



persone x persone

Informazioni relative all'adeguamento di RIDInet in relazione al regolamento europeo 2016/679

Premessa

Lo scopo di questo documento è quello di riportare i necessari approfondimenti in relazione ai principi della privacy by design e della privacy by default, per ciò che si riferisce al servizio di teletrattamento riabilitativo RIDInet.

Minimizzazione nella durata del trattamento dati (5.1.f – 25.2)

Nel caso in questione, così come riportato nell'apposita informativa al consenso dei dati predisposta per gli operatori e per gli utenti che usano RIDInet, la durata del trattamento dei dati personali è stata minimizzata ad un periodo di due anni successivo alla cessazione del servizio stesso. Il servizio di cui parliamo viene fruito in modalità abbonamento con tempi diversi di durata (annuale, semestrale, trimestrale, ecc.) e sono correlate alla durata dei trattamenti riabilitativi, che spesso vengono riproposti attraverso un certo numero di cicli. Quindi, un operatore o un utente può abbonarsi più volte allo stesso servizio a seconda le proprie necessità e tale durata minima permette di poter accedere ai propri dati d'uso del servizio anche in relazione alle sessioni passate e quindi disporre della continuità di servizio e delle informazioni ad esso correlate, fino ad un periodo massimo di 24 mesi rispetto alla scadenza del proprio abbonamento non più rinnovato.

Minimizzazione nella tipologia di dati trattati (5.1.f – 25.2)

La tipologia dei dati personali che vengono trattati è strettamente connessa alle esigenze del servizio e all'efficacia delle app presenti nella piattaforma RIDInet, a disposizione degli operatori e degli utenti. In generale per gli operatori i dati personali richiesti riguardano il nominativo, il profilo professionale e l'indirizzo email. Per ciò che si riferisce agli utenti presi in carico dagli operatori, i dati personali registrati si riferiscono al nominativo, sesso, data di nascita e relativo indirizzo mail. Il resto della tipologia dei dati dell'utente riguarda le sessioni d'uso del servizio di teletrattamento rispetto alle app, nelle quali generalmente vengono registrati pochi dati di tipo prestazionale e cioè, ad esempio la velocità di sillabe lette al secondo, il grado di accuratezza rilevato, la durata della sessione di trattamento, la data, l'avanzamento nel percorso di presa in carico, ecc. Infine, nella parte relativa ai dati facoltativi, l'operatore in relazione all'utente può inserire i documenti afferenti alle valutazioni diagnostiche e i risultati derivanti dalla somministrazione dei test psicometrici.

Minimizzazione negli accessi ai dati (5.1.f – 25.2)

La quantità di dati raccolta è esclusivamente funzionale alle esigenze del servizio per garantire una efficace ed efficiente gestione del teletrattamento. La base dei dati, relativa agli utenti presi in carico dai professionisti, si incrementa esclusivamente sulla base dell'accesso dell'utente finalizzato allo svolgimento delle sessioni di trattamento riabilitativo, che possono raggiungere un numero di 4 o 5 volte alla settimana, sulla base delle indicazioni ricevute.

Limitazione del trattamento (considerando 67 – art. 4.3 – 18)

Il diritto alla limitazione del trattamento dei dati è garantito ed esplicitato nell'informativa al consenso che l'operatore o l'utente leggono ed eventualmente sottoscrivono prima dell'accesso al

servizio RIDInet. Inoltre, il sistema è predisposto per adempiere alle eventuali richieste di limitazione del trattamento.

Cancellazione dei dati (art. 17)

Il diritto alla cancellazione dei dati e all'oblio è garantito ed esplicitato nell'informativa al consenso che l'operatore o l'utente leggono ed eventualmente sottoscrivono prima dell'accesso al servizio RIDInet. Inoltre, il sistema è predisposto per adempiere alle eventuali richieste di cancellazione dei dati, nei limiti di quanto riportato nell'art. 17 del Regolamento UE n. 679/2016.

Possibilità di individuare una tempistica di conservazione dei dati (art. 13.2.a – 30.1.f)

Nell'informativa al consenso che l'operatore o l'utente leggono ed eventualmente sottoscrivono prima dell'accesso al servizio RIDInet, sono riportate con chiarezza le informazioni necessarie per il rispetto dei vincoli di legge e cioè:

- il periodo di conservazione dei dati personali;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo ad un'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4

Pseudonimizzazione dei dati (Considerando 26 - 28 - 29, Art. 4.5 - Art. 25 - Art. 32.1 - Art.40.2.d - Art. 89.2) e anonimizzazione dei dati (Considerando 26)

Nessun dato riguardante l'utilizzo di RIDInet da parte degli utenti è inviato a terzi, in nessuna forma (in chiaro, sotto pseudonimo o in forma anonima).

I dati riguardanti l'utilizzo di RIDInet da parte degli operatori è inviato a terzi in forma anonima a Google Analytics. Vengono inviati anche a Facebook e LinkedIn ma l'operatore viene identificato solo qualora abbia fatto accesso, su propria responsabilità, a questi servizi nello stesso computer in cui sta usando RIDInet.

Di default i cognomi dei bambini sono mostrati all'operatore solo con l'iniziale (pseudonimizzazione; es. Mario R.), per salvaguardare la loro privacy nei momenti in cui l'operatore mostra RIDInet alle famiglie.

L'operatore può scegliere di mostrare il nome per intero nei momenti in cui lo ritiene necessario e sotto la propria responsabilità.

I dati di utilizzo usati da Anastasis per fini commerciali e/o di ricerca sono sempre in forma aggregata e anonima.

Cifratura dei dati (art. 34.3.a)

Le comunicazioni tra il computer dell'operatore o della famiglia e il sito di RIDInet avvengono tutti con protocollo HTTPS e sono quindi cifrati.

All'interno del database di RIDInet (raggiungibile solo dagli amministratori di sistema di Anastasis), gli unici dati che identificano il bambino sono cognome ed email. Anastasis sta lavorando ad una nuova versione di RIDInet in cui questi dati saranno cifrati.

Sicurezza dei dati (art. 24, 25 e 32 GDPR)

Privacy by design e privacy by default

RIDInet viene sviluppato secondo i principi della privacy by design e della privacy by default da prima che venissero formalizzati. Anche (ma non solo) In base a questi principi, Anastasis segue per RIDInet un ciclo di sviluppo iterativo e quindi i suddetti principi vengono via via affinati nel tempo.

Integrità del servizio

Il server che ospita RIDInet è mantenuto aggiornato ed è configurato con l'obiettivo di impedire gli accessi non consentiti. Il server è inoltre monitorato in automatico ed eventuali disservizi sono segnalati automaticamente agli amministratori di sistema Anastasis.

Integrità dei dati

Violazione dei dati (art. 33 e 34 del GDPR)

Viene eseguito ogni notte il backup dei dati conservati in RIDInet. Il backup viene conservato in duplice copia in due server esterni al servizio RIDInet.

I due server sono geograficamente distanti per la salvaguardia da eventi catastrofici e sono protetti con lo stesso livello di sicurezza del server principale di RIDInet.

Per maggiori approfondimenti, si allegano al presente documento le informative privacy che RIDInet sottopone agli operatori e agli utenti, i contratti di servizio e l'allegato A, in cui Anastasis dichiara il rispetto della normativa in materia di privacy ai sensi del Regolamento UE n.679/2016. Distinti saluti.

Bologna, 27 giugno 2018

Il Rappresentante Legale
Tullio Maccarrone

