VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

NOME DEL PROGETTO:	**SuperMappeX EDU**
DESCRIZIONE DEL PROGETTO:	**Servizio online per creare mappe multimediali per una didattica inclusiva e collaborativa.**

Responsabile elaborazione DPIA:	Tullio Maccarrone	Posizione:	Soggetto designato ex art. 29 del GDPR al trattamento dei dati con funzione specifica e delega per la gestione e l'applicazione del Regolamento UE 779/2016: con apposita delibera del CdA Anastasis in data 10/07/2023

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 dell'aggiornamento della DPIA:	20/02/2024

Sezione 1 - Avvio della valutazione

1.1 Traccia del progetto

SuperMappeX EDU è un servizio online composto da un'app web, da un'app Android e da un'app iOS.
Le tre app hanno funzionalità simili e permettono, nei vari ambienti, di aprire e modificare mappe multimediali. Per mappa qui si intende la rappresentazione grafica di relazioni tra più concetti.
SuperMappeX EDU è una piattaforma web che funziona in modalità SaaS (Software as a Service) e che offre la possibilità di creare mappe multimediali in classe e a casa, per una didattica inclusiva e collaborativa. Il servizio è inteso come supporto alla didattica e ai servizi correlati con le attività scolastiche e/o educative in generale: pertanto gli account creati in tale contesto devono essere utilizzati esclusivamente per tali fini.
L'accesso alla piattaforma: Il servizio può essere acquistato in abbonamento annuale da singoli privati, da gruppi di utenti (ad esempio classi scolastiche) o da intere scuole.
Ogni utente può visualizzare le proprie mappe oppure mappe che altri utenti hanno reso pubbliche o che hanno condiviso specificatamente con lui.

1.2 Valutazione preliminare dell'utilizzo dei dati.

Le mappe create attraverso SuperMappeX EDU vengono salvate sul Google Drive dell'utente, il quale ne ha la disponibilità anche dopo l'eventuale cessazione del servizio.
Alcuni dati di base dell'utente vengono salvati su Cloud SQL di Google Cloud al solo fine di permettere il funzionamento e la fruizione del servizio.
Durante l'uso di SuperMappeX EDU le mappe aperte vengono salvate su Cloud Storage di Google Cloud per permetterne la fruizione in tempo reale.

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?

SuperMappeX EDU è ospitata dalla piattaforma Google Cloud.
Anastasis e SuperMappeX EDU non eseguono backup in quanto le mappe create dall'utente vengono salvate sul suo personale Google Drive.
Viene invece fatto un backup ogni notte delle informazioni salvate su database. Il backup è conservato su un Cloud Storage di Google Cloud separato da quello usato dall'applicazione.

I dati personali: Nome, Cognome e indirizzo email dell'account Google, 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;
- I dipendenti (presidi, personale di segreteria, animatori digitali, insegnanti) e gli studenti della scuola che acquista un abbonamento al servizio;
- I privati che si registrano alla piattaforma nella modalità "demo gratuita per un mese".

Sezione 1 completata da:	Tullio Maccarrone	Data:	20/02/2024

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 richiede la memorizzazione di dati anagrafici degli utenti su Google Cloud.
L'utente nelle mappe può inserire ogni tipo di contenuto: immagini, documenti, informazioni che possano essere definibili in maniera implicita od esplicita Dati Particolari ex art. 9, co.1. Reg UE. Il contenuto delle mappe è comunque responsabilità dell'utente creatore e le mappe vengono salvate nel suo Google Drive e rimangono di sua proprietà. Nel contratto di servizio, nell'art. 4, le responsabilità dell'utente vengono opportunamente dettagliate in particolar modo di deve astenere da: creare, caricare o condividere mappe concettuali e/o materiale che possa violare il diritto d'autore, la normativa Privacy, presentare forme o contenuti di carattere osceno, diffamatorio che possano arrecare danno o lesione di diritti e dignità delle persone o comunque contrari alla normativa vigente in materia civile, penale ed amministrativa.

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 è relazione fra i dati degli interessati già presenti su database esistenti e i dati di SuperMappeX.

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 SuperMappeX EDU 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:

- Agli amministratori scolastici:
    - Accettazione di aver preso visione della Privacy policy di SuperMappeX EDU 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 SuperMappeX EDU.
- Agli insegnanti e studenti che fanno riferimento alla scuola che ha attivato SuperMappeX EDU e che accedono con il proprio account scolastico:
    - Accettazione di aver preso visione della Privacy policy di SuperMappeX EDU e consenso al trattamento dei dati personali, come specificato nell'apposita policy.
    - Accettazione dell'apposito contratto di servizio.

  Nel caso di utenti minorenni i consensi devono essere dati da chi ha la responsabilità genitoriale.
- Ai soggetti privati che acquistano e/o richiedono la demo a SuperMappeX EDU:
    - Accettazione di aver preso visione della Privacy policy di SuperMappeX EDU e consenso al trattamento dei dati personali, come specificato nell'apposita policy.
    - Accettazione dell'apposito contratto di servizio.
    - Accettazione, facoltativa, della richiesta di iscrizione alla newsletter Anastasis, qualora l'utente sia maggiore di età.

  Nel caso di utenti minorenni i consensi devono essere dati da chi ha la responsabilità genitoriale e l'iscrizione alla newsletter Anastasis non viene affatto proposta.

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?

Il trattamento è svolto da una persona fisica. In particolare le mappe vengono create dal singolo utente e può decidere se condividere le mappe e con chi (altro singolo utente, gruppo di utenti o condivisione pubblica).

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:	20/02/2024

Sezione 3 - Esito dell’analisi preliminare dei rischi

DEFINIZIONI E CRITERI DI VALUTAZIONE DEL RISCHIO ex art. 35, Regolamento EU 679/2016.

Le **fasi** per individuare e ridurre il rischio sono:

1. individuazione della minaccia;
2. individuazione della vulnerabilità;

3. riduzione del rischio;
4. limitazione dell'impatto sugli interessati.

Al fine di fornire un criterio oggettivo da utilizzarsi in fase di Valutazione di Impatto, come descritta ai sensi dell'art. 35 del Regolamento UE 679/2016, si riportano di seguito le seguenti definizioni:

- **Pericolo (fattore di rischio):** proprietà o qualità intrinseca di una determinata circostanza avente il potenziale di causare un danno.
- **Rischio:** probabilità che sia raggiunto il livello potenziale di danno nelle condizioni di esposizione ad una causa, nonché dimensioni possibili del danno stesso.
- **Gravità:** conseguenza negativa derivante dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3.1 Scala delle probabilità

La scala della Probabilità fa riferimento principalmente all'esistenza di una correlazione più o meno diretta tra la carenza riscontrata ed il danno ipotizzato.

Valore	Livello	Definizioni / criteri
4	Altamente probabile	● Esiste una correlazione diretta tra la mancanza ed il verificarsi del danno ipotizzato alla privacy. ● Si sono già verificati danni per la stessa mancanza rilevata nella stessa azienda, in aziende o situazioni simili. ● Il verificarsi del danno non susciterebbe alcuno stupore in azienda.
3	Probabile	● La mancanza rilevata può provocare un danno anche se non in modo automatico o diretto; ● È noto qualche episodio in cui alla mancanza ha fatto seguito il danno; ● Il verificarsi del danno susciterebbe una moderata sorpresa in azienda.
2	Poco probabile	● La mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi; ● Sono noti solo rarissimi episodi già verificatisi; ● Il verificarsi del danno susciterebbe grande sorpresa.
1	Improbabile	● La mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili indipendenti; ● Non sono noti episodi già verificatisi; ● Il verificarsi del danno susciterebbe incredulità.

3.2. Scala dell'entità della gravità

La scala di Gravità del danno fa, invece, principalmente riferimento al grado di lesività della circostanza dannosa sul diritto alla privacy dei soggetti interessati e alla reversibilità o meno del danno.

Valore	Livello	Definizioni / criteri
4	Gravissimo	• Episodio dannoso con effetti sul diritto alla privacy irreversibili; • Esposizione dell'azienda a gravissime conseguenze sanzionatorie.
3	Grave	• Episodio dannoso con effetti sul diritto alla privacy difficilmente reversibili; • Esposizione dell'azienda a gravi conseguenze sanzionatorie.
2	Medio	• Episodio dannoso con effetti sul diritto alla privacy reversibili; • Esposizione dell'azienda a conseguenze sanzionatorie di media entità.
1	Lieve	• Episodio dannoso con effetti sul diritto alla privacy facilmente reversibili; • Esposizione dell'azienda a conseguenze sanzionatorie di lieve entità.

3.3. Matrice di valutazione del rischio

Definita la gravità e la probabilità, il rischio viene automaticamente graduato mediante la formula R = P x G e si può rappresentare nella seguente forma grafica:

Matrice del Rischio R=PxG			
4	**8**	**12**	**16**
3	**6**	**9**	**12**
2	**4**	**6**	**8**
1	**2**	**3**	**4**

Livello	Lieve	Medio	Grave	Gravissimo
Valore	1-3	4-6	7-12	13-16

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 impatto dei rischi
Informatici	Furto di informazioni, accesso non autorizzato ad un sistema informatico, malware, reati	2/4 (Medio)

	informatici (es. 617 septies c.p)	
Privacy	Furto, perdita, divulgazione di informazioni, accesso non autorizzato	2/4 (Medio)
Compliance	Violazione di leggi o regolamenti	2/4 (Medio)
Naturali	Alluvioni, uragani, terremoti	2/4 (Medio)

Legenda valutazione analisi impatto dei rischi

1 - Lieve	2 - Medio	3 - Grave	4 - Gravissimo

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:	20/02/2024

Sezione 4 - Preparazione per la fase di consultazione ed analisi

4.1 Disposizioni afferenti alla Governance

Questa DPIA verrà gestita come parte del progetto SuperMappe X EDU. 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 Generale.

Sezione 4 completata da:	Tullio Maccarrone	Data:	20/02/2024

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:	20/02/2024

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 personale scolastico, operatori di doposcuola, studenti (anche minorenni) e in generale privati (anche minorenni).
Le operazioni hanno le seguenti finalità:

A. Accesso al servizio SuperMappeX EDU per visualizzare, creare e modificare mappe dell'utente o mappe che un altro utente ha condiviso con lui.
B. Invio della newsletter informativa di Anastasis ed eventuali invii di contenuti e materiale informativo, attraverso apposite campagne online.

L'accettazione della finalità B è facoltativa.

Nel caso di minori, l'accettazione della finalità A viene data dai genitori, mentre l'accettazione della finalità B non viene proposta e viene considerata automaticamente come non accettata.

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: mappe generate da egli stesso o mappe che qualcuno ha condiviso con lui.

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

Si ritiene che i rischi sui diritti e la libertà della persona siano molto bassi: il servizio non contiene dati che possano discriminare l'interessato e la presenza stessa dell'interessato nel database di SuperMappeX EDU non può portare ad alcuna discriminazione, essendo SuperMappeX EDU un servizio rivolto potenzialmente a chiunque.

6.4 Descrizione delle misure individuate per mettere sotto controllo i rischi e ridurre al https://safety.google/volume di dati personali da trattare

SuperMappeX EDU è stato sviluppato 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 SuperMappeX EDU in ogni caso non contengono dati sensibili riguardo salute, religione o orientamento sessuale.
Non si può escludere che l'utente inserisca dati sensibili nel contenuto stesso delle mappe, di cui comunque da contratto si dichiara responsabile. Al tal riguardo, si riporta il comma b dell’art. 4 del suddetto contratto di servizio, in cui nelle condizioni di utilizzo l’utente si impegna su quanto segue:
a non creare, caricare o condividere mappe concettuali e/o materiale che possa violare il diritto d’autore, la normativa Privacy, presentare forme o contenuti di carattere osceno, diffamatorio che

possano arrecare danno o lesione di diritti e dignità delle persone o comunque contrari alla normativa vigente in materia civile, penale ed amministrativa.
Infine, le mappe e il loro contenuto sono salvati all'interno di Google Drive e la loro conservazione è quindi gestita da Google e non da Anastasis. Si veda in proposito privacy.google.com.

6.5 Elenco dettagliato delle salvaguardie, delle misure di sicurezza e dei meccanismi adottati per garantire la protezione dati personali, come ad esempio la pseudonimizzazione, 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

Le comunicazioni di SuperMappeX EDU con i browser, con le sue varie versioni (webapp, Android e iOS) e con i servizi di Google sono protette con SSL.
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 SuperMappeX EDU 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 SuperMappeX EDU 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 SuperMappeX EDU, la durata del trattamento dei dati personali è stata minimizzata ad un periodo di 2 anni successivo alla cessazione del servizio stesso. Anche allo scadere dell'abbonamento, per altri 2 anni, l'utente può comunque accedere in sola lettura alle mappe da esso create. Qualora all'interno dei 2 anni dovesse rinnovare l'abbonamento, gli è garantita continuità di servizio e pieno accesso alle mappe 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: nome, indirizzo email e (opzionale) profilo professionale.

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 SuperMappeX EDU. 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 SuperMappeX EDU. 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 SuperMappeX EDU, 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 SuperMappeX EDU 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 SuperMappeX EDU da parte degli operatori sono inviati a terzi in forma anonima a Google Analytics.

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
SuperMappeX EDU usa Google Cloud come infrastruttura su cui operare e l'accesso al database è configurato in modo tale che solo gli operatori autorizzati possano accedere.
Il servizio è inoltre monitorato in automatico ed eventuali disservizi sono segnalati automaticamente agli amministratori di sistema Anastasis.

Integrità dei dati
Ogni notte viene eseguito il backup dei dati conservati in SuperMappeX EDU. Il backup viene conservato in un Google Storage separato dal resto dei servizi cloud di Google

Profilazione degli utenti: autenticazione ed autorizzazioni
Il sistema prevede tre diversi profili di accesso, tutti con autenticazione tramite account Google e i seguenti permessi funzionali:

- Studente di una scuola. Può creare mappe e visualizzare o modificare mappe create da lui o con lui condivise. Può inoltre vedere delle statistiche sul proprio utilizzo del servizio (numero di mappe create, numero di condivisioni fatte ecc.).
- Utente privato. Oltre alle autorizzazioni degli studenti può vedere le informazioni relative al proprio abbonamento (data di scadenza, storico degli ordini e simili) e rinnovarlo autonomamente.
- Amministratore di un gruppo di utenti. Oltre alle autorizzazioni di un utente privato, può concedere o revocare l'accesso al servizio ad altri utenti. Se gli utenti a cui è stato revocato l'accesso al servizio hanno comunque un altro abbonamento (perché utenti privati, studenti o facenti parte di un altro gruppo di account), potranno comunque accedere al servizio.
  Inoltre l'amministratore può visualizzare le statistiche sull'utilizzo del servizio da parte di tutti gli utenti a cui ha concesso l'accesso.
  Da notare che un amministratore non può accedere alle mappe di altri utenti, neanche a quelle degli utenti a cui ha concesso l'accesso, a meno che quelle mappe non siano state esplicitamente condivise dagli utenti interessati.
- Amministratore di un dominio (ad esempio amministratore di una scuola). Oltre alle autorizzazioni dell'amministratore di un gruppo di account, può impostare l'accesso ad un intero dominio di account (es, tutti gli studenti e i dipendenti di una scuola). Analogamente può accedere alle statistiche di utilizzo di tutti gli account di quel dominio.
- Operatori Anastasis di primo livello. Possono accedere alla configurazione degli abbonamenti (comprese le date di scadenza, gli account o i domini autorizzati all'accesso) con il fine di risolvere assistenze tecniche.
  Non possono in alcun modo accedere alle mappe degli utenti e tanto meno modificarle o eliminarle. Non possono neanche 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.
- Operatori 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 utenti 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:	20/02/2024

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 **media** 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 **medio** a **lieve** e pertanto di contenere al massimo l’eventuale impatto.
Le opzioni descritte nell’allegato B riportano a **lieve** 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 SuperMappeX EDU.

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:	20/02/2024

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 SuperMappeX EDU:

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:	20/02/2024

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, cognome ed e-mail.
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 SuperMappeX EDU, un servizio di creazione e modifica di mappe concettuali multimediali.
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 genitori degli utenti minorenni.
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 (insegnanti, studenti e soggetti privati) che usufruiscono del servizio SuperMappeX EDU.
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. 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	Tutta la strumentazione e le procedure per la raccolta dei

	non eccessive, in relazione alle finalità per i quali i dati vengono trattati?	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 ricavati dall'account Google degli utenti che entrano. La correttezza delle informazioni inserite è quindi responsabilità dell'utente che ha creato l'account Google (l'utente stesso o l'amministratore del dominio scolastico di Google Workplace).
10.	È stata effettuata una valutazione circa il fatto che il trattamento dei dati personali raccolti potrebbe causare danno o stress agli interessati coinvolti?	SuperMappeX EDU non tratta dati all'infuori di quelli personali.
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	Grado di rischio		Impatto	Probabilità	Grado di rischio
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	2/4	SuperMappeX EDU è ospitato da Google Cloud. Maggiori informazioni sulla sicurezza garantita da Google Cloud: https://cloud.google.com/trust-center		Bassa	1/4
Privacy (divulgazione di informazioni)	Potrebbe venire divulgati i dati di accesso degli utenti	Moderata	2/4	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:		Bassa	1/4
Compliance	Interruzione del	Moderata	2/4	SuperMappeX EDU rispetta il		Bassa	1/4

(Violazione di leggi o regolamenti)	servizio e perdita dei dati di accesso.			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.			
	Errori in fase di aggiornamento e manutenzione della web 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)		Moderata	2/4	La gestione del rischio è parzialmente gestita dall'infrastruttura Google Cloud.		Bassa	1/4

				Circa la SLA garantita da Google Cloud si veda cloud.google.com/terms/sla. 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. ● Le mappe non sono salvate dentro SuperMappeX EDU bensì dentro il Google Drive dell'utente.			

ALLEGATO C

Bologna, 20 febbraio 2024

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

Applicazione e Server

SuperMappeX EDU è un'applicazione web based SaaS ospitata dall'architettura PaaS di Google Cloud. In particolare SuperMappeX EDU usa i seguenti servizi di Google Cloud: Firebase Hosting, Cloud Functions, Cloud Storage, Realtime Database, FireStore Database e Big Query.

Backup del database e degli allegati

Ogni notte viene effettuato in automatico un backup del database su un Cloud Storage separato da quello di produzione, in maniera tale da rendere possibile il reperimento di dati vecchi. Tali backup vengono mantenuti per 100 giorni.
Non è previsto un backup dei dati in quanto il Cloud Storage di produzione è usato solo per motivi di performance: le mappe create dall'utente sono sempre salvate sul Google Drive dell'utente e non sono quindi gestite da SuperMappeX EDU.

Sicurezza del Server

La sicurezza dell'infrastruttura è garantita dai servizi di Google Cloud. Maggiori informazioni da parte di Google qui:
https://cloud.google.com/security/infrastructure/design/resources/google_infrastructure_whitepaper_fa.pdf
Il servizio inoltre è configurato affinché l'accesso diretto ai dati sia permesso solo agli account degli operatori Anastasis autorizzati.

Conformità alla legge 196

Per accedere a SuperMappeX EDU è necessario utilizzare un account Google. Maggiori informazioni su Google e privacy qui: https://policies.google.com/privacy?hl=it
I dati relativi agli account Google autorizzati ad accedere a SuperMappeX EDU(nome, cognome e email) sono conservati da Anastasis fino a 2 anni dopo la scadenza dell'abbonamento al servizio.

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:

- Vincenzo Carnazzo, nato a Milazzo il 2/9/1980, CF CRNVCN80P02F206D
- Fabrizio Piazza, nato a Bologna il 4/9/1970, CF PZZFRZ70P04A944W

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.

Data Center in cui risiedono i dati di SuperMappeX EDU e SLA

I data center su cui risiedono i dati di SuperMappeX EDU sono collocati esclusivamente nei Paesi che appartengono all'Unione Europea, nello specifico nelle seguenti aree geografiche:

- Saint-Ghislain, Belgio:
  https://www.google.com/intl/it/about/datacenters/locations/st-ghislain/
- Eemshaven, Paesi Bassi:
  https://www.google.com/intl/it/about/datacenters/locations/eemshaven/
- Middenmeer, Paesi Bassi:
  https://www.google.com/intl/it/about/datacenters/locations/middenmeer/

La percentuale di funzionamento del servizio che viene garantita in un anno è del 99,7%, che vuol dire all'incirca 1 giorno di down su 365.

Riferimenti per il Data Privacy Framework relativo ai servizi Google

- https://policies.google.com/privacy/frameworks?hl=it