VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

NOME DEL PROGETTO:	**TeleFE**
DESCRIZIONE DEL PROGETTO:	**TeleFE è una piattaforma web per la tele-valutazione multidimensionale delle Funzioni Esecutive (FE) in età evolutiva.**

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

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 una valutazione d'impatto ex art. 33. 2a Reg. UE;

· 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 valutazione d'impatto.

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

Data di avvio della DPIA:	29/03/2023

Sezione 1 - Avvio della valutazione

1.1 Traccia del progetto

TeleFE è una piattaforma web per che funziona in modalità SaaS (Software as a Service) e che offre la possibilità di effettuare la valutazione integrata delle FE (Funzioni Esecutive) su tre dimensioni:

- valutazione delle FE di base
- valutazione delle FE complesse
- valutazione del comportamento esecutivo

Si tratta di una batteria di televalutazione delle FE, fruibile tramite browser sia in presenza che a distanza, standardizzata su ragazze e ragazzi dai 6 ai 13 anni.
E' composta da 5 test, suddivisi in 15 subtest per un tempo totale di circa 1 ora, che il clinico può decidere di includere selettivamente:

- QUFE - Questionario sulle Funzioni Esecutive per famiglia ed insegnanti
- Flanker - Controllo interferenza e flessibilità cognitiva
- Go/NoGo - Inibizione
- N.back - Memoria di lavoro ad alto e basso carico
- TPQ - Abilità di pianificazione quotidiana

Il servizio è inteso come supporto agli specialisti della clinica che operano nel campo della valutazione e osservazione cognitiva dei soggetti in età evolutiva e cioè:

- Psicologi iscritti all'albo regionale di riferimento operanti in Aziende sanitarie pubbliche e in convenzione o in Centri clinici privati

Pertanto gli account creati per l'accesso alla piattaforma possono essere utilizzati esclusivamente dai suddetti soggetti.
Ogni utente può accedere esclusivamente ai dati di propria pertinenza.

1.2 Valutazione preliminare dell'utilizzo dei dati.

I dati inseriti dagli operatori o raccolti tramite i test sono salvati all'interno dei server gestiti da Anastasis.
Gli operatori potranno accedere ai dati in sola lettura anche dopo aver esaurito i crediti acquistati o ricevuti come demo, per 2 anni dal consumo dell'ultimo credito.

1.2.3 Chi avrà accesso ai dati?

I tecnici Anastasis dichiarati nell'allegato C 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 dati personali non vengono in nessun modo trasferiti a soggetti terzi.

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

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

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.

I dati personali: Nome, Cognome e indirizzo mail, 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;
- Operatori
    - Gli specialisti che operano all'interno di strutture sanitarie pubbliche, private o in convenzione;
    - I professionisti che accedono alla piattaforma in modalità demo;
    - I professionisti che acquistano autonomamente l'accesso alla piattaforma, sottoscrivendo uno o più pacchetti di somministrazione delle prove di valutazione

Sezione 1 completata da:	Tullio Maccarrone	Data:	03/04/2023

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?

No.

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 dell'interessato?

Il servizio, oltre a richiedere la memorizzazione di dati anagrafici dei professionisti (nome, cognome, indirizzo mail), registra alcuni dati relativi ai pazienti che vengono presi in carico dallo specialista per la somministrazione delle prove di valutazione funzionali alla definizione del profilo di funzionamento per ciò che si riferisce alle Funzioni Esecutive. Ecco qui di seguito i principali dati personali relativi ai pazienti: dati anagrafici, livello scolastico frequentato, tipo di sviluppo (atipico o non atipico), eventuale codice diagnostici ICD10, prima lingua parlata ed eventuale bilinguismo. Il professionista inoltre potrà inserire in un campo libero note libere: Anastasis invita a non inserire dati sensibili nelle note ma la responsabilità ultima è del professionista. Infine, può essere richiesto l’indirizzo mail della famiglia e dell’insegnante del paziente, a cui sottoporre la compilazione di un questionario online.

2.4.2 I dati personali, afferenti ad un interessato, già presenti in un esistente database, verranno assoggettati a nuove o modificate modalità di trattamento?

No, non vi sono relazioni fra i dati degli interessati già presenti su database esistenti e i dati di TeleFE.

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?

L'utilizzo di TeleFE richiede la raccolta di dati anagrafici 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 professionisti:
    - Accettazione di aver preso visione della Privacy policy di TeleFE e consenso al trattamento dei dati personali, come specificato nell'apposita policy.
    - Accettazione dell'apposito contratto di servizio.
    - Accettazione dei termini riportati nel documento Data Processing Agreement TeleFe.
- Ai responsabili dei centri clinici e/o privati:
    - Accettazione di aver preso visione della Privacy policy di TeleFE e consenso al trattamento dei dati personali, come specificato nell'apposita policy.
    - Accettazione dell'apposito contratto di servizio.
    - Accettazione dei termini riportati nel documento Data Processing Agreement TeleFe.

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 del paziente sono accessibili solo al professionista che ha effettuato la valutazione o, nel caso delle strutture sanitarie, da parte degli specialisti che compongono l'equipe multidisciplinare e che sono stati autorizzati al trattamento dei dati.

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?

Sì.

Sezione 2 completata da:	Tullio Maccarrone	Data:	0304/2023

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, reati informatici (es. 617 septies c.p)	3/5
Privacy	Furto, perdita, divulgazione di informazioni, accesso non autorizzato	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

Legenda valutazione analisi impatto dei rischi

1 - Molto Basso	2 - Basso	3 - Moderato	4 - Alto	5 - Molto Alto

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:	Vincenzo Carnazzo, responsabile sistemistico, Massimo Di Menna (DPO)

Sezione 3 completata da:	Tullio Maccarrone	Data:	03/04/2023

Sezione 4 - Preparazione per la fase di consultazione ed analisi

4.1 Disposizioni afferenti alla Governance

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

Nome	**Ruolo e mansione**
Tullio Maccarrone	Titolare del trattamento dei dati
Vincenzo Carnazzo	Responsabile sistemistico

4.2 Altri soggetti coinvolti, da consultare

Con quali modalità viene sviluppata la consultazione con questo soggetto?	**Con quali modalità viene sviluppata la consultazione con questo soggetto?**	**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:	03/04/2023

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 GDPR

In relazione al provvedimento sopra elencato, è stata effettuata una verifica di conformità, come parte di questa DPIA, secondo quanto illustrato nell'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:	03/04/2023

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 operazioni di trattamento riguardano psicologi e personale sanitario.
Il trattamento dei dati ha le seguenti finalità:

A. Accesso al servizio di televalutazione per la somministrazione di una batteria di prove specialistiche finalizzate a valutare impulsività, memoria di lavoro e flessibilità cognitiva.

Per quanto riguarda gli interessi legittimi del titolare del trattamento dei dati, le suddette finalità sono intrinseche alla natura del servizio tecnologico specializzato erogato.

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. I dati che vengono trattati sono funzionali al corretto funzionamento del servizio. Ogni utente potrà accedere solo ai dati di cui ha diritto: esito dei singoli test somministrati, accesso al profilo di funzionamento sulla base degli esiti della somministrazione dei test.

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

TeleFE, pur essendo un sistema funzionale alla valutazione delle Funzioni Esecutive, non definisce e non elabora alcuna etichetta diagnostica relativamente ai pazienti che vengono sottoposti all'osservazione. In ogni caso, il trattamento registra alcuni dati (es: prestazione sulle diverse funzioni esecutive) attraverso i quali è possibile inferire una o più cadute su competenze o prestazioni.
Anche se per i pazienti presenti, i cui dati presenti nella piattaforma TeleFE non aggiungono niente rispetto alle informazioni sulla persona già in possesso del servizio o del professionista che svolge la valutazione, è necessario valutare il rischio derivante dal furto informatico di tali dati e la loro divulgazione.

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

La piattaforma TeleFE è stata sviluppata seguendo i concetti di Data Protection By Design e Data Protection By Default per rispettare gli adempimenti previsti dalla legge 196 (allegato B).
I dati gestiti da TeleFE in ogni caso riguardano solo la sfera cognitiva, ma non la salute, la religione o l'orientamento sessuale.
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 crittografia, al fine di dimostrare la congruità con il regolamento, tenendo conto dei diritti e dei legittimi interessi degli interessati ed altre persone coinvolte

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 TeleFE fanno sì che eventuali criticità in merito alla privacy vengano affrontate e risolte appena se ne percepisce il sentore.
Inoltre, in base alla Data Protection by Default, la scelta di TeleFE è quella di ridurre al minimo la quantità dei dati raccolti, evitando ogni dato potenzialmente sensibile o discriminatorio.

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 utenti di TeleFE, la durata del trattamento dei dati personali è stata minimizzata ad un periodo di 2 anni successivo alla cessazione del servizio stesso. Il servizio di cui parliamo viene fruito in modalità di uso di pacchetti di prove di valutazione a consumo. Anche nel caso in cui le prove a disposizione per la valutazione siano esaurite, per altri 2 anni, l'utente può comunque accedere in sola lettura delle valutazioni da esso create.

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 sono ridotti al minimo: nominativo, indirizzo email, data di nascita, sesso, classe frequentata, prima lingua parlata e status (S/N) sul tipo di sviluppo (atipico o non atipico) ed eventuali codici ICD10.

Minimizzazione negli accessi ai dati (5.1.f – 25.2)
La quantità di dati raccolta è esclusivamente funzionale alle esigenze del servizio. La base dei dati si incrementa esclusivamente sulla base dell'accesso dell'utente.

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'utente legge ed eventualmente sottoscrive prima dell'accesso a TeleFe. 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'utente legge ed eventualmente sottoscrive prima dell'accesso a TeleFE. 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'utente legge ed eventualmente sottoscrive prima dell'accesso a TeleFE, 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 TeleFE da parte degli utenti è inviato a terzi, in nessuna forma (in chiaro, sotto pseudonimo o in forma anonima).

Cifratura dei dati (art. 34.3.a)

Le comunicazioni tra il dispositivo dell'utente (browser su computer o app su dispositivo mobile) avvengono tutti con protocollo HTTPS e sono quindi cifrati.

Integrità del servizio

Il server che ospita TeleFE 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 TeleFE. Il backup viene conservato in duplice copia in due server esterni al servizio TeleFE. 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 TeleFE.

Profilazione degli utenti: autenticazione ed autorizzazioni

l sistema prevede due diversi profili di accesso:

- Professionista. Può accedere tramite autenticazione. Può visionare, inserire, modificare ed eliminare i dati relativi agli utenti gestiti da lui e a quelli del centro a cui è afferente. Non può in alcun modo accedere a dati di utenti di altri professionisti e di altri centri.
- Genitore/Insegnante. Può accedere tramite link diretto ricevuto via email, senza autenticazione, ma l'unica attività che possono svolgere è compilare un questionario. Non possono accedere ai dati.
- Operatore Anastasis di primo livello. Possono accedere alla configurazione degli accessi (compresi gli account, i centri e i crediti) con il fine di risolvere assistenze tecniche. Non possono fare operazioni di tipo distruttivo sui dati o sugli abbonamenti.
  Gli operatori Anastasis di primo livello, sono stati autorizzati ad operare con apposito incarico prescrittivo.
- Operatore Anastasis di secondo livello. Oltre alle autorizzazioni degli operatori Anastasis di primo livello, possono accedere direttamente ai dati nel database degli utenti, al fine di risolvere problemi tecnici.
  Gli operatori Anastasis di secondo livello, sono stati autorizzati ad operare con apposito incarico prescrittivo.

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

Gli operatori possono accedere solo ai propri dati personali.
Gli operatori Anastasis autorizzati possono accedere inoltre ai dati degli abbonamenti degli utenti.

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:	03/04/2023

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 “Furto di informazioni, accesso non autorizzato ad un sistema informatico, malware, reati informatici (es. 617 septies c.p)
con esposizione comunque moderata - 3 su 5 – in virtù dello 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 3/5 ad 2/5, 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 prosieguo del servizio TeleFE.

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:	03/04/2023

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 TeleFE:

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:	03/04/2023

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 del paziente: nome, cognome, e-mail, sesso, status sviluppo evolutivo (tipico o atipico), icd10
2.	Sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?	Il trattamento dei dati è necessario per l'erogazione di TeleFE, una piattaforma web per la tele-valutazione multidimensionale delle Funzioni Esecutive (FE) in età evolutiva.
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?	Prima di procedere con il trattamento dei dati è stato raccolto il consenso informato in forma chiara e inequivocabile da parte dei professionisti.
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 dei professionisti che usufruiscono del servizio TeleFE.
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?	Per i professionisti, 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. Per genitori e insegnanti (per i quali non è prevista registrazione), nella schermata iniziale che precede la compilazione dei questionari. Gli stessi documenti sono scaricabili anche successivamente attraverso un'apposita pagina dell'applicazione web.

7.	Il progetto di trattamento dei dati comporta l'utilizzo di dati personali già raccolti, che verranno utilizzati per nuove finalità?	No.
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 professionisti che hanno in carico gli utenti. La correttezza delle informazioni inserite è lasciata alla loro deontologia professionale.
10.	È stata effettuata una valutazione circa il fatto che il trattamento dei dati personali raccolti potrebbe causare danno o stress agli interessati coinvolti?	TeleFE è uno strumento di valutazione sulle Funzioni Esecutive che non può essere ascritta ad alcuna forma di etichetta diagnostica: le informazioni generate riguardano un profilo di funzionamento cognitivo che arricchisce informazioni già detenute dal professionista.
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
Reati informatici (furto di informazioni, accesso non autorizzato ad un sistema informatico, malware, reati informatici, es. 617 septies c.p)	Potrebbero venire persi e/o divulgati dati personali degli utenti (nominativo ed email: nessuna password)	Moderata	3/5	TeleFE 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.		Bassa	2/5

				• 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.			
Privacy (divulgazione di informazioni)	Potrebbe venire divulgati i dati di accesso degli utenti	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 si veda il punto relativo ai rischi naturali:		Molto bassa	1/5
Compliance (Violazione di leggi o regolamenti)	Interruzione del servizio e perdita dei dati di accesso.	Bassa	2/5	TeleFE rispetta il GDPR e sono pertanto stati attivati tutti i ruoli e le procedure previste dal regolamento. Si aggiunge che poiché parte importante dei clienti sono parte di Pubbliche Amministrazioni, la compliance è costantemente monitorata e validata dai clienti stessi. Per quanto riguarda l'interruzione del servizio si veda il punto relativo ai rischi naturali. Per quanto riguarda la perdita dei dati di accesso si veda il punto relativo ai rischi relativi alla privacy.		Molto bassa	1/5

	Errori in fase di aggiornamento e manutenzione dell'app			Il malfunzionamento del software, che può essere determinato da errori dell'operatore o da cause tecnologiche, può comportare disservizi (ritardi nell'erogazione del servizio) ed errori. Inoltre, può esporre il sistema alla perdita di disponibilità e/o di integrità dei dati elaborati. Modifica o cancellazione dati per errore umano o di programma. Anastasis adotta un protocollo di controlli finalizzati a ridurre fortemente i rischi di cui sopra.			
Naturali (alluvioni, uragani, terremoti)		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.		Molto bassa	1/5

ALLEGATO B

Bologna, 3 aprile 2023

Il presente documento integra e approfondisce informazioni sulla sicurezza dei server e sul personale tecnico autorizzato all'accesso.

Applicazione e Server

TeleFE è un'applicazione web based SaaS ospitata in un sistema ad architettura cloud server ridondante multiprocessore multicore fornito da Hetzner.

Backup del database e degli allegati

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 interno.

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.

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.
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 un datacenter: per ogni accesso ai server, sia fisico che software, il personale del datacenter richiede autorizzazione scritta ad Anastasis.
Server, relativi strumenti anti-intrusione e applicazione sono aggiornati con cadenza almeno semestrale. Il backup 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 TeleFE

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

- TeleFE 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