Valutazione d'impatto sulla protezione dei dati DPIA

NOME DEL PROGETTO:	**RIDInet**
DESCRIZIONE DEL PROGETTO:	**Teleriabilitazione integrata in presenza e online per Disturbi Specifici dell'Apprendimento e Bisogni Educativi Speciali**

Responsabile elaborazione DPIA:	Tullio Maccarrone	Posizione:	Titolare del trattamento dei dati

Sommario

Sezione 0 - Verifica preliminare di applicabilità della DPIA, in conformità all'articolo 33, comma 2 del regolamento generale

Sezione 1 - Avvio della valutazione

Sezione 2 - Impostazione dell'analisi di rischio preliminare

Sezione 3 - Esito dell'analisi preliminare dei rischi

Sezione 4 - Preparazione per la fase di consultazione ed analisi

Sezione 5 - Congruità con altre leggi, codici o regolamenti afferenti alla protezione dei dati

Sezione 6 - Contenuti analitici della DPIA

Sezione 7 - Approvazione della DPIA

Sezione 8 - Attivazione del trattamento

Appendice A - Lista di controllo della congruità del trattamento previsto con le esigenze di protezione dei dati

Appendice B - Tabella dei rischi afferenti alla DPIA

Appendice C - allegato B della legge 196

Sezione 0 - Verifica preliminare di applicabilità della DPIA, in conformità all'articolo 33, comma 2 del regolamento generale

Verificare se il trattamento coinvolto, dopo essere stato assoggettato all'analisi di rischio, può ricadere in uno dei casi previsti, per i quali è obbligatoria la conduzione di una DPIA

- ☐ Trattamenti sistematici ed estensivi di valutazione di aspetti personali dell'interessato, basati su sistemi automatizzati, inclusa la profilazione, i cui esiti portino a decisioni che possono avere effetti legali diretti ed indiretti sull'interessato-articolo 33 comma 2a

- ☐ Trattamento di dati afferenti a profili penali e giudiziari come illustrato nell'articolo 9a

- ☐ monitoraggio automatico di aree pubbliche, su larga scala

- ☐ altre attività di trattamento che siano inseriti nell'elenco pubblico dell'autorità garante nazionale, e che richiedono specificamente allo sviluppo di un data protection impart assessment-articolo 33. 2a

- ☐ trattamenti in cui una violazione dei dati può avere un impatto negativo sulla protezione dei dati stessi, nonché la riservatezza e i diritti o i legittimi interessi degli interessati coinvolti

- ☐ attività di trattamento che non rientra nei casi precedenti, ma per le quali il data controller redatto processo ritengono comunque sia appropriato svolgere una data protection impact assessment

X attività di trattamento rivolte a soggetti minori di età e su larga scala

Data di avvio della DPIA:	16/04/2023

Sezione 1 - Avvio della valutazione

1.1 traccia del progetto

RIDInet è una web application composta da:

- una “console” per la gestione dei Centri, degli operatori, degli abbonamenti, degli utenti, delle attività riabilitative assegnate, della parametrizzazione e del monitoraggio delle attività stesse
- una serie di applicazioni “riabilitative” attraverso le quali gli utenti si esercitano su lettura, scrittura, calcolo, comprensione del testo, funzioni esecutive etc. per il conseguimento degli obiettivi riabilitativi fissati dal clinico

I profili degli utenti vengono attivati solo da figure cliniche: le famiglie non possono acquistare un abbonamento a RIDInet in autonomia.

1.2 valutazione preliminare dell’utilizzo dei dati

1.2.2 Come i dati verranno raccolti?

I dati vengono raccolti nei database MySql della console e delle App all’interno di server Linux protetti da firewall e costantemente sottoposti ad audit di sicurezza.

1.2.3 Chi avrà accesso ai dati?

I tecnici Anastasis dichiarati nel DPS allegato al presente documento.
In occasione dei periodici AUDIT di sicurezza, il consulente incaricato con accesso temporaneo.

1.2.4 In che modo i dati verranno trasferiti a soggetti terzi?

I soggetti terzi a cui alcuni dati possono essere trasferiti sono:

- clinici e ricercatori che conducono sperimentazioni. In questo caso i dati sono trasferiti in forma anonima ed in ogni caso con l’esplicito consenso degli utenti, memorizzato in fase di iscrizione alla piattaforma

1.2.5 Come i dati verranno archiviati, aggiornati ed eliminati quando non più necessari ?

RidiNet è un'applicazione web based ospitata in un sistema ad architettura Cloud server ridondante multiprocessore multicore con connettività a banda illimitata, max 100MB/sec.

Il server è virtualizzato all'interno di un cluster: un eventuale crash di una macchina fisica non sarà percepito dall'utente finale in quanto tutto il sistema è replicato su un cluster di più macchine fisiche.

Indipendentemente dal clustering, ogni notte viene effettuato in automatico un backup del database consistente nel suo dump in formato SQL, compresso con compressione gzip: ad ogni backup viene creato un file nuovo con nome
db <nomeapplicazione> <data>.sql.gz, in maniera tale da rendere possibile il

reperimento di dati vecchi, o il ripristino della situazione ad una determinata data. Tali backup vengono mantenuti per un mese: superato il quale, viene mantenuto solo il backup relativo al primo giorno di ogni mese.

Il server che ospita l'applicazione ha aperte dall'esterno verso l'interno esclusivamente le seguenti porte:

- 22 per le comunicazioni SSH
- 80 per le comunicazioni HTTP
- 443 per le comunicazioni HTTPS

Il filtraggio dei pacchetti IP è affidato ad un firewall esterno.

I dati personali verranno conservati per tutta la durata dei servizi erogati da Anastasis e per un periodo successivo fino ad almeno 2 anni, per garantire gli adempimenti normativi e amministrativi di legge. Si precisa che i citati dati non sono soggetti ad un trasferimento ad un paese terzo o ad una organizzazione internazionale.

1.3 analisi preliminare dei soggetti coinvolti

- Anastasis, ed in particolare:
  - product owner
  - team di sviluppo
  - team commerciale
  - assistenza clienti
- Il comitato scientifico
- I clinici (psicologi, logopedisti e neuropsichiatri infantili) che acquistano un abbonamento al servizio per il proprio Centro, di cui sono denominati “referenti”
- I clinici colleghi dei referenti che vengono da questi registrati nella piattaforma
- I clinici che si registrano alla piattaforma nella modalità “demo gratuita per un mese”
- Le famiglie dei bambini presi in carico sono registrate dai clinici, non possono iscriversi autonomamente.

Sezione 1 completata da:	Tullio Maccarrone	Data:	28/04/2023

Sezione 2 - Impostazione dell'analisi di rischio preliminare

2.1 Tecnologie utilizzate

2.1.1 in questo progetto verranno utilizzate nuove tecnologie informatiche che potrebbero avere un significativo potenziale di violazione della protezione dei dati personali e riduzione del livello di protezione dei dati, che bisogna garantire agli interessati?

No

2.2 Metodi di identificazione

2.2.1 verranno utilizzati nuovi metodi di identificazione dei dati o verranno riutilizzati identificatori già esistenti ed in uso?

No

2.2.3 verranno utilizzati nuovi o significativamente modificati requisiti di autentica di identità, che possono risultare intrusivi od onerosi?

No

2.3 Coinvolgimento di altre strutture

2.3.1 Questa iniziativa di trattamento coinvolge altre strutture, sia pubbliche, sia private, sia appartenenti a settori non-profit e volontari?

RIDInet è una piattaforma online: il trattamento è erogato dai clinici che acquistano il servizio. Possono essere psicologi, logopedisti e neuropsichiatri infantili che lavorano privatamente o in strutture, piccole o grandi, pubbliche o private.

2.4 Modifiche alle modalità di trattamento dei dati

2.4.1 Questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di trattamento dei dati personali, che potrebbero destare preoccupazioni nell'interessato?

Il servizio richiede la memorizzazione di dati anagrafici degli utenti su server Anastasis. Discorso a parte va fatto per i dati sulla salute: se è vero che la registrazione di diagnosi ed esiti di test psicometrici è solo facoltativa, di fatto la piattaforma contiene dati come la velocità di lettura e le accuratezze di lettura e scrittura, dai quali si può inferire una condizione di disturbo (Disturbi Specifici dell'Apprendimento, Disturbi del Linguaggio o altro).

2.4.2 i dati personali, afferenti ad un interessato, già presenti in un esistente data base, verranno assoggettati a nuove o modificate modalità di trattamento?
No, non vi è relazione fra i dati degli interessati già presenti su database esistenti e i dati di RIDInet.

2.4.3 i dati personali, afferenti ad un gran numero di interessati, verranno assoggettati a nuove o significative modifiche delle modalità di trattamento?
No

2.4.4 questa iniziativa di trattamento apporterà nuove o significative modifiche alle modalità di consolidamento, interscambio, riferimenti incrociati, abbinamento di dati personali, provenienti da più sistemi di trattamento ?
No

2.5 Modifiche alle procedure di trattamento dei dati

2.5.1 questo trattamento potrà introdurre nuove modalità e procedure di raccolta dei dati, che non siano sufficientemente trasparenti o siano intrusive?
Come detto prima, il trattamento richiede la raccolta di dati anagrafici e memorizza dati da cui si possono inferire informazioni sulla salute degli utenti. Tutte le procedure sono trasparenti e non intrusive: in particolare, sono richiesti i seguenti consensi a norma GDPR in fase di registrazione: ● ai clinici: ◦ Accettazione contratto di servizio (in allegato) ◦ Accettazione “Esprimo il mio libero consenso al trattamento dei dati personali, così come specificato nella parte informativa, con particolare riferimento alle finalità riportate al punto 2a: accesso al servizio di riabilitazione e potenziamento della lettura, della scrittura, del linguaggio, della comprensione del testo scritto e delle abilità di calcolo, attraverso l'accesso al servizio telematico di riabilitazione a distanza denominato “RIDInet” ◦ Accettazione “Esprimo il mio libero consenso al trattamento dei dati personali, così come specificato nella parte informativa, con riferimento alle finalità riportate al punto 2b: invio di materiali informativi/formativi per facilitare l'utilizzo del servizio e della newsletter informativa di Anastasis con eventuali informazioni di tipo commerciale dedicate agli specialisti del settore“ [FACOLTATIVO] ◦ Accettazione “Dichiarazione del rispetto della normativa in materia di privacy ai sensi del Regolamento UE n.679/2016. Il/la sottoscritto/a

conferma la presa visione della Dichiarazione del rispetto della normativa in materia di privacy“

- alle famiglie:
  - Accettazione contratto di servizio: Confermo di aver letto il Contratto di servizi informatici per l'accesso al servizio di riabilitazione a distanza RIDInet.
  - Accettazione informativa sul trattamento dati e Privacy: Riguardo al trattamento dei tuoi dati personali, puoi consultare l'Informativa ai sensi dell’articolo 13 del regolamento UE 679/2016 Dato atto di aver esaminato l'informativa di cui sopra, il/la sottoscritto/a esprime il suo libero consenso al trattamento dei dati personali, così come specificato nella parte informativa, con particolare riferimento alle finalità riportate al punto 2.
  - Accettazione “Esprimo il mio libero consenso al trattamento dei dati personali, così come specificato nella parte informativa, con particolare riferimento alle finalità riportate al punto 2a: riabilitazione e potenziamento della lettura, della scrittura, del linguaggio, della comprensione del testo scritto e delle abilità di calcolo, attraverso l'accesso al servizio telematico di riabilitazione a distanza denominato “RIDInet”.

2.5.2 questo trattamento potrà introdurre modifiche a sistemi e processi, appoggiati a normative in vigore, che possano avere esiti non chiari o non soddisfacenti ?
No.

2.5.3 questo trattamento potrà introdurre modifiche a sistemi e processi, che modifichino il livello di sicurezza dei dati, in modo da portare ad esiti non chiari o non soddisfacenti?
No.

2.5.4 questo trattamento potrà introdurre nuove o modificate procedure sicure di accesso ai dati o modalità di comunicazione e consultazione, che possano essere non chiare o permissive?
No

2.5.5 questo trattamento introdurrà nuove o modificate modalità di conservazione dei dati, che possano essere non chiare o prolungate oltremodo?
No

2.5.6 questo trattamento modificherà le modalità di messa a disposizione di dati pubblicamente disponibili, in modo tale che i dati diventino più accessibili, in quanto non avveniva in precedenza?
No

2.6 Esenzioni dalla applicazione delle disposizioni del regolamento - art.2

2.6.1 l'attività di trattamento esula dall'ambito delle disposizioni legislative dell'unione europea?
No

2.6.2 L'attività di trattamento è sviluppata dagli Stati membri, e tali attività non ricadono nell'ambito del capitolo 2 del titolo quinto del trattato dell'unione europea?
L'attività di trattamento è sviluppata dagli Stati membri e tali attività ricadono nell'ambito del capitolo 2 del titolo quinto del trattato dell'unione europea

2.6.3 Il trattamento è svolto da una persona fisica esclusivamente per fini personali e familiari? In questo caso è anche consentita la diffusione di dati personali che saranno accessibili solo ad un limitato numero di persone, come i familiari e conoscenti?
In ogni caso i dati personali dell'utente sono accessibili solo ai clinici che l'hanno in carico e ai genitori per l'esercizio a casa.

2.6.4 L'attività di trattamento è svolta da autorità pubbliche al fine di prevenzione, indagine, individuazione e perseguimento di reati o al fine di applicare pene?
No

2.7 Giustificazioni per l'avvio del progetto di trattamento

2.7.1 le giustificazioni per l'avvio del trattamento includono contributi significativi a misure in grado di migliorare il livello della sicurezza pubblica?
No

2.7.2 si prevede di sviluppare una consultazione pubblica?
No

2.7.3 la giustificazione per il nuovo progetto di trattamento dei dati è sufficientemente chiara e sufficientemente pubblicizzata?			
Si			
Sezione 2 completata da:	Tullio Maccarrone	Data:	02/05/2023

Sezione 3 - Esito dell'analisi preliminare dei rischi

3.1 Identificazione preliminare dei rischi

La tabella seguente illustra i principali rischi afferenti alla protezione dei dati, che sono stati identificati in fase di valutazione preliminare

	Descrizione del rischio	Valutazione preliminare di esposizione
Informatici	**Furto di informazioni, accesso non autorizzato ad un sistema informatico, malware**	**2/5**
Privacy	**Furto, perdita, divulgazione di informazioni**	**2/5**
Compliance	**Violazione di leggi o regolamenti**	**2/5**
Naturali	**Alluvioni, uragani, terremoti**	**2/5**
Sociali	**Criminalità, terrorismo**	**1/5**
Finanziari	**Andamento del mercato, variazione delle condizioni praticate da clienti e fornitori**	**1/5**
Competitivi	**Contraffazione, Sabotaggio**	**1/5**
Fisici	**Incidenti sul lavoro, accessi non autorizzati ad aree protette**	**1/5**

3.2 Decisione su come procedere

Come prevede l'articolo 35 del GDPR, si ritiene necessario procedere con la valutazione d'impatto (DPIA) in quanto il trattamento riguarda dati sensibili su larga scala.

Nome di colui che ha assunto la decisione	Tullio Maccarrone
Nome di altri soggetti che hanno condiviso questa decisione	Andrea Frascari, Project Manager, DPO incaricato

Sezione 3 completata da	Tullio Maccarrone	Data	02/05/2023

Sezione 4 - Preparazione per la fase di consultazione ed analisi

4.1 Disposizioni afferenti alla Governance

Questa DPIA verrà gestita come parte del progetto RIDInet. Le seguenti persone fisiche, appartenenti al team di progetto, saranno coinvolte nella prosecuzione dello sviluppo del documento:

Nome	Ruolo e mansione
Tullio Maccarrone	Titolare trattamento dei dati
Andrea Frascari	Project Manager
Vincenzo Carnazzo	Responsabile sistemistico

4.2 Altri soggetti coinvolti, da consultare

Soggetto terzo: la nome/ organizzazione/ ruolo	Quale interesse ha questo soggetto terzo in questo progetto di trattamento ?	Con quali modalità viene sviluppata la consultazione con questo soggetto?
Ing. Massimo di Menna	DPO - Data Protection Officer	Il DPO viene consultato periodicamente nell'arco dell'anno, in merito agli adempimenti a cui deve rispondere per l'incarico che ricopre.

Soggetti interni coinvolti	Quale interesse ha questo soggetto terzo in questo progetto di trattamento ?	Con quali modalità viene sviluppata la consultazione con questo soggetto?
Governance aziendale (CdA e Direzione Operativa), che viene coinvolta quando i temi legali di congruità sono complessi.	Garanzia di congruità con ogni disposizione legislativa applicabile e necessità di conoscere le scelte che vengono fatte in tema di sicurezza e tutela della privacy.	La consultazione avviene nei normali contesti di funzionamento dell'azienda, quando il Titolare del trattamento dati incontra il CdA e la Direzione Operativa.

Sezione 4 completata da	Tullio Maccarrone	Data	02/05/2023

Sezione 5 - Congruità con altre leggi, codici o regolamenti afferenti alla protezione dei dati

5.1 Adempimenti per facilitare l'applicazione dell'art. n. 38 del DGPR

In relazione al provvedimento sopra elencato, è stata effettuata una verifica di conformità, come parte di questa DPIA, secondo quanto illustrato nella appendice A e siamo giunti alla seguente conclusione:

1. mettere a disposizione del DPO le necessarie risorse al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate;
2. non rimuovere o penalizzare il DPO in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
3. garantire che il DPO eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse
4. Il DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
5. Il DPO può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Sezione 5 completata da	Tullio Maccarrone	Data	02/05/2023

Sezione 6 - Contenuti analitici della DPIA

Fare riferimento all'appendice B laddove sono illustrati tutti i rischi identificati e illustrate le opzioni che permettano di mitigare, evitare o mettere sotto controllo questi stessi rischi

6.1 Descrizione analitica delle operazioni di trattamento, con indicazione delle finalità e dei legittimi interessi perseguiti dal Titolare del trattamento dei dati

Le principali operazioni di trattamento riguardano due distinti, seppur correlati, target di utenti: i professionisti della riabilitazione cognitiva per l'età evolutivi e i pazienti (minori di età) presi in carico dagli con il consenso e la partecipazione attiva dei genitori al percorso di teletrattamento riabilitativo.

Per quanto riguarda i professionisti ecco le principali finalità:

a) accesso al servizio di riabilitazione e potenziamento della lettura, della scrittura, del linguaggio, della comprensione del testo scritto e delle abilità di calcolo, attraverso l'accesso al servizio telematico di riabilitazione a distanza denominato "RIDInet, ivi incluso l'eventuale accesso ai dati relativi alla produzione scritta dei testi presenti nell'ambiente "Editor" e "Mappe" e dei titoli dei documenti elaborati dai propri pazienti e inviati alla piattaforma RIDInet attraverso il software compensativo GECO;

b) invio della newsletter informativa di Anastasis ed eventuali informazioni di tipo professionale dedicate agli specialisti del settore e invio di contenuti e materiale informativo, attraverso apposite campagne online.

L'accettazione della finalità b è facoltativa.

Per quanto riguarda i pazienti minori di età presi in carico dal professionista e dal servizio di teletrattamento riabilitativo, ecco le finalità di trattamento dati:

a) riabilitazione e potenziamento della lettura, della scrittura, del linguaggio, della comprensione del testo scritto e delle abilità di calcolo, attraverso l'accesso al servizio telematico di riabilitazione a distanza denominato "RIDInet";

b) ricerca statistica ed epidemiologica, finalizzata al miglioramento delle metodiche e delle tecniche d'intervento nell'ambito dei percorsi di trattamento riabilitativo per i Disturbi Specifici dell'Apprendimento e/o nell'ambito della sfera cognitiva. I dati saranno trattati in forma rigorosamente anonima e in modalità aggregata.

L'accettazione del consenso informato viene dato dai genitori e la finalità b è facoltativa.

Per quanto riguarda gli interessi legittimi del titolare del trattamento dei dati, le suddette finalità sono intrinseche alla natura del servizio tecnologico specializzato, erogato dalla piattaforma RidiNet, che ha come scopo principale quello di mettere a

disposizione strumenti e modelli d'intervento in grado di favorire il benessere scolastico degli pazienti presi in carico.

6.2 Valutazione della necessità e proporzionalità delle operazioni di trattamento, in relazione alle finalità

La necessità e la proporzionalità delle operazioni di trattamento sono connesse alle finalità del servizio e al modello d'intervento proposto per gli interventi di riabilitazione cognitiva in presenza e a distanza. I dati che vengono trattati sono funzionali all'osservazione e alla valutazione del percorso intrapreso dai pazienti da parte dei professionisti che li prendono in carico.

6.3 Valutazione dei rischi afferenti ai diritti e alle libertà degli interessati, incluso il rischio di discriminazione connesso o rinforzato dal trattamento

Il sistema può registrare etichette diagnostiche di bambini con Disturbi Specifici dell'Apprendimento o Bisogni Educativi Speciali. In ogni caso, il trattamento memorizza dati (es: la velocità e l'accuratezza di lettura) attraverso i quali è possibile inferire una o più cadute su competenze o prestazioni.

Anche se gli utenti presenti hanno una diagnosi antecedente all'inizio del trattamento ed i dati presenti nella piattaforma RIDInet non aggiungono niente rispetto alle informazioni sulla persona già in possesso del servizio o del professionista che eroga il trattamento, è necessario valutare il rischio derivante dal furto informatico di tali dati e la loro divulgazione.

Si ritiene che i rischi sui diritti e la libertà della persona siano in tal caso moderati: in virtù di certificazioni (legge n.170/2010 e/o n.104/1992), delle relative misure compensative e dispensative per la scuola e del possibile sostegno scolastico, la condizione di salute degli utenti è infatti generalmente nota. Oltre l'etichetta diagnostica – comunque facoltativa e presente nella minoranza dei casi – il sistema non contiene informazioni di natura anamnestica o personale.

6.4 Descrizione delle misure individuate per mettere sotto controllo i rischi e ridurre al minimo il volume di dati personali da trattare- DPbDefault

Nonostante RIDInet sia stato progettato ed implementato ben prima del GDPR, i concetti di Data Protection By Design e Data Protection By Default sono stati tenuti ben presenti per tutelare i dati sensibili degli utenti e per rispettare gli adempimenti previsti dalle legge 196 (allegato B).

In particolare, sebbene il sistema fornisca supporto ad un trattamento di natura riabilitativa e ne misuri i progressi, non sono presenti in maniera persistente “letture” dei dati che forniscano esplicitamente informazioni sulla conseguente modifica alla situazione di salute dell’utente. Anche i sistemi di monitoraggio si basano su elaborazioni dinamiche: il mero impossessarsi dei dati non darebbe quindi accesso a questa tipologia di informazioni.

I dati anagrafici sono limitati al minimo e non assicurano l’identificazione univoca della persona: non è presente per esempio il codice fiscale, né il luogo di nascita, né la nazionalità.

6.5 Elenco dettagliato delle salvaguardie, delle misure di sicurezza e dei meccanismi adottati per garantire la protezione dati personali, come ad esempio la pseudoanonimizzazione, oppure la criptografia, al fine di dimostrare la congruità con il regolamento, tenendo conto dei diritti e dei legittimi interessi degli interessati ed altre persone coinvolte

Poiché i clinici hanno in carico molti utenti, le interfacce con la “lista utenti” mostrano una forma di semplice pseudonimizzazione dei nomi, in modo che gli utenti non possano identificare eventuali conoscenti.

I dati memorizzati sono partizionati in tabelle relazionali; la comunicazione è protetta da SSL. I server che ospitano i dati sono protetti da firewall e sottoposti a periodici audit sulla sicurezza.

Altro aspetto importante è l’alto livello di trasparenza per quanto riguarda le funzioni e il trattamento di dati personali per consentire all’interessato di controllare il trattamento dei dati. Si consulti la risposta alla domanda 2.5.1. per il dettaglio di questo aspetto.

Le prassi di continuous delivery e continuous improvement, oltre alle frequenti richieste ed analisi di feedback da parte degli utenti che governano il progetto RIDInet fanno sì eventuali criticità in merito alla privacy vengano affrontate e risolte appena se ne percepisce il sentore.

La data protection by design si basa anche su un’attenta valutazione dei dati proposti di default (preimpostati) nell’ambito della configurazione e personalizzazione del servizio: in questo caso, la scelta di RIDInet è quella di ridurre al minimo la quantità dei dati raccolti. Ad esempio, il referente del Centro potrebbe richiedere un monitoraggio sulle attività degli operatori, ma tale opzione di default è disattivata. Ancora più importante, i dati riferiti all’etichetta diagnostica sono facoltativi.

6.6 Indicazione generale dei limiti di tempo per procedere alla cancellazione delle diverse categorie di dati raccolti

I dati personali verranno conservati per tutta la durata dei servizi erogati da Anastasis e per un periodo successivo fino ad almeno 2 anni, per garantire gli adempimenti normativi e amministrativi di legge. Si precisa che i citati dati non sono soggetti ad un trasferimento ad un paese terzo o ad una organizzazione internazionale.

6.7 Illustrazione di quali procedure di data protection by design e data protection by default verranno adottate, in conformità all'articolo 23

Le misure in tema di data protection by design e data protection by default, sono le seguenti:

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.

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 (pseudonomizzazione; 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.

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.

6.8 Elenco dei destinatari o delle categorie di destinatari dei dati personali

I clinici di ogni “centro” possono consultare i dati personali di tutti gli utenti registrati presso quel centro.

6.9 Se applicabile, dare elenco nominativo dei trasferimenti previsti dei dati verso paesi terzi o organizzazioni internazionali

Nessun trasferimento

6.10 Verificare che il trasferimento verso paesi terzi od organizzazioni internazionali rispetti le varie modalità previste, come ad esempio l’inserimento in un elenco di paesi approvati, clausole di salvaguardia, Binding corporate rules o EU-USA privacy shield

Nessun trasferimento

6.11 Valutazione del contesto del trattamento dei dati, presso paesi terzi

Nessun paese terzo

6.12 Eventuale coinvolgimento del DPO

Il DPO aziendale è stato coinvolto nell'analisi dei rischi e nella stesura del presente documento.

Sezione 6 completata da	Tullio Maccarrone	Data	08/05/2023

Sezione 7 - Approvazione della DPIA

7.1 Raccomandazioni

Come evidenziato nello sviluppo del precedente documento, ed in particolare della sezione 3 “Identificazione preliminare dei rischi”, il primo punto emerso è quello di “Rischi Informatici (Furto di informazioni, accesso non autorizzato ad un sistema informatico, malware)” con esposizione comunque relativamente bassa - 2 su 5 – in virtù del scarso interesse economico e politico dei dati contenuti.
Le “opzioni che permettono di evitare o mitigare questo rischio” descritte nell’Allegato B del presente documento permettono di ridurre ulteriormente l’esposizione da 2/5 ad 1/5, e pertanto di considerare questo rischio BASSO.

Le opzioni descritte nell’allegato B riportano ad 1/5 anche le esposizioni degli altri rischi individuati:

- Privacy: Furto, perdita, divulgazione di informazioni
- Naturali: Alluvioni, uragani, terremoti
- Compliance: Violazione di leggi o regolamenti

Si ritiene che seguendo tali raccomandazioni il rischio residuo sia sufficientemente basso da permettere il proseguo del servizio RIDInet.

7.2 Approvazione

Le raccomandazioni al punto 8.1 sono state approvate dal Titolare del trattamento dei dati e dal DPO incaricato. Inoltre, è stata accertata l’adeguatezza delle misure e delle risorse adottate per l’attuazione e il monitoraggio del presente DPIA.

Sezione 7 completata da:	Tullio Maccarrone	Data:	08/05/2023

Sezione 8 - Attivazione del trattamento

8.1 Controlli effettuati prima dell'avvio del trattamento

L'azienda ha operato i seguenti controlli preliminari prima dell'avvio del trattamento dei dati, relativamente al servizio denominato RIDInet:

1) stress test per verificare l'inviolabilità dei server nel quale vengono conservati i dati;

2) verifica delle procedure di backup per il salvataggio e l'integrità dei dati

3) verifica della correttezza e della congruenza delle procedure adottate per la protezione dei dati in relazione a quanto previsto dal regolamento europeo e riportato in questo documento;

4) verifica dell'adeguatezza dei ruoli assunti dalle diverse figure responsabili incaricate dall'azienda per la tutela e la protezione dei dati trattati.

Sezione 8 completata da:	Tullio Maccarrone	Data:	08/05/2023

Appendice A - Lista di controllo della congruità del trattamento previsto con le esigenze di protezione dei dati

	Domanda	Risposta
1.	Che tipologie di dati personali devono essere trattate?	• Dati anagrafici: nome e cognome, data di nascita, genere, email • Dati relativi alla parametrizzazione e agli esiti degli esercizi che il trattamento propone: interpolando da tali dati è teoricamente possibile inferire una condizione di disturbo (Disturbi Specifici dell'Apprendimento o altri Bisogni Educativi Speciali) • Facoltativo: etichetta diagnostica (nessuna diagnosi formale allegata).
2.	Sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?	Il trattamento dei dati è necessario per la personalizzazione degli esercizi e per la configurazione del trattamento.
3.	Se vengono trattati speciali categorie di dati, elencati all'articolo 9 comma 1, sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?	Il trattamento dei dati è finalizzato all'erogazione di un servizio specialistico di riabilitazione cognitiva, ascrivibile alla terapia sanitaria come riportato nel punto h della comma 2 dell'articolo 9. Prima di procedere con il trattamento dei dati è stato raccolto il consenso informato in forma chiara e inequivocabile da parte dei genitori del paziente.
4.	Vi sono aspetti afferenti al rispetto dell'articolo 1, comma 2, del regolamento, che protegge i diritti fondamentali e le libertà delle persone fisiche, ed in particolare il loro diritto alla protezione dei dati personali, che non siano trattati in questa DPIA?	No, in questo DPIA sono trattati e illustrati tutti gli aspetti che si riferiscono alla protezione dei dati personali degli utenti (professionisti e pazienti) che usufruiscono del servizio di teletrattamento riabilitativo RIDInet.
5.	Tutti i dati personali che verranno trattati sono coperti da garanzie di riservatezza? Se sì, come questa riservatezza viene garantita?	Si, tutti i dati personali sono coperti da garanzie di sicurezza. In particolare, fare riferimento a quanto esplicitato nelle sezioni 1.2 e 6.7
6.	Come viene offerta agli interessati l'informativa in merito al fatto che i loro dati personali verranno raccolti e trattati?	In fase di registrazione alla piattaforma (si veda il dettaglio del punto 2.5.1. Nella stessa fase di registrazione, gli utenti sono tenuti a scaricare i documenti di riferimento.
7.	Il progetto di trattamento dei dati comporta l'utilizzo di dati personali già	No

	raccolti, che verranno utilizzati per nuove finalità?	
8.	Quali procedure vengono adottate per verificare che le procedure di raccolta dei dati sono adeguate, coerenti e non eccessive, in relazione alle finalità per i quali i dati vengono trattati?	Tutta la strumentazione e le procedure per la raccolta dei dati personali sono state allestite da una società di consulenza specializzate sulla privacy. Le suddette procedure sono state validate dal Titolare del trattamento dei dati e dal DPO incaricato. Infine, nel corso dell'anno vengono effettuati dei monitoraggi delle procedure da parte della società di consulenza.
9.	Con quali modalità viene verificata la accuratezza dei dati personali raccolti e trattati?	I dati personali sono inseriti dai clinici (psicologi, logopedisti, neuropsichiatri infantili) che hanno in carico gli utenti. La correttezza delle informazioni inserite è lasciata alla loro deontologia professionale.
10.	È stato effettuato una valutazione circa il fatto che il trattamento dei dati personali raccolti potrebbe causare danno o stress agli interessati coinvolti?	La piattaforma RIDInet non contiene dati altri rispetto a quelli che i clinici gli utenti già conservano sugli utenti che hanno in carico. In particolare, il dato principale in questione è l'etichetta diagnostica (es: Dislessia) la cui comunicazione all'utente avviene precedentemente all'inizio del trattamento con RIDInet.
11.	È stato stabilito un periodo massimo di conservazione dei dati?	I dati personali verranno conservati per tutta la durata dei servizi erogati da Anastasis e per un periodo successivo fino ad almeno 2 anni, per garantire gli adempimenti normativi e amministrativi di legge.
12.	Quali misure tecniche e organizzative di sicurezza sono state adottate per prevenire qualsivoglia trattamento di dati personali non autorizzato o illegittimo?	Si veda allegato B.
13.	È previsto il trasferimento di dati personali in un paese non facente parte dell'unione europea? Se sì, quali provvedimenti sono stati adottati per garantire che i dati siano salvaguardati in modo appropriato?	No

Appendice B - Tabella dei rischi afferenti alla DPIA

Descrizione del rischio	Rischi inerenti alla protezione dei dati			Opzioni che permettono di evitare o mitigare questo rischio	Rischi residui		
	Impatto	Probabilità	Esposizione		Impatto	Probabilità	Esposizione
Rischi Informatici (Furto di informazioni, accesso non autorizzato ad un sistema informatico, malware)	Potrebbero venire divulgate informazioni sensibili su alto numero di utenti	**Bassa**	**3/5**	RIDInet è ospitato da Hetzner, uno dei principali fornitori di datacenter in Europa, di cui riportiamo estratti salienti dal loro sito relativi alla sicurezza (traduzione dall'inglese nostra): “Un perimetro video-sorvegliato e ad alta sicurezza intorno all'intero datacenter, nonché sistemi di controllo degli accessi garantiscono il più alto livello di sicurezza. Gestiamo tutti i nostro datacenter in conformità con le rigide normative europee sulla protezione dei dati.” I server sono gestiti direttamente da Anastasis ed implementano le seguenti caratteristiche di sicurezza: protetto da firewall ssh consentita ai soli operatori Anastasis censiti del DPS e solo tramite chiavi audit sicurezza periodici da parte di consulenti esterni specializzati aggiornamento continuo del software (sistema operativo, web server, application server, database etc. le comunicazioni sono tutte tramite protocollo HTTPS e quindi criptate. il sistema di autenticazione alla piattaforma prevede un controllo tramite username e password. Le password sono cifrate, hanno scadenza a 3 mesi e non può essere inserita due volte la stessa password.	**“”**	**Bassa**	**1/5**

Privacy (Furto, perdita, divulgazione di informazioni)	**Interruzione dei trattamenti in corso e perdita del monitoraggio degli stessi**	**Bassa**	**2/5**	Il rischio in questione è relativo ai soli dati digitali presenti sui server, in quanto il servizio non contempla dati cartacei o di altra natura. Per quanto riguarda i **furti** digitali valgono quindi le opzioni definite nel punto precedente. Per quanto riguarda la **perdita** dei dati, il rischio è quello di possibili rotture dell'infrastruttura. A tale proposito: ● L'infrastruttura di rete è completamente ridondata, con percorsi rame e fibra sempre separati e compartimentati e la massima tutela da eventi accidentali. Un sistema di alimentazione a norme EIE-CE e completamente ridondante su doppia linea per ogni fila di armadi con prese e spine di sicurezza antistrappo e antifuoco. ● Ogni armadio del datacenter riceve l'alimentazione da due diverse linee provenienti da UPS ridondati. I gruppi elettrogeni ad avvio automatico sono a lunga autonomia con possibilità di rifornimento rapido a piano strada. ● Viene effettuato backup giornalieri di tutti i dati: i backup vengono spostati in altro luogo ● Viene eseguito un regolare programma di "prove ripristino" dei dati di backup per verificare la congruenza dei dati e l'efficienza delle procedure di ripristino stesse	**“”**	**Bassa**	**1/5**
Compliance (Violazione di leggi o regolamenti)	**Necessità di interruzione servizio da**	**Bassa**	**2/5**	RIDInet rispetta il GDPR e sono pertanto stati attivati tutti i ruoli e le procedure previste dal regolamento.	**“”**	**Bassa**	**1/5**

	parte di clienti PA, sanzioni			Si aggiunge che poiché parte importante dei clienti sono parte di Pubbliche Amministrazioni, la compliance è costantemente monitorata e validata dai clienti stessi.			
Naturali Alluvioni, uragani, terremoti	**Interruzione dei trattamenti in corso e perdita del monitoraggio degli stessi**	**Bassa**	**2/5**	La gestione del rischio è parzialmente gestita dal fornitore cloud Hetzner, i cui termini di servizio garantiscono una disponibilità di rete dei loro data center del 99,9% A ciò si aggiunge il disaster recovery plan di Anastasis: I dati degli utenti sono conservati tramite backup. Anche in caso di perdita dei backup, i dati di accesso degli utenti si possono ricostruire dagli ordini e dai dati contabili in possesso di Anastasis. Il sistema di continuous delivery permette di ricreare il servizio da zero anche in caso di catastrofe.	**“”**	**Bassa**	**1/5**

Appendice C - allegato B della legge 196

Il presente documento descrive i servizi in oggetto in riferimento al “disciplinare tecnico in materia di misure minime di sicurezza ”, allegato B della legge 196.

Applicazione e Server

RidiNet è un'applicazione web based ospitata in un sistema ad architettura Cloud server ridondante multiprocessore multicore con connettività a banda illimitata, max 100MB/sec.
Il server è virtualizzato all'interno di un cluster: un eventuale crash di una macchina fisica non sarà percepito dall'utente finale in quanto tutto il sistema è replicato su un cluster di più macchine fisiche.

Backup del database e degli allegati

Indipendentemente dal clustering, ogni notte viene effettuato in automatico un backup del database consistente nel suo dump in formato SQL, compresso con compressione gzip: ad ogni backup viene creato un file nuovo, in maniera tale da rendere possibile il reperimento di dati vecchi, o il ripristino della situazione ad una determinata data. Tali backup vengono mantenuti per un mese: superato il quale, viene mantenuto solo il backup relativo al primo giorno di ogni mese.

Sicurezza del Server

Il server che ospita l'applicazione ha aperte dall'esterno verso l'interno esclusivamente le seguenti porte:

- 22 per le comunicazioni SSH
- 80 per le comunicazioni HTTP
- 443 per le comunicazioni HTTPS

Il filtraggio dei pacchetti IP è affidato ad un firewall esterno.

Sistema di log

I log dell'applicazione sono salvati su file all'interno del database. I log di errori gravi vengono inviati automaticamente alle persone incaricate.
Per mantenere validi i log di accesso, l'orologio del server è mantenuto sincronizzato tramite timesyncd.

A ulteriore protezione:

- Il monitoraggio sulla capacità e il funzionamento del server e dell'applicazione avviene in automatico ogni 5 minuti tramite CheckMk. Eventuali anomalie vengono segnalate immediatamente alle persone incaricate.
- Il server web è configurato con un blocco contro gli attacchi DOS;
- Il server web e il servlet container sono configurati per permettere l'accesso diretto solo alle servlet del programma e ai file relativi alla grafica dello stesso (GIF, CSS e simili). Ogni altro tipo di accesso (in particolare l'accesso a ogni tipo di allegato) è sempre filtrato dal gestore dei permessi dell'applicazione.

L'accesso SSH è consentito solo a tre account (nessuno dei quali è root) con password ad alta sicurezza.

Conformità alla legge 196

Ad ogni operatore è richiesta una credenziale di autenticazione tramite inserimento di username e password: la parola chiave deve essere composta obbligatoriamente da almeno otto caratteri e deve contenere almeno una lettera ed un numero. Tale parola chiave è impostata direttamente dall'operatore e deve essere aggiornata dallo stesso con cadenza trimestrale: il sistema stesso impone il cambio della password ogni 3 mesi, e non permette la registrazione della stessa password. Solo l'operatore conosce la propria password e neanche l'amministratore di sistema è in grado di poterla ricavare: sarà responsabilità dell'operatore stesso mantenere la segretezza sulla propria password. Credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, ad eccezione di quelle preventivamente autorizzate per soli scopi di gestione tecnica.
I dati personali idonei a rivelare lo stato di salute e la vita sessuale sono separati dagli altri dati personali del paziente essendo allocati in diverse tabelle di un database relazionale.
Dal punto di vista tecnico, avranno possibilità di accesso ai dati per motivi di gestione e manutenzione i soli dipendenti Anastasis autorizzati dal cliente tramite compilazione e firma del modulo preposto fornito dal cliente stesso. In attesa, o in assenza di tale modulo, si notifica che le persone incaricate sono:

- Andrea Frascari, nato a Bologna il 23/0/1970, CF FRSNDR70P23A944M
- Vincenzo Carnazzo, nato a Milazzo il 2/9/1980, CF CRNVCN80P02F206D
- Enzo Ferrari, nato a Bologna il 30/09/1971, CF FRRNZE71P30A944H

Tale personale è formato a aggiornato sulle tematiche della sicurezza e riservatezza dei dati.
I server risiedono fisicamente in una web-farm: per ogni accesso ai server, sia fisico che software, il personale della web farm richiede autorizzazione scritta ad Anastasis.
Server, relativi strumenti anti-intrusione e applicazione sono aggiornati con cadenza almeno semestrale. Il salvataggio dei dati avviene su base giornaliera.
Il sistema prevede la possibilità di creare diversi profili di autorizzazione per l'accesso ai dati. Tali profili riguardano ciascun incaricato o classi omogenee di incaricati e sono individuati e configurati anteriormente all'attività operativa, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni previste. In particolare, l'operatore è riconosciuto ed abilitato a determinate operazioni su determinati dati in base ai gruppi a cui appartiene, e, indirettamente, in base ai profili associati a questi gruppi, che determinano i permessi.
In particolare ogni gruppo di operatori avrà accesso unicamente ai dati degli utenti da loro stessi inseriti ovvero agli utenti inseriti da operatori appartenenti allo stesso gruppo. Non sarà possibile in alcun modo avere accesso ad altri dati.
In aggiunta alla conformità alla legge 196, il sistema è stato progettato con criteri di robustezza rispetto ai principali tipi di attacchi web (SQL injection, cross-site scripting, command injection etc.).

Data Center in cui risiedono i dati di RIDInet

I data center su cui risiedono i dati di RIDInet sono collocati esclusivamente nei Paesi che appartengono all'Unione Europea, nello specifico:

- RIDInet è ospitato presso il datacenter di Falkenstein (Germania) gestito da Hetzner.
- I backup sono ospitati presso il datacenter di Helsinki (Finlandia) gestito da Hetzner.

Hetzner ha ricevuto la certificazione ISO 27001. Maggiori informazioni:
https://docs.hetzner.com/general/others/certificates/

Riferimenti per il Data Privacy Framework relativo ai servizi Hetzner:
https://www.hetzner.com/legal/privacy-policy