



Protezione dei dati personali e conformità normativa

GDPR (UE) 2016/679 - D.Lgs. 196/2003 s.m.i. - D.Lgs. 101/2018

Documento tecnico-organizzativo - settembre 2026

ACCOUNTABILITY

responsabilizzazione

PRIVACY BY DESIGN

protezione fin dalla progettazione

SECURITY

misure tecniche e organizzative

DATA SUBJECTS

tutela dei diritti

1. Finalità, ambito e quadro normativo

Il presente documento descrive il modello tecnico-organizzativo adottato da Italsenior srls per i trattamenti di dati personali effettuati nell'erogazione dei propri servizi software e SaaS e, in particolare, quando Italsenior opera quale Responsabile del trattamento per conto dei propri clienti.

Il riferimento normativo è costituito dal Regolamento (UE) 2016/679 (GDPR), dal D.Lgs. 30 giugno 2003 n. 196 - Codice in materia di protezione dei dati personali, come modificato e coordinato con il GDPR - e dal D.Lgs. 10 agosto 2018 n. 101, oltre ai provvedimenti applicabili dell'Autorità Garante.

Precisazione: la conformità privacy non può essere garantita da un documento isolato né dal solo fornitore tecnologico. Essa dipende anche dalle finalità e basi giuridiche definite dal Titolare, dalle informative, dai tempi di conservazione, dalle autorizzazioni, dai contratti e dalle concrete modalità di utilizzo del servizio. Italsenior garantisce, per la parte di propria competenza, l'adozione e il mantenimento delle misure e delle procedure qui descritte.

ARTICOLI 24, 26, 28 E 29 GDPR

2. Ruoli privacy e disciplina contrattuale

- **Titolare del trattamento:** il cliente determina finalità e mezzi essenziali del trattamento effettuato mediante il servizio.
- **Responsabile del trattamento:** quando tratta dati per conto del cliente, Italsenior opera sulla base di un atto conforme all'art. 28 GDPR, con oggetto, durata, natura, finalità, categorie di dati, interessati, obblighi e diritti del Titolare.
- **Persone autorizzate:** l'accesso ai dati è limitato ai soggetti autorizzati per necessità operative, vincolati alla riservatezza e istruiti sulle modalità di trattamento.
- **Sub-responsabili:** eventuali ulteriori responsabili sono gestiti secondo l'art. 28 GDPR, con preventiva autorizzazione specifica o generale del Titolare e obblighi sostanzialmente equivalenti.
- **Contitolarità:** qualora una specifica iniziativa determini congiuntamente finalità e mezzi, i ruoli devono essere valutati e, se necessario, disciplinati ai sensi dell'art. 26 GDPR.

ARTICOLO 5 GDPR

3. Principi applicati al trattamento

Liceità, correttezza e trasparenza Italsenior tratta i dati esclusivamente nell'ambito delle istruzioni documentate e delle finalità del servizio.	Limitazione della finalità I dati non sono utilizzati autonomamente per finalità incompatibili con quelle affidate dal cliente.
Minimizzazione Applicazioni e database sono progettati per trattare i dati necessari alle funzioni previste.	Esattezza Le piattaforme mettono a disposizione strumenti per aggiornamento, rettifica e gestione coerente delle informazioni.
Limitazione della conservazione I tempi di conservazione sono definiti dal Titolare e implementati tecnicamente ove previsti dal servizio.	Integrità e riservatezza Sono adottate misure di sicurezza, segregazione, controllo accessi, backup e protezione applicativa.
Accountability Misure, responsabilità e procedure sono documentate e riesaminate in funzione del rischio.	

4. Privacy by design e by default

La progettazione dei servizi segue un criterio di protezione dei dati fin dalla progettazione e per impostazione predefinita. Le funzioni vengono strutturate per evitare esposizioni non necessarie e per consentire al Titolare di configurare ruoli, permessi, accessi e dati effettivamente necessari.

- Separazione logica: dati e funzioni sono accessibili attraverso le sole applicazioni e credenziali autorizzate.
- Least privilege: profili e permessi sono assegnati in funzione del ruolo operativo.
- Database non esposti: i database applicativi non sono direttamente pubblicati su Internet.
- Risorse documentali: i collegamenti non devono rivelare direttamente la struttura fisica degli archivi; identificatori applicativi e controlli autorizzativi mediano l'accesso.
- Configurabilità: ove previsto, il Titolare può determinare quali categorie di dati e funzioni utilizzare.

ARTICOLO 32 GDPR

5. Sicurezza del trattamento

Le misure tecniche e organizzative sono definite tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

- Infrastruttura dedicata: server fisici di proprietà ItalSenior presso web farm Aruba IT2 di Arezzo.
- Stack ridotto: Linux, Apache HTTP Server, MariaDB e sole utilità strettamente necessarie; assenza di CMS e framework applicativi general-purpose sui sistemi di produzione.
- Firewall: filtraggio restrittivo consolidato, impostazione default deny e apertura dei soli flussi necessari.
- Hardening: disabilitazione dei servizi non necessari e riduzione della superficie di attacco.
- Software proprietario: applicazioni sviluppate internamente in Perl, con misure contro SQL Injection e XSS e controllo diretto del ciclo di rilascio.
- Accessi amministrativi: limitati ai soggetti autorizzati e alle esigenze tecniche.
- Segregazione: database e strutture interne non esposti direttamente alla rete pubblica.
- Continuità: server gemelli sincronizzati, procedure di subentro e riallocazione del servizio in caso di failure.
- Backup: copie di sicurezza dei programmi e dei dati, inclusa una copia separata presso la sede ItalSenior di Roma.
- Ripristino: procedure tecniche finalizzate a ripristinare disponibilità e accesso ai dati in caso di incidente fisico o tecnico.
- Monitoraggio: controllo operativo dei sistemi e analisi delle anomalie rilevanti.

ARTICOLI 9 E 10 GDPR

6. Categorie particolari di dati e dati sanitari

Alcuni servizi, in particolare quelli di telemedicina e assistenza domiciliare, possono comportare il trattamento di categorie particolari di dati personali, inclusi dati relativi alla salute. In tali casi ItalSenior tratta i dati esclusivamente nell'ambito delle istruzioni del Titolare e delle basi giuridiche da questo individuate.

Per tali trattamenti sono richieste misure rafforzate e una valutazione specifica del rischio. L'eventuale trattamento di dati relativi a condanne penali e reati deve avvenire esclusivamente nei casi e con le garanzie previste dall'art. 10 GDPR e dalla normativa nazionale applicabile.

7. Gestione delle credenziali, autorizzazioni e logging

- Identificazione individuale: gli accessi applicativi devono essere riconducibili a utenze e ruoli definiti.
- Autorizzazioni: ogni profilo accede alle sole funzioni e informazioni necessarie alla propria attività.
- Amministrazione: le credenziali tecniche e amministrative sono riservate ai soggetti autorizzati.
- Revoca: utenze e privilegi devono essere revocati o modificati quando cessano i presupposti di accesso.
- Tracciabilità: ove richiesto dalla natura del servizio, vengono registrati eventi applicativi e tecnici utili alla sicurezza e alla ricostruzione delle operazioni.
- Segretezza: password, token e altre credenziali non devono essere condivisi né conservati in chiaro nei flussi applicativi.

ARTICOLI 33 E 34 GDPR

8. Data breach

ItaSenior adotta una procedura per la gestione degli incidenti di sicurezza che possano determinare distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali.

- Rilevazione e contenimento: identificazione dell'evento, limitazione degli effetti e conservazione degli elementi utili all'analisi.
- Valutazione: analisi dei dati coinvolti, categorie e numero approssimativo di interessati e registrazioni, conseguenze probabili e misure adottate.
- Comunicazione al Titolare: quando ItaSenior opera come Responsabile, informa il Titolare senza ingiustificato ritardo dopo essere venuta a conoscenza della violazione, fornendo le informazioni disponibili e gli aggiornamenti successivi.
- Notifica all'Autorità: compete al Titolare, ove ricorrano i presupposti, effettuare la notifica al Garante entro il termine previsto dall'art. 33 GDPR, normalmente 72 ore dalla conoscenza.
- Comunicazione agli interessati: compete al Titolare nei casi di rischio elevato previsti dall'art. 34 GDPR, salvo le eccezioni applicabili.
- Registro degli incidenti: le violazioni e le relative valutazioni devono essere documentate secondo i ruoli e le responsabilità applicabili.

ARTICOLI 12-22 GDPR

9. Diritti degli interessati

Le piattaforme sono progettate per consentire al Titolare di gestire, nei limiti delle funzioni del servizio, le richieste di esercizio dei diritti degli interessati. ItaSenior, quale Responsabile, assiste il Titolare con misure tecniche e organizzative adeguate per dare seguito alle richieste.

- accesso ai dati personali e alle informazioni sul trattamento;
- rettifica dei dati inesatti e integrazione;
- cancellazione, quando applicabile;
- limitazione del trattamento;
- portabilità, nei casi previsti;
- opposizione, quando applicabile;
- gestione delle richieste relative a processi decisionali automatizzati, se presenti.

ARTICOLO 30 GDPR

10. Registro dei trattamenti e documentazione

ItaSenior mantiene, ove richiesto, la documentazione dei trattamenti effettuati in qualità di Responsabile ai sensi dell'art. 30, par. 2 GDPR, comprendente le categorie di trattamenti svolti per conto dei Titolari, gli eventuali trasferimenti e una descrizione generale delle misure tecniche e organizzative di sicurezza.

Il Titolare resta responsabile del proprio registro ex art. 30, par. 1 e della corretta descrizione di finalità, categorie di interessati e dati, destinatari, conservazione e misure applicabili.

11. Valutazione d'impatto e consultazione preventiva

Quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche - ad esempio per natura dei dati, monitoraggio sistematico, ampiezza o tecnologie impiegate - il Titolare valuta la necessità di una DPIA - Data Protection Impact Assessment.

ItalSenior, quale Responsabile, mette a disposizione del Titolare le informazioni tecniche ragionevolmente necessarie sulla piattaforma, sulle misure di sicurezza, sui flussi e sulle modalità di trattamento per supportare la DPIA e, ove necessario, la consultazione preventiva dell'Autorità.

ARTICOLI 37-39 GDPR

12. DPO e governance

La designazione del Responsabile della protezione dei dati (DPO/RPD) è valutata da ciascun soggetto sulla base dei presupposti dell'art. 37 GDPR e della normativa applicabile. Il presente documento non sostituisce tale valutazione.

Quando il cliente dispone di un DPO, ItalSenior coopera per gli aspetti tecnici e contrattuali relativi ai servizi affidati, nei limiti del proprio ruolo di Responsabile.

CICLO DI VITA DEI DATI

13. Conservazione, restituzione e cancellazione

- Conservazione: i tempi sono definiti dal Titolare in relazione alle finalità e agli obblighi di legge; ItalSenior implementa le regole tecniche previste dal servizio.
- Cessazione: al termine del rapporto, i dati personali sono restituiti o cancellati secondo le istruzioni contrattuali del Titolare, fatti salvi gli obblighi di conservazione previsti dalla legge.
- Backup: le copie di sicurezza seguono cicli tecnici di sovrascrittura/eliminazione coerenti con le procedure di continuità e con gli accordi applicabili.
- Supporti e sistemi dismessi: la dismissione deve evitare che dati residui restino accessibili a soggetti non autorizzati.

ARTICOLI 44-49 GDPR

14. Trasferimenti extra SEE

Per l'infrastruttura direttamente gestita da ItalSenior, i server descritti sono collocati in Italia. Eventuali servizi o fornitori esterni che comportino trasferimenti di dati personali verso Paesi al di fuori dello Spazio Economico Europeo devono essere preventivamente valutati e gestiti secondo il Capo V del GDPR, verificando la base del trasferimento e le garanzie applicabili.

ItalSenior non considera la semplice localizzazione europea dei server sufficiente, da sola, a escludere ogni possibile trasferimento: la valutazione deve comprendere anche eventuali subfornitori, servizi di comunicazione, assistenza o altri soggetti coinvolti nello specifico servizio.

15. Obblighi di ItalSenior quale Responsabile

Obbligo	Impegno
Istruzioni	trattare i dati personali soltanto su istruzione documentata del Titolare, salvo obblighi di legge applicabili.
Riservatezza	garantire che le persone autorizzate al trattamento siano vincolate alla riservatezza.
Sicurezza	adottare le misure richieste dall'art. 32 GDPR in relazione al rischio.
Sub-responsabili	rispettare le condizioni dell'art. 28, parr. 2 e 4, per il ricorso ad altri responsabili.
Diritti	assistere il Titolare, per quanto possibile, nel riscontro alle richieste degli interessati.
Compliance	assistere il Titolare negli obblighi relativi a sicurezza, data breach, DPIA e consultazione preventiva, tenendo conto della natura del trattamento e delle informazioni disponibili.
Fine servizio	cancellare o restituire i dati, a scelta del Titolare, salvo obblighi legali di conservazione.
Audit	mettere a disposizione le informazioni necessarie a dimostrare il rispetto dell'art. 28 e consentire verifiche secondo modalità contrattualmente definite, compatibili con sicurezza e continuità dei servizi.

ACCOUNTABILITY

16. Audit, verifiche e miglioramento continuo

Il modello di conformità viene mantenuto nel tempo mediante riesame delle misure tecniche e organizzative, aggiornamento dei sistemi, verifica delle configurazioni e adeguamento alle modifiche dell'architettura o dei trattamenti.

- Verifiche del cliente: possono essere concordate richieste documentali o audit, nel rispetto della riservatezza, della sicurezza degli altri clienti e della continuità operativa.
- Non conformità: eventuali criticità rilevate vengono valutate, prioritarizzate e corrette in relazione al rischio.
- Modifiche sostanziali: nuove categorie di dati, nuove integrazioni, nuovi subfornitori o nuove finalità richiedono una rivalutazione privacy e contrattuale.

17. Matrice di conformità essenziale

Norma	Tema	Presidio ItalSenior
Art. 5	Principi	minimizzazione, finalità, esattezza, conservazione, integrità/riservatezza, accountability
Art. 24	Responsabilità Titolare	supporto tecnico e documentale al cliente
Art. 25	Privacy by design/default	ruoli, segregazione, accessi minimi, configurabilità
Art. 28-29	Responsabile e autorizzati	DPA, istruzioni, riservatezza, sub-responsabili
Art. 30	Registro	documentazione delle categorie di trattamenti del Responsabile
Art. 32	Sicurezza	hardening, firewall, access control, backup, replica, ripristino
Art. 33-34	Data breach	procedura incidenti e comunicazione senza ingiustificato ritardo al Titolare
Art. 35-36	DPIA	supporto tecnico al Titolare per valutazione d'impatto
Art. 37-39	DPO	cooperazione con il DPO quando designato
Art. 44-49	Trasferimenti	valutazione di eventuali trasferimenti extra SEE

CHECKLIST CLIENTE + ITALSENIOR

18. Condizioni necessarie per la piena conformità del singolo servizio

- definizione documentata dei ruoli privacy e sottoscrizione dell'accordo ex art. 28, quando applicabile;
- individuazione da parte del Titolare delle finalità e delle basi giuridiche del trattamento;
- informative agli interessati e gestione degli eventuali consensi, quando necessari;
- definizione dei tempi di conservazione e delle regole di cancellazione;
- configurazione di utenti, ruoli e autorizzazioni coerente con le mansioni;
- valutazione delle categorie particolari di dati e delle eventuali misure rafforzate;
- valutazione DPIA quando ricorrono i presupposti;
- censimento di eventuali sub-responsabili e trasferimenti extra SEE;
- procedure per diritti degli interessati e data breach;
- riesame periodico di sicurezza, organizzazione e configurazione del servizio.

IMPEGNO ITALSENIOR

19. Dichiarazione conclusiva

ItalSenior srls dichiara di adottare, per i servizi ricadenti nel proprio perimetro operativo, misure tecniche e organizzative finalizzate al rispetto del Regolamento (UE) 2016/679 e del D.Lgs. 196/2003 s.m.i., secondo il ruolo concretamente assunto nel trattamento e secondo le istruzioni contrattuali ricevute dal Titolare.

Il presente documento costituisce una descrizione del modello di protezione dei dati e delle garanzie offerte dal fornitore. Non sostituisce l'accordo di nomina a Responsabile del trattamento ex art. 28 GDPR, il registro dei trattamenti, le informative, la DPIA o gli altri atti che risultino necessari per lo specifico trattamento.

20. Riferimenti normativi ufficiali

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR), in particolare artt. 5, 12-22, 24-30, 32-39 e 44-49.
- D.Lgs. 30 giugno 2003 n. 196 - Codice in materia di protezione dei dati personali, nel testo vigente e coordinato con il GDPR.
- D.Lgs. 10 agosto 2018 n. 101 - disposizioni di adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679.
- Provvedimenti, linee guida e indicazioni applicabili dell'Autorità Garante per la protezione dei dati personali.

Roma, 4 settembre 2026

Il Legale Rappresentante

Ing. Alvisè Valsecchi

Allegato A - Schema minimo di accordo ex art. 28 GDPR

Per rendere il fascicolo realmente operativo, al presente documento deve essere affiancato un accordo di nomina a Responsabile del trattamento riferito allo specifico cliente/servizio. L'accordo dovrebbe contenere almeno i seguenti elementi:

- Parti e ruoli: identificazione del Titolare e di Italsenior quale Responsabile.
- Oggetto e durata: servizio affidato e periodo del trattamento.
- Natura e finalità: operazioni svolte e scopi determinati dal Titolare.
- Tipologie di dati: dati anagrafici, contatti, dati amministrativi, documenti, credenziali, eventuali dati sanitari o altre categorie particolari.
- Categorie di interessati: utenti, iscritti, dipendenti, professionisti, assistiti, fornitori o altre categorie pertinenti.
- Istruzioni documentate: modalità con cui il Titolare impartisce e aggiorna le istruzioni.
- Riservatezza e autorizzati: obblighi delle persone che possono accedere ai dati.
- Misure di sicurezza: rinvio alle misure tecniche e organizzative applicabili al servizio.
- Sub-responsabili: autorizzazione, informativa sulle variazioni e obblighi equivalenti.
- Data breach: canali e tempi di comunicazione al Titolare.
- Diritti degli interessati: modalità di assistenza tecnica.
- DPIA e Autorità: collaborazione nei limiti delle informazioni disponibili.
- Restituzione/cancellazione: gestione dei dati alla cessazione.
- Audit: modalità, preavviso, riservatezza, costi e tutela degli altri clienti.
- Trasferimenti: regole applicabili a eventuali trattamenti o subfornitori extra SEE.

Nota: questo Allegato A è una checklist contrattuale, non una nomina già compilata. La nomina deve essere adattata allo specifico servizio e sottoscritta dalle parti.

ITALSENIOR SRLS

Allegato B - Dati societari

Ragione sociale	Italsenior srls
Sede	Via Donato Menichella 282 - 00156 Roma
PEC	italsenior@pec.it
P. IVA	14083161001
REA	RM-1495115
IBAN	IT23 U030 6984 8101 00000004379
Sito	www.italsenior.it