestione delle transazioni finanziarie relative ai pacchetti di certificati.

5. Trasferimento dei Dati Personali verso Paesi Terzi (Extra-UE)

I dati trattati da APP-ARE sono prioritariamente archiviati ed elaborati su server collocati all'interno dell'Unione Europea.

Qualora taluni fornitori di supporto tecnico o di infrastruttura cloud (quali Google) abbiano sede o instradino porzioni di traffico verso gli Stati Uniti o altri Paesi extra-SEE, il trasferimento avviene nel rigoroso rispetto delle condizioni stabilite dal Capo V del GDPR:

- 1) Verso Paesi destinatari di una Decisione di Adeguatezza adottata dalla Commissione Europea (art. 45 GDPR), ivi incluso il regime stabilito dall'*EU-U.S. Data Privacy Framework*;
- 2) In subordine, sulla base dell'adozione delle Clausole Contrattuali Standard (SCC) conformi al modello approvato dalla Commissione Europea (art. 46, par. 2, lett. c, GDPR), integrate da misure supplementari tecniche, logiche e di cifratura end-to-end.

6. Periodo di Conservazione dei Dati (Data Retention)

Il Titolare conserva i dati personali per il tempo strettamente necessario al conseguimento delle finalità per cui sono stati raccolti, secondo i seguenti criteri:

- 1) **Dati anagrafici dell'Account:** Conservati per l'intera durata del rapporto di fornitura e, a seguito della chiusura dell'account, per un periodo di 10 (dieci) anni, in ottemperanza agli obblighi civilistici e di prescrizione dei diritti contrattuali (art. 2220 c.c.).
- 2) **Dati di Fatturazione e Pagamento:** Conservati per 10 (dieci) anni dall'emissione del documento fiscale, in conformità agli obblighi tributari di legge.

3) Flusso Immagini, PDF efimeri e File Temporanei: solo tempo tecnico di assemblaggio, consegna al dispositivo e (se prevista) finestra OTP controparte; eliminazione automatica al termine e comunque entro massimo 24 ore (Zero Knowledge / Termini Art. 14).

futuro la validazione dell'integrità del reperto da parte dell'Utente o dei periti incaricati in sede giudiziaria.

- 5) **Log della Controfirma OTP (Email, IP, Timestamp):** Conservati per 10 (dieci) anni dall'emissione del Report, quale evidenza tecnica a supporto della validità della firma elettronica bilaterale in caso di contenzioso sulla paternità dell'atto.
- 6) **Notarizzazione Blockchain (Polygon):** Permanente e non reversibile in virtù dell'architettura intrinseca del registro distribuito decentralizzato.

7. Diritti dell'Interessato (Artt. 15-22 GDPR)

In conformità agli articoli da 15 a 22 del Regolamento UE 2016/679, ciascun Utente ha il diritto di esercitare in qualsiasi momento nei confronti del Titolare i seguenti diritti:

1. **Diritto di Accesso (Art. 15):** Ottenere la conferma che sia o meno in corso un trattamento di propri dati e riceverne copia intelligibile;
2. **Diritto di Rettifica (Art. 16):** Chiedere l'aggiornamento, la correzione o l'integrazione dei propri dati inesatti;

3. **Diritto alla Cancellazione ("Diritto all'Oblio", Art. 17):** Chiedere la cancellazione dei dati personali trattati, qualora non sussistano più le finalità contrattuali o obblighi di conservazione imposti dalla legge;
4. **Diritto di Limitazione del Trattamento (Art. 18):** Ottenere il contrassegno dei dati conservati nei casi previsti dalla norma;
5. **Diritto alla Portabilità dei Dati (Art. 20):** Ricevere i dati personali forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico, o richiederne il trasferimento a un altro titolare;
6. **Diritto di Opposizione (Art. 21):** Opporsi in qualsiasi momento al trattamento fondato sul legittimo interesse del Titolare;
7. **Revoca del Consenso (Art. 7, par. 3):** Revocare in qualsiasi momento il consenso all'accesso a GPS, fotocamera o fingerprint (tale revoca preclude tuttavia la facoltà di generare nuovi Report forensi, senza pregiudicare la liceità del trattamento antecedentemente prestato).

Nota Operativa sull'Esercizio del Diritto alla Cancellazione in Ambito Blockchain

L'impronta registrata sulla blockchain pubblica di Polygon è un digest crittografico SHA-256 matematico. In virtù della struttura decentralizzata e immutabile del registro distribuito, non è tecnicamente possibile operare la cancellazione o la riscrittura del blocco convalidato. Tuttavia, la totale disassociazione e cancellazione dei dati anagrafici dell'Utente dai database del Titolare garantisce la definitiva e assoluta impossibilità di ricollegare tale hash a un soggetto identificabile, realizzando una totale e irreversibile de-identificazione/anonimizzazione.

Modalità di Esercizio dei Diritti e Reclamo

L'Utente può esercitare i propri diritti inviando apposita istanza all'indirizzo email: privacy@app-are-web.com

Qualora l'Utente ritenga che il trattamento dei propri dati violi il GDPR, ha il diritto inderogabile di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali (Piazza Venezia 11, 00187 Roma – www.garanteprivacy.it) o di adire le opportune sedi giudiziarie competenti.

8. Gestione delle Violazioni dei Dati Personali (Data Breach Policy)

In ossequio agli articoli 33 e 34 del GDPR, APP-ARE ha adottato una specifica procedura interna per il rilevamento tempestivo, l'analisi del rischio e la gestione delle violazioni di sicurezza che comportino accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque trattati.

- 1) Qualora si verifichi una violazione suscettibile di presentare un rischio per i diritti e le libertà delle persone fisiche, il Titolare provvederà a notificare l'evento all'Autorità Garante per la Protezione dei Dati Personali senza ingiustificato ritardo e, ove fattibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza.
- 2) Ove la violazione comporti un rischio elevato per i diritti degli interessati, il Titolare provvederà a comunicare la violazione direttamente agli Utenti coinvolti senza ritardo, fornendo le raccomandazioni idonee ad attenuarne le potenziali conseguenze negative.
- 3) **Recapito dedicato esclusivo per la segnalazione di vulnerabilità, incidenti informatici o Data Breach:**

dpo@app-are-web.com

COOKIE POLICY E STRUMENTI DI TRACCIAMENTO

(Informativa estesa per l'Applicazione APP-ARE e il portale web app-are-web.com)

La presente Cookie Policy descrive le modalità con cui l'applicazione mobile APP-ARE e il portale di verifica indipendente app-are-web.com impiegano cookie, web storage locale e identificatori tecnici equivalenti.

1. Dichiarazione Tassativa di Assenza di Cookie di Profilazione

Si informa formalmente e categoricamente l'Utente che la piattaforma APP-ARE e il portale web app-are-web.com **NON UTILIZZANO IN ALCUN MODO** cookie di profilazione, cookie comportamentali, pixel di monitoraggio per retargeting pubblicitario o identificatori di marketing di terze parti.

Nessun dato di navigazione, di ricerca o di utilizzo del servizio viene ceduto, analizzato o incrociato con piattaforme esterne di ad-tech per finalità pubblicitarie, di marketing diretto o di profilazione commerciale delle abitudini dell'Utente.

2. Tipologie di Marcatori Tecnici Utilizzati

L'infrastruttura web e mobile di APP-ARE utilizza esclusivamente:

A. Cookie Tecnici e di Navigazione Strettamente Necessari

Tali strumenti sono indispensabili per il corretto e sicuro funzionamento della piattaforma telematica. Essi includono:

- 1) **Cookie di Autenticazione e Sessione:** Necessari a mantenere attiva la sessione di accesso protetta dell'Utente sul portale di verifica o durante le chiamate API protette;
- 2) **Marcatori Anti-CSRF (Cross-Site Request Forgery):** Token di sicurezza generati per impedire l'esecuzione non autorizzata di comandi e garantire che le chiamate al backend provengano unicamente dall'interfaccia autenticata;
- 3) **Storage Locale Tecnico (Local Storage / SharedPreferences):** Memoria locale del terminale mobile utilizzata dall'Applicazione per mantenere le preferenze di interfaccia (es. selezione lingua "IT / EN") e l'eventuale memorizzazione temporanea del digest da verificare.

Base giuridica: L'utilizzo di questi strumenti non richiede il preventivo consenso dell'interessato ai sensi dell'art. 122 del Codice Privacy (D.Lgs. 196/2003) e dell'art. 6, par. 1, lett. b ed f del GDPR, in quanto essi sono strettamente funzionali all'erogazione di un servizio esplicitamente richiesto dall'Utente.

B. Cookie Analitici di Prima Parte Anonimizzati (Ove Presenti)

Qualora vengano impiegati strumenti di conteggio statistico degli accessi al portale web app-are-web.com, tali strumenti operano esclusivamente con **anonimizzazione completa e preventiva dell'indirizzo IP** (mascheramento dell'ultimo otte).

I dati statistici ricavati sono totalmente aggregati e anonimi, non consentono in alcun caso la re-identificazione dell'Utente e sono assimilati ai cookie tecnici per espressa statuizione delle Linee Guida del Garante Privacy del 10 giugno 2021, risultando pertanto esenti dall'obbligo di consenso preventivo o banner bloccante.

3. Strumenti Utilizzati sui Dispositivi Mobili (In-App SDKs)

All'interno dell'Applicazione mobile per iOS e Android:

- 1) Non vengono integrati SDK o framework software di circuiti pubblicitari (ad esempio, Google AdMob, Meta Audience Network o simili);
- 2) Sono presenti esclusivamente le librerie tecniche di runtime necessarie per il funzionamento dell'acquisizione della fotocamera, l'interrogazione delle API di geolocalizzazione, la gestione crittografica dell'algoritmo SHA-256 e i canali di pagamento ufficiali previsti da Apple Inc. e Google LLC.

4. Tabella Riepilogativa dei Marcatori Tecnici

Denominazione	Tipologia e Finalità	Soggetto Erogatore	Durata di Conservazione
__session_id	Tecnico di navigazione: mantenimento sessione sicura di verifica report.	Prima Parte (app-are-web.com)	Sessione (eliminato alla chiusura del browser)
XSRF-TOKEN	Tecnico di sicurezza: protezione contro attacchi Cross-Site Request Forgery.	Prima Parte (app-are-web.com)	Sessione / Fino a 2 ore
app_lang_pref	Tecnico di funzionalità: memorizzazione della preferenza linguistica (IT/EN).	Prima Parte (Locale in-app / web)	Persistente (fino a 12 mesi o cancellazione cache)
secure_api_key	Tecnico di sistema: autorizzazione scambio chiavi crittografiche verso backend Google Cloud.	Prima Parte / Google Cloud	Sessione tecnica di calcolo

5. Gestione e Disabilitazione dei Cookie da Parte dell'Utente

Fermo restando che l'infrastruttura di APP-ARE impiega esclusivamente marcatori tecnici, l'Utente può configurare in qualunque momento le preferenze del proprio browser web per bloccare, limitare o cancellare i cookie.

Le istruzioni dettagliate per la gestione dei cookie sui principali browser sono reperibili ai seguenti canali ufficiali:

- **Google Chrome:** Impostazioni > Privacy e sicurezza > Cookie di terze parti e dati dei siti
- **Mozilla Firefox:** Opzioni > Privacy e sicurezza > Cookie e dati dei siti web
- **Apple Safari (macOS / iOS):** Impostazioni > Safari > Blocca tutti i cookie
- **Microsoft Edge:** Impostazioni > Cookie e autorizzazioni sito > Gestisci ed elimina cookie e dati del sito

Avvertenza tecnica: La disattivazione totale o il blocco preventivo dei cookie tecnici strettamente necessari all'interno del browser web può impedire la corretta visualizzazione delle pagine del portale app-are-web.com e pregiudicare la corretta esecuzione della verifica telematica dei Report crittografici.

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.