Informativa sul Trattamento dei Dati Personali

ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679 (GDPR)

e del D.lgs. 196/2003 e successive modificazioni

Titolare del Trattamento: ARYEL S.R.L.
Qualifica: Internet Service Provider (ISP) – Operatore di comunicazioni elettroniche in postazione fissa
Sede legale: Via Cappuccini 19/A, 36015 Schio (VI)
P.IVA: 04273730244
PEC: aryel@pec.it
E-mail: assistenza@aryel.it
Sito web: www.aryel.it

La presente Informativa descrive le modalità con cui ARYEL SRL (di seguito "Titolare"), in qualità di Internet Service Provider (ISP) e operatore di comunicazioni elettroniche in postazione fissa, raccoglie, utilizza e protegge i dati personali dei propri Clienti, Utenti e altri interessati nell'ambito della fornitura dei Servizi di connettività e telecomunicazioni, in conformità al Regolamento UE 2016/679 (GDPR), al D.lgs. 196/2003 e s.m.i., al D.lgs. 259/2003 (Codice delle Comunicazioni Elettroniche) e alle delibere AGCOM applicabili.

1. Categorie di Dati Personali Trattati

1.1 Dati dei Clienti – persone fisiche (Consumatori)

- Dati anagrafici e identificativi: nome, cognome, codice fiscale, data e luogo di nascita, documento di identità
- Dati di contatto: indirizzo di residenza, e-mail, telefono fisso e mobile, PEC
- Dati di pagamento: IBAN per addebito SEPA/SDD, metodi di pagamento elettronico (gestiti tramite circuiti certificati PCI-DSS; il Titolare non conserva i dati completi della carta)
- Dati tecnici del servizio: indirizzo IP assegnato (statico o dinamico), MAC address dell'apparato, configurazioni tecniche
- Dati di utilizzo: volumi di traffico aggregati, date di attivazione/disattivazione, stato del servizio

1.2 Dati dei Clienti – persone giuridiche (Business)

- Dati aziendali: ragione sociale, partita IVA, codice fiscale, sede legale e operativa
- Dati del referente/rappresentante legale: nome, cognome, e-mail, telefono, carica
- Dati di fatturazione e pagamento: coordinate bancarie, metodi di pagamento concordati

1.3 Dati tecnici e operativi specifici ISP

- Log di connessione e traffico: indirizzi IP di origine e destinazione, timestamp di connessione/disconnessione, protocolli utilizzati, dati necessari ai fini di sicurezza della rete e degli obblighi di legge (art. 123 D.lgs. 196/2003; D.lgs. 259/2003)
- Dati di autenticazione PPPoE/AAA: credenziali di accesso alla rete, sessioni attive

- Dati di diagnostica e monitoraggio: metriche di qualità (latenza, packet loss, velocità), log di malfunzionamenti e interventi tecnici
- Dati degli Apparati in comodato d'uso: numero seriale, MAC address, firmware, configurazioni

1.4 Dati di supporto e relazione con il Cliente

- Storico dei reclami, ticket di assistenza e comunicazioni (e-mail, Area Clienti, telefono)
- Registrazioni delle chiamate al servizio clienti (ove effettuate, con informativa specifica)
- Dati relativi a procedure di conciliazione ADR/Corecom

1.5 Dati di fornitori e collaboratori

- Dati anagrafici, fiscali e bancari di fornitori, vettori, professionisti e collaboratori per la gestione dei rapporti commerciali, contabili e fiscali

1.6 Dati particolari (categorie speciali)

Il Titolare non tratta, di norma, categorie particolari di dati ai sensi dell'art. 9 GDPR. Qualora il Cliente segnali esigenze legate a disabilità o condizioni di salute (es. attivazione Parental Control, servizi di telesoccorso), tali dati sono trattati esclusivamente con consenso esplicito e limitatamente alle finalità indicate.

2. Finalità e Basi Giuridiche del Trattamento

Finalità	Base giuridica (art. 6 GDPR)	Obbligatorio?
Conclusione ed esecuzione del Contratto (attivazione, gestione, fatturazione, assistenza, recesso, migrazione, trasloco)	Art. 6(1)(b) – Esecuzione contrattuale	Sì – senza questi dati il contratto non può essere eseguito
Adempimenti legali: obblighi fiscali, contabili, conservazione log di traffico ex D.lgs. 259/2003, normativa AGCOM	Art. 6(1)(c) – Obbligo legale	Sì – obbligatorio per legge
Erogazione, monitoraggio e garanzia della qualità del Servizio (SLA, misurazioni AGCOM, diagnostica)	Art. 6(1)(b) – Esecuzione contrattuale	Sì
Sicurezza della rete: prevenzione abusi, rilevamento intrusioni, gestione blacklist IP, rispetto AUP	Art. 6(1)(f) – Legittimo interesse	No, ma necessario per integrità della rete

Gestione reclami, procedure ADR/Corecom, tutela legale e contenziosi	Art. 6(1)(b)/(f) – Esecuzione contrattuale e legittimo interesse	No, ma inerente al rapporto contrattuale
Comunicazioni di servizio obbligatorie (variazioni contrattuali, manutenzioni, indennizzi automatici)	Art. 6(1)(b)/(c) – Esecuzione contrattuale e obbligo legale	Sì
Portabilità del numero (SPP) e migrazione verso/da altri operatori	Art. 6(1)(b)/(c) – Esecuzione contrattuale e obbligo legale (delibere AGCOM)	Sì se richiesta dal Cliente
Gestione anagrafica fornitori, collaboratori, professionisti esterni	Art. 6(1)(b)/(c) – Esecuzione contrattuale e obbligo legale	Sì per adempimenti fiscali e commerciali
Marketing diretto e profilazione (offerte commerciali, newsletter, sondaggi di soddisfazione)	Art. 6(1)(a) – Consenso	No – facoltativo, revocabile in qualsiasi momento

3. Tempi di Conservazione

Categoria di dati	Periodo di conservazione
Dati contrattuali e anagrafici clienti	10 anni dalla cessazione del contratto (art. 2220 c.c.)
Dati di fatturazione e pagamento	10 anni dalla data della fattura (obbligo fiscale)
Log tecnici di traffico e connessione (IP, sessioni, timestamp)	6 anni ai sensi del D.lgs. 259/2003 e delibere AGCOM, ovvero il termine di legge vigente al momento del trattamento
Dati di autenticazione e sessioni di rete	12 mesi dalla fine della sessione, salvo obblighi di legge più lunghi
Dati diagnostica e qualità del servizio	24 mesi
Storico reclami, ticket e comunicazioni assistenza	5 anni dalla chiusura
Dati procedure ADR/Corecom e contenziosi	10 anni dalla definizione della controversia
Log di accesso all'Area Clienti	12 mesi
Dati fornitori e collaboratori	10 anni dalla fine del rapporto (obbligo fiscale e civilistico)
Dati per marketing (con consenso)	Fino alla revoca del consenso o, in assenza di attività, 24 mesi dall'ultimo contatto

Alla scadenza dei termini di conservazione i dati sono cancellati o resi definitivamente anonimi. I termini possono essere prorogati in presenza di contenziosi pendenti, obblighi normativi sopravvenuti o richieste dell'Autorità Giudiziaria.

4. Destinatari e Comunicazione dei Dati

4.1 Responsabili del trattamento (art. 28 GDPR)

Il Titolare si avvale di soggetti terzi che trattano i dati per suo conto in qualità di Responsabili del Trattamento, con i quali sono stipulati appositi accordi di nomina. Le principali categorie sono:

- Operatori di accesso e infrastruttura wholesale (es. Open Fiber, TIM, Fastweb wholesale): per l'attivazione tecnica, la manutenzione e la gestione della rete di accesso
- Fornitori di sistemi di autenticazione e gestione AAA/RADIUS
- Fornitori di software gestionale, CRM, sistemi di ticketing e piattaforme di assistenza
- Fornitori di servizi di fatturazione elettronica e conservazione sostitutiva
- Istituti di pagamento e banche per la gestione degli addebiti SEPA/SDD
- Fornitori di servizi cloud e hosting per l'Area Clienti e i sistemi informativi aziendali
- Fornitori di servizi di monitoraggio della rete e sicurezza informatica (NOC, SOC)
- Studi legali e di consulenza, nei limiti strettamente necessari alla tutela dei diritti del Titolare

4.2 Titolari autonomi

- Autorità giudiziarie, di polizia e amministrative (AGCOM, Agenzia delle Entrate, Guardia di Finanza, Polizia Postale) quando obbligatorio per legge o per ordine dell'autorità
- CO.RE.COM e organismi ADR nell'ambito di procedure di conciliazione ex Delibera AGCOM n. 194/23/CONS
- Operatori di telecomunicazioni destinatari/cedenti nell'ambito di procedure di portabilità (SPP) e migrazione
- Istituti bancari per la gestione delle domiciliazioni e dei pagamenti

4.3 Diffusione

I dati personali non sono diffusi a soggetti terzi non identificati né ceduti o venduti per finalità commerciali proprie di terzi.

5. Trasferimento dei Dati verso Paesi Terzi

Il Titolare tratta i dati prevalentemente all'interno del territorio dell'Unione Europea. Qualora, per esigenze tecniche legate a specifici fornitori di servizi cloud o infrastrutturali, si renda necessario il trasferimento verso Paesi extra-UE, il Titolare assicura che tale trasferimento avvenga esclusivamente:

- verso Paesi riconosciuti dalla Commissione Europea come adeguati (art. 45 GDPR), oppure
- sulla base di Clausole Contrattuali Standard approvate dalla Commissione Europea (art. 46 GDPR), oppure
- in presenza di altre garanzie appropriate ai sensi del Capo V del GDPR.

Su richiesta, il Titolare fornisce informazioni specifiche sui trasferimenti in atto e sulle garanzie adottate.

6. Misure di Sicurezza e Asset Protection

ARYEL SRL adotta un insieme strutturato di misure tecniche e organizzative in linea con lo standard ISO/IEC 27001 e con i requisiti del GDPR (art. 32), applicate in modo costante e verificato periodicamente. Di seguito le principali misure adottate per categoria.

6.1 Sicurezza della rete e delle infrastrutture

- Cifratura di tutte le comunicazioni in transito tramite protocolli TLS/SSL
- Accesso ai sistemi IT consentito esclusivamente da dispositivi pre-autorizzati tramite filtro MAC e Network Access Control (NAC)
- Segmentazione della rete e isolamento dei sistemi di trattamento dei dati personali
- Monitoraggio continuo del traffico di rete per il rilevamento di anomalie e intrusioni

6.2 Controllo degli accessi e autenticazione

- Autenticazione a due fattori (2FA) per l'accesso a tutti i sistemi che trattano dati personali
- Autenticazione endpoint: ogni dispositivo deve essere pre-autorizzato nella rete aziendale
- Sistema di controllo degli accessi basato su ruoli (RBAC): i diritti di accesso sono assegnati secondo il principio del minimo privilegio
- Divieto di account condivisi; ogni utente dispone di credenziali personali
- Politiche di complessità delle password configurate e verificate automaticamente dal sistema
- Procedura formalizzata di revoca immediata dei diritti in caso di cessazione o cambio di ruolo del personale

6.3 Sicurezza di server e database

- I server operano con account di sistema a privilegi minimi (principio del least privilege)
- I database trattano esclusivamente i dati necessari alle finalità perseguite (principio di minimizzazione, art. 5 GDPR)
- Tecniche di protezione a livello database: interrogazioni autorizzate, controllo degli accessi granulare
- Cifratura dei dati sensibili a riposo

6.4 Backup e Business Continuity

- Backup completi eseguiti regolarmente, con verifica dell'integrità e della completezza
- Backup cifrati e archiviati in modo sicuro, anche offline
- Livello di protezione fisica e ambientale dei backup coerente con quello dei dati di origine
- Piano di Disaster Recovery definito e documentato con tempi di ripristino (RTO/RPO) definiti
- Personale con responsabilità, autorità e competenza specifiche per la gestione della Business Continuity in caso di incidente

6.5 Gestione degli incidenti e data breach

- Registro degli incidenti e delle violazioni dei dati personali, con documentazione dell'evento e delle azioni di mitigazione

- Incident Response Plan formalizzato con procedure dettagliate per una risposta efficace e ordinata
- Procedura di notifica al Garante entro 72 ore ai sensi dell'art. 33 GDPR
- Procedura di comunicazione agli interessati ai sensi dell'art. 34 GDPR, ove necessario
- Obbligo per i Responsabili del Trattamento di notificare al Titolare qualsiasi violazione senza indebito ritardo

6.6 Generazione di log e monitoraggio

- File di log generati per ogni sistema e applicazione utilizzata nel trattamento dei dati personali, comprensivi di tutte le tipologie di accesso (visualizzazione, modifica, cancellazione)
- Log contrassegnati con data e ora, sincronizzati con fonte temporale di riferimento (NTP)
- Log adeguatamente protetti da manomissioni e accessi non autorizzati
- Registrazione delle azioni degli amministratori di sistema (syslog, audit trail)

6.7 Sicurezza delle postazioni di lavoro e dispositivi mobili

- Software antivirus e firme di rilevamento aggiornati regolarmente (cadenza almeno settimanale)
- Aggiornamenti critici di sicurezza del sistema operativo installati regolarmente
- Timeout di sessione automatico in caso di inattività
- Gli utenti non possono disattivare le impostazioni di sicurezza né installare software non autorizzato
- Procedure documentate per la gestione dei dispositivi mobili e portatili, con pre-registrazione e pre-autorizzazione
- I dispositivi mobili sono soggetti agli stessi controlli di accesso delle postazioni fisse

6.8 Cancellazione sicura dei dati

- Sovrascrittura software su tutti i supporti prima della loro dismissione; distruzione fisica ove non applicabile (es. CD, DVD)
- Triturazione dei documenti cartacei e dei supporti portatili contenenti dati personali

6.9 Sicurezza nel ciclo di vita delle applicazioni

- Lo sviluppo software avviene in ambiente separato e non connesso ai sistemi di produzione
- Nei test vengono utilizzati dati fittizi; ove necessario l'uso di dati reali, sono previste procedure specifiche di protezione
- Adozione di framework e standard di codifica sicura e tecnologie PET (Privacy Enhancing Technologies)
- Requisiti di sicurezza definiti nelle fasi iniziali del ciclo di vita dello sviluppo

6.10 Gestione delle risorse IT (Asset Management)

- Registro/censimento aggiornato di tutte le risorse IT (hardware, software, rete) utilizzate per il trattamento dei dati personali
- Il registro include: tipo di risorsa, posizione fisica/elettronica, responsabile assegnato
- Revisione e aggiornamento annuale delle risorse IT
- Monitoraggio e registrazione di tutte le modifiche alle risorse e ai sistemi IT

6.11 Formazione e obblighi del personale

- Tutto il personale autorizzato al trattamento riceve formazione specifica sulla protezione dei dati e sulla sicurezza informatica
- Campagne periodiche di sensibilizzazione sui rischi e sugli obblighi in materia di privacy
- Ruoli e responsabilità relativi al trattamento chiaramente definiti e comunicati in fase di assunzione/incarico
- Obblighi di riservatezza formalmente assunti da tutto il personale coinvolto nel trattamento

6.12 Gestione dei Responsabili del Trattamento (fornitori)

- Prima dell'avvio di qualsiasi attività di trattamento, vengono definite e concordate linee guida e procedure formali con tutti i Responsabili del Trattamento
- I Responsabili del Trattamento devono garantire lo stesso livello di sicurezza adottato dal Titolare
- I Responsabili del Trattamento sono tenuti a fornire prove documentate di conformità
- Revisione periodica dei contratti con i Responsabili del Trattamento

6.13 Politiche di sicurezza

- La politica di sicurezza delle informazioni è documentata e forma parte integrante delle procedure aziendali
- Revisione semestrale delle policy di sicurezza con aggiornamento ove necessario
- Revisione annuale con verifica dell'effettiva adozione di tutte le misure

7. Diritti dell'Interessato

L'interessato ha il diritto di esercitare, in qualsiasi momento, i seguenti diritti nei confronti del Titolare:

Diritto	Contenuto
Accesso (art. 15)	Ottenere conferma del trattamento e copia dei dati personali trattati
Rettifica (art. 16)	Correggere dati inesatti o incompleti
Cancellazione (art. 17)	Ottenere la cancellazione dei dati ("diritto all'oblio"), ove non ostino obblighi di conservazione legale
Limitazione (art. 18)	Richiedere la sospensione del trattamento in determinati casi previsti dalla norma
Portabilità (art. 20)	Ricevere i dati in formato strutturato, di uso comune e leggibile da dispositivo automatico
Opposizione (art. 21)	Opporsi al trattamento basato sul legittimo interesse o per finalità di marketing diretto
Revoca del consenso (art. 7)	Revocare il consenso prestato in qualsiasi momento, senza pregiudizio per il trattamento precedente

Reclamo all'Autorità (art. 77)	Proporre reclamo al Garante per la Protezione dei Dati Personali (www.garanteprivacy.it)

Per esercitare i propri diritti, l'interessato può contattare il Titolare tramite:

- E-mail: assistenza@aryel.it
- PEC: aryel@pec.it
- Area Clienti: https://login.aryel.it
- Posta: ARYEL SRL, Via Cappuccini 19/A, 36015 Schio (VI)

Il Titolare risponde entro 30 giorni dal ricevimento, con possibilità di proroga di ulteriori 60 giorni in caso di complessità o numerosità delle richieste, previa comunicazione all'interessato.

8. Cookie e Tecnologie di Tracciamento

Il sito www.aryel.it e l'Area Clienti https://login.aryel.it utilizzano cookie tecnici necessari al funzionamento della piattaforma. L'utilizzo di cookie analitici o di profilazione è subordinato al consenso dell'utente, acquisito tramite banner cookie visualizzato al primo accesso.

L'informativa cookie dettagliata, con l'elenco dei cookie utilizzati e le relative finalità, è disponibile nella sezione "Cookie Policy" del sito www.aryel.it.

9. Minori

I Servizi di ARYEL SRL sono destinati a persone maggiorenni. Il Titolare non raccoglie consapevolmente dati personali di minori di 18 anni. Qualora vengano rilevati trattamenti non intenzionali di dati di minori, il Titolare provvederà alla loro immediata cancellazione. ARYEL SRL mette a disposizione il servizio gratuito di Parental Control per la protezione dei minori nella navigazione, ai sensi della Delibera AGCOM n. 9/23/CONS.

10. Aggiornamenti dell'Informativa

La presente Informativa può essere aggiornata in qualsiasi momento per adeguarsi a modifiche normative, tecnologiche o operative. Le versioni aggiornate sono pubblicate su www.aryel.it con indicazione della data di ultimo aggiornamento. In caso di modifiche sostanziali che incidano sui diritti degli interessati, il Titolare ne dà comunicazione tramite e-mail o Area Clienti con almeno 30 giorni di anticipo.

Documento: Informativa Privacy – v.2.0 – Aprile 2025 – Redatto ai sensi del GDPR e del D.lgs. 259/2003 – Depositato presso AGCOM