DPIA : 109

Data 01/09/2024

Società Ospedale San Raffaele S.r.l.

Panoramica del trattamento

Processo Ricerca Scientifica

Fase Ricerca clinica

Attività Esecuzione di attività di ricerca scientifica

ID 109

Descrizione

Il trattamento fa riferimento ai dati personali del paziente utilizzati per finalità di ricerca scientifica condotta dal personale medico di Chirurgia Oncologia Generale, in particolare:
- raccolta dati personali presso il paziente, i sistemi e le strutture interne;
- monitoraggio del paziente e raccolta di ulteriori dati clinici;
- elaborazione ed analisi dei dati sulla base degli obiettivi dello studio;
- elaborazione dei risultati dello studio.

L'unita svolge attività di ricerca di base, traslazione, e clinica di tipo sperimentale e osservazionale retrospettiva e prospettica, multicentrica e spontanea.
Per tutti i dettagli relativi ai singoli progetti di ricerca (e.g. finalità del singolo studio, soggetti coinvolti, dati personali trattati, asset fisici e/o tecnologici impiegati, ecc.), si rimanda quindi ai rispettivi fascicoli di progetto di ricerca (e.g. protocolli e documentazione affine), conservati da ciascun P.I., il quale è identificato alla voce "Referente" di cui al presente trattamento.

Unità Organizzativa Medicina 1Q-A - Oncologia Medica

Categoria di Interessato	Numerosità degli interessati	Soggetti Vulnerabili	Finalità	Termini di conservazione	Criteri
Pazienti	Migliaia	Soggetti arruolati in studi clinici	Finalità di ricerca scientifica in campo medico, biomedico o epidemiologico	10 anni	

Note

Protocollo AI Hope

Il **protocollo AI-HOPE** è uno studio osservazionale multicentrico non interventistico che mira a sviluppare un algoritmo predittivo per il carcinoma polmonare metastatico, utilizzando tecnologie di **Machine Learning**. Ecco un riassunto dei punti principali:

1. Titolo e Scopo

Lo studio, denominato **AI-HOPE**, ha l'obiettivo di identificare variabili predittive e/o prognostiche per migliorare la risposta ai trattamenti standard per il carcinoma polmonare metastatico. Verranno create due coorti di pazienti:

- **Coorte A**: Pazienti con carcinoma polmonare non a piccole cellule (NSCLC) stadio IV con espressione di PD-L1 ≥ 50%, trattati con immunoterapia in monoterapia.
- **Coorte B**: Pazienti con NSCLC stadio IV con espressione di PD-L1 < 50%, trattati con chemio-immunoterapia.

2. Obiettivo Primario

L’obiettivo è identificare variabili che possano predire:

- **Progressione precoce** (entro 3 mesi dall'inizio del trattamento).
- **Tossicità moderato-severa** (con focus su tossicità polmonari).
- **Lunga sopravvivenza** (superiore alla mediana degli studi clinici).

3. Metodologia

Verranno utilizzate tecnologie di **Machine Learning** (in partnership con Microsoft) per sviluppare un algoritmo predittivo. I dati raccolti includeranno variabili cliniche, laboratoristiche, radiologiche, molecolari e patologiche. Lo studio prevede la raccolta di dati retrospettivi e prospettici da diverse strutture ospedaliere.

4. Durata dello Studio

Lo studio retrospettivo raccoglierà dati fino al primo semestre del 2024, mentre la fase prospettica si concluderà il 31 dicembre 2025. L'osservazione dei pazienti proseguirà fino a decesso o ritiro del consenso.

5. Popolazione

Lo studio include pazienti maggiorenni con diagnosi di carcinoma polmonare non a piccole cellule trattati almeno con un ciclo di terapia per la malattia metastatica. I criteri di esclusione includono pazienti con carcinoma polmonare a piccole cellule o che hanno ricevuto solo un ciclo di terapia senza ulteriori follow-up.

6. Gestione dei Dati e Privacy

I dati dei pazienti verranno raccolti in forma **pseudo-anonima** e gestiti attraverso un sistema di **CRF elettronica** (Redcap), garantendo il rispetto delle normative di privacy previste dal GDPR. Nei centri non IRCCS, i dati saranno raccolti in forma completamente anonima.

7. Analisi Statistica

L'analisi statistica sarà condotta utilizzando approcci di **Machine Learning** come **AutoML** e strumenti per interpretare il modello predittivo. I risultati saranno validati con tecniche di cross-validation, e i dati saranno rappresentati con curve di sopravvivenza e grafici di probabilità.

8. Aspetti Etici

Lo studio rispetta le normative etiche secondo la **Dichiarazione di Helsinki** e le **Buone Pratiche Cliniche**. È prevista l'approvazione del Comitato Etico prima dell'attivazione dello studio. I pazienti coinvolti nella fase prospettica firmeranno un consenso informato specifico.

9. Aspetti Economici

Lo studio è di natura no-profit e non riceve finanziamenti esterni. Non sono previsti costi aggiuntivi per i partecipanti e non è necessaria copertura assicurativa.

10. Pubblicazione dei Risultati

I dati e i risultati saranno pubblicati in forma anonima in riviste scientifiche e presentazioni congressuali.

In sintesi, il protocollo AI-HOPE si propone di sfruttare l'intelligenza artificiale per migliorare le decisioni terapeutiche in pazienti con carcinoma polmonare metastatico, raccogliendo dati osservazionali e sviluppando un modello predittivo che aiuti a identificare i pazienti che beneficiano maggiormente dei trattamenti disponibili.

Ruolo dalla Società Titolare del Trattamento

Il trattamento è effettuato in contitolarità? (art. 26 GDPR) No

Il trattamento è effettuato per conto del titolare? (art. 28 GDPR) Sì

Fornitore	Fornitore Proposto	Motivazione della Trasmissione	Modalità di Trasmissione	Tipo Dato	Autorizzazione utilizzo ulteriori Responsabili	Note
Microsoft Italia				Dati Comuni, Dati Particolari	Sì	

È prevista una comunicazione ad altri Titolari? (art. 2.4 ter a) CP) No

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Categorie di Dati Personali	Subcategoria di Dati Personali
Dati Comuni	Anagrafica e/o dati di contatto
Dati Particolari	Dati relativi alla salute
Dati Particolari	Dati genetici

I dati sono pubblicamente disponibili? No

È prevista diffusione dati a terzi indeterminati? (art. 2.4 ter b) CP) No

Note

1. Raccolta dei dati

- I dati vengono raccolti da cartelle cliniche esistenti (retrospettivi) e durante la fase prospettica dello studio per nuovi pazienti arruolati.
- Le informazioni includono dati clinici, radiologici, laboratoristici e molecolari.
- La raccolta dei dati avviene attraverso sistemi di **Case Report Form (CRF)** elettronica tramite la piattaforma **Redcap**.

2. Pseudonimizzazione e Anonimizzazione

- Per i dati retrospettivi e prospettici, viene garantita la **pseudo-anonimizzazione**, con l'assegnazione di un codice identificativo unico che dissocia i dati dal nominativo del paziente.
- Nei centri non IRCCS, i dati vengono raccolti in forma **completamente anonima** per garantire una maggiore protezione della privacy.

3. Archiviazione e Accesso

- I dati raccolti vengono archiviati su server sicuri, accessibili solo al personale autorizzato coinvolto nello studio.
- Un repository separato mantiene i codici di identificazione dei pazienti, garantendo che solo individui autorizzati possano riconnettere i dati al paziente.

4. Elaborazione e Analisi

- I dati vengono elaborati e analizzati tramite tecniche di **Machine Learning** per sviluppare l'algoritmo predittivo.
- L'analisi statistica include l'uso di modelli di apprendimento automatico per identificare le variabili predittive e la loro correlazione con gli outcome clinici.

5. Conservazione e Cancellazione

- I dati sono conservati fino al termine dello studio e successivamente per il tempo previsto dalla normativa per la conservazione di dati di ricerca.
- Alla fine del progetto, i dati saranno resi completamente anonimi o cancellati in conformità con le normative vigenti in materia di protezione dei dati (GDPR).

Questo ciclo garantisce la protezione della privacy e la sicurezza dei dati personali in ogni fase, rispettando i principi del GDPR.

Modalità di raccolta Dati raccolti presso interessato e/o presso terzi

Quali sono le risorse di supporto ai dati?

Il trattamento è effettuato in modalità cartacea? Sì

Il trattamento è effettuato in modalità automatizzata? Sì

Asset	Asset Proposto
Secure Web Application (RedCap)	

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi? Sì

Spiegare perché le finalità del trattamento sono specifiche, esplicite e legittime.

Il razionale per cui gli scopi del trattamento all'interno del **protocollo AI-HOPE** possono essere considerati specifici, espliciti e legittimi, nel rispetto del **GDPR**, si basa su diversi punti chiave emersi dal documento:

1. Scopi specifici:

Il trattamento dei dati nel contesto del protocollo AI-HOPE ha obiettivi chiaramente definiti. Come indicato nel documento, lo scopo primario è sviluppare un algoritmo predittivo basato sull'intelligenza artificiale per individuare variabili che possano predire la risposta dei pazienti con carcinoma polmonare metastatico ai trattamenti immunoterapici e chemioterapici standard. Le variabili di interesse sono delineate con precisione, inclusi dati clinici, radiologici, laboratoristici e patologici.

2. Scopi espliciti:

Il protocollo delinea esplicitamente gli obiettivi di raccogliere e analizzare i dati dei pazienti al fine di sviluppare uno strumento di previsione che possa migliorare le decisioni terapeutiche in oncologia polmonare. Questo scopo è stato dichiarato sin dall'inizio del protocollo, descrivendo chiaramente l'uso della tecnologia di machine learning per analizzare variabili cliniche al fine di migliorare l'efficacia del trattamento oncologico. Inoltre, il protocollo fornisce dettagli sull'uso specifico dei dati raccolti e sull'integrazione con gli strumenti di machine learning, evidenziando come le informazioni saranno utilizzate.

3. Scopi legittimi:

Gli scopi del trattamento sono legittimi perché mirano a migliorare l'efficacia clinica e i risultati terapeutici per i pazienti affetti da carcinoma polmonare metastatico, rispettando i principi del Regolamento Generale sulla Protezione dei Dati (GDPR). Lo studio è condotto in conformità con i principi etici, seguendo le linee guida delle **Buone Pratiche Cliniche** e della **Dichiarazione di Helsinki**. Inoltre, la raccolta e il trattamento dei dati sono giustificati dall'interesse scientifico e clinico, e sono espressamente collegati alla ricerca medica e al miglioramento delle cure oncologiche.

Rispetto del GDPR:

- **Limitazione delle finalità (Art. 5, par. 1, lett. b GDPR)**: Il protocollo garantisce che i dati raccolti siano utilizzati solo per gli scopi scientifici esplicitamente dichiarati, ossia lo sviluppo dell'algoritmo predittivo e non per altre finalità non collegate.

- **Minimizzazione dei dati (Art. 5, par. 1, lett. c GDPR)**: I dati raccolti includono solo le informazioni strettamente necessarie per l'analisi predittiva e non si prevede il trattamento di dati non essenziali.
- **Base giuridica per il trattamento (Art. 6 e 9 GDPR)**: Lo studio è supportato da una solida base giuridica, in quanto il trattamento dei dati sensibili è giustificato dall'interesse pubblico nella ricerca scientifica in ambito sanitario. Inoltre, i pazienti della coorte prospettica firmeranno un consenso informato specifico per lo studio.

Conclusione:

Gli scopi del trattamento sono specifici, espliciti e legittimi, poiché mirano a sviluppare un algoritmo predittivo per migliorare l'efficacia delle terapie per il carcinoma polmonare metastatico, nel pieno rispetto dei principi etici e delle norme previste dal GDPR.

Quali sono le basi legali che rendono lecito il trattamento?

Dati Comuni
Consenso dell'interessato, ai sensi dell'art. 6, par. 1 lett. a) del GDPR
Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ai sensi dell'art. 6, par. 1, lett. e) del GDPR

Categorie particolari di dati
Consenso dell'interessato, ai sensi dell'art. 9, par. 2 lett. a) del GDPR
Necessità del trattamento per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici effettuato in conformitÃ dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, a condizione che sia proporzionato alla finalitÃ perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, ai sensi dell'art. 9, par. 2 lett. j) del GDPR

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? Sì

Spiegare perché ogni dato raccolto è necessario per le finalità del trattamento.

Nel protocollo **AI-HOPE**, i dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in conformità con il principio di **minimizzazione dei dati** previsto dal **GDPR (Art. 5, par. 1, lett. c)**. Ecco il razionale che dimostra come viene rispettato tale principio:

1. Adeguatezza dei dati raccolti

I dati trattati sono strettamente connessi agli obiettivi dello studio, che consistono nello sviluppo di un algoritmo predittivo in grado di migliorare le decisioni terapeutiche nel carcinoma polmonare metastatico. I dati raccolti includono:

- **Dati clinici** (anagrafici, comorbidità, sintomi, ecc.)
- **Dati radiologici e laboratoristici** (dimensione del tumore, risultati delle PET, ecc.)
- **Dati molecolari e anatomo-patologici** (espressione di PD-L1, analisi genetiche, ecc.).

Queste informazioni sono essenziali per raggiungere l'obiettivo dello studio, poiché consentono di sviluppare un modello predittivo basato sull'analisi delle variabili che influenzano la risposta alle terapie. La raccolta di questi dati è quindi adeguata rispetto alle finalità dello studio, che richiede un ampio spettro di variabili cliniche e biologiche per produrre previsioni accurate.

2. Pertinenza dei dati rispetto agli scopi

Tutti i dati raccolti sono direttamente pertinenti al fine di individuare variabili predittive e prognostiche utili a guidare le scelte terapeutiche. Il protocollo specifica che vengono raccolti solo i dati necessari per lo sviluppo dell'algoritmo, evitando la raccolta di informazioni non correlate agli scopi dello studio. Ad esempio, non vengono raccolti dati che non hanno un impatto diretto sulla prognosi e sulla risposta alle terapie oncologiche, come informazioni personali non mediche o dati irrilevanti per l'outcome clinico.

3. Limitazione a quanto è necessario (minimizzazione dei dati)

Il principio di **minimizzazione dei dati** è rispettato, poiché il protocollo limita la raccolta dei dati alle sole informazioni che sono necessarie per rispondere alle domande cliniche e scientifiche dello studio. I seguenti elementi ne sono la prova:

- **Pseudo-anonimizzazione**: I dati raccolti vengono pseudo-anonimizzati per proteggere l'identità dei pazienti, trattando solo le informazioni necessarie per l'algoritmo predittivo. La gestione dei dati prevede l'assegnazione di un codice identificativo che non è collegato ai dati personali del paziente, salvo per il personale autorizzato.
- **Selezione mirata delle variabili**: Le variabili raccolte sono selezionate in base alla loro rilevanza scientifica per l'outcome dello studio. Il protocollo sottolinea che i dati clinici, molecolari e di imaging sono fondamentali per creare modelli predittivi robusti, ma non vengono raccolte informazioni superflue che non abbiano un impatto diretto sull'algoritmo.
- **Utilizzo di dati retrospettivi e prospettici**: I dati retrospettivi vengono raccolti dalle cartelle cliniche solo se strettamente necessari per l'addestramento dell'algoritmo, evitando così la raccolta di informazioni aggiuntive o non pertinenti.

4. Misure di sicurezza per garantire la minimizzazione dei dati

Per garantire che i dati siano limitati a quanto necessario, il protocollo prevede rigide misure di sicurezza. Tra queste vi è l'anonimizzazione completa per i centri che non sono IRCCS, che elimina qualsiasi informazione che possa rendere identificabile un paziente. Inoltre, per i centri che non possono ottenere il consenso informato per i dati retrospettivi, vengono adottate procedure di pseudo-anonimizzazione e anonimizzazione, riducendo al minimo la quantità di informazioni personali trattate.

Conclusione:

Il protocollo AI-HOPE rispetta il principio di **minimizzazione dei dati** del GDPR, raccogliendo solo le informazioni strettamente necessarie per raggiungere gli scopi dello studio. La raccolta è limitata a dati clinici e biologici pertinenti, e vengono applicate misure di pseudo-anonimizzazione e anonimizzazione per ridurre al minimo il trattamento di dati personali sensibili.

I dati sono esatti e aggiornati? Sì

Descrivere le misure previste per garantire la qualità dei dati.

Nel protocollo **AI-HOPE**, i dati raccolti sono gestiti in conformità con il principio di **esattezza** previsto dal **GDPR (Art. 5, par. 1, lett. d)**, che impone che i dati personali siano esatti e, ove necessario, aggiornati. Ecco il razionale che spiega come viene rispettato questo principio:

1. Esattezza dei dati raccolti

- **Fonte dei dati**: I dati vengono raccolti direttamente dalle **cartelle cliniche** dei pazienti, che costituiscono la principale fonte di informazioni mediche verificate e validate. Essendo queste cartelle costantemente aggiornate durante il percorso di cura, garantiscono che i dati clinici, radiologici e patologici siano accurati e riflettano lo stato di salute del paziente al momento del trattamento.
- **Dati retrospettivi e prospettici**: Nel protocollo AI-HOPE, i dati retrospettivi sono già presenti nelle cartelle cliniche e vengono raccolti per il periodo di trattamento già avvenuto. Questi dati sono stati registrati in tempo reale durante la somministrazione delle cure, riducendo così il rischio di errori o discrepanze. Per quanto riguarda i dati prospettici, questi saranno raccolti man mano che i pazienti vengono trattati, assicurando che i dati siano sempre esatti e aggiornati in tempo reale.

2. Aggiornamento continuo dei dati

- **Parte prospettica dello studio**: La parte prospettica del protocollo prevede la raccolta e l'aggiornamento costante dei dati man mano che i pazienti continuano a essere trattati e monitorati. I dati clinici, laboratoristici e radiologici vengono aggiornati a ogni nuova valutazione medica, assicurando che le informazioni raccolte siano sempre attuali e pertinenti. Questo aggiornamento regolare permette che i dati utilizzati per alimentare l'algoritmo predittivo siano tempestivamente adeguati agli sviluppi clinici del paziente.
- **Monitoraggio e follow-up regolari**: Il protocollo prevede visite di follow-up periodiche per ogni paziente, durante le quali vengono raccolti nuovi dati clinici e laboratoristici. Questo processo di monitoraggio continuo garantisce che i dati siano aggiornati e che eventuali cambiamenti nello stato di salute dei pazienti siano prontamente registrati.

3. Verifica e controllo della qualità dei dati

- **Strumenti per la gestione dei dati**: I dati vengono raccolti e gestiti tramite un sistema di **Case Report Form (CRF)** sviluppato con **Redcap**, una piattaforma che permette l'inserimento e il monitoraggio strutturato e preciso dei dati clinici. Questo sistema supporta il controllo di qualità durante la raccolta dei dati e riduce il rischio di errori.
- **Supervisione del personale autorizzato**: La raccolta e l'aggiornamento dei dati sono effettuati da personale medico e di ricerca autorizzato, che è addestrato a garantire l'accuratezza delle informazioni inserite. La supervisione dello sperimentatore principale e del personale incaricato assicura un controllo regolare della qualità e dell'accuratezza dei dati.

4. Procedure per la correzione dei dati

- **Correzione tempestiva di eventuali errori**: Il protocollo prevede che, nel caso in cui vengano rilevati errori o inesattezze nei dati raccolti, siano immediatamente corretti. Questo processo garantisce che i dati trattati rimangano il più possibile esatti nel tempo, in conformità con il diritto degli interessati a ottenere la rettifica dei propri dati personali.

Conclusione:

Nel protocollo AI-HOPE, i dati raccolti sono **esatti** e **aggiornati**, poiché provengono da fonti affidabili e validate come le cartelle cliniche, sono costantemente aggiornati durante il corso dello studio e sono soggetti a rigorosi controlli di qualità. Il protocollo prevede anche procedure per la correzione immediata di eventuali inesattezze, in linea con i principi del GDPR.

Qual è il periodo di conservazione dei dati?

Dati comuni	Da definire
Categorie particolari di dati	Da definire

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Informativa somministrata direttamente agli interessati per i soggetti arruolati prospetticamente.

Informativa pubblicata per pubblici proclami sui siti internet del promotore e dei partecipanti allo studio per i soggetti arruolati retrospettivamente.

Ove applicabile: come si ottiene il consenso degli interessati?

direttamente presso l'interessato in forma scritta

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Fornitore	Fornitore Proposto	Nomina Responsabile del Trattamento (DPA)	Autorizzazione utilizzo ulteriori Responsabili
Microsoft Italia		Sì	Sì

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Non è previsto trasferimento extra UE.

Misure esistenti o pianificate

Misure di Sicurezza

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
	Secure Web Application (RedCap)	No	Sì	Sì	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
	Secure Web Application (RedCap)	No	Sì	Sì	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.
	Secure Web Application (RedCap)	No	Sì	Sì	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	No	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.
	Secure Web Application (RedCap)	Sì	No	No	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
	Secure Web Application (RedCap)	No	Sì	Sì	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.
	Secure Web Application (RedCap)	Sì	No	No	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup completi devono essere eseguiti regolarmente.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.
	Secure Web Application (RedCap)	Sì	Sì	No	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
	Secure Web Application (RedCap)	Sì	Sì	No	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Devono essere eseguiti test periodici di penetrazione.
	Secure Web Application (RedCap)	Sì	No	No	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere seguiti standard e pratiche di codifica sicure.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.
	Secure Web Application (RedCap)	Sì	No	No	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.
	Secure Web Application (RedCap)	Sì	No	No	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.
	Secure Web Application (RedCap)	Sì	Sì	No	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.
	Secure Web Application (RedCap)	No	No	Sì	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

Misure di Sicurezza in Corso

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
	Secure Web Application (RedCap)	Sì	No	No	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.
	Secure Web Application (RedCap)	Sì	Sì	No	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).
	Secure Web Application (RedCap)	Sì	Sì	No	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.
	Secure Web Application (RedCap)	Sì	Sì	No	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.
	Secure Web Application (RedCap)	Sì	Sì	No	Le password degli utenti devono essere memorizzate in una forma "hash".
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.
	Secure Web Application (RedCap)	Sì	No	No	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
	Secure Web Application (RedCap)	Sì	No	Sì	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
	Secure Web Application (RedCap)	No	No	Sì	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.
	Secure Web Application (RedCap)	Sì	Sì	No	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.
	Secure Web Application (RedCap)	Sì	No	No	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.
	Secure Web Application (RedCap)	Sì	No	No	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	Secure Web Application (RedCap)	Sì	Sì	No	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	Secure Web Application (RedCap)	Sì	No	No	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.
	Secure Web Application (RedCap)	Sì	No	No	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	No	No	Sì	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).

Misure di Sicurezza Aziendali

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
			Formazione						Basso		Trasversale			
A.1	A - Security Policy e Procedure Protezione PII	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.2	A - Security Policy e Procedure Protezione PII	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.3	A - Security Policy e Procedure Prote	L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	zione PII	policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate.												
A.4	A - Security Policy e Procedure Protezione PII	La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.5	A - Security Policy e Procedure Protezione PII	Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.6	A - Security Policy e Procedure Protezione PII	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	"
B.1	B - Ruoli e Resp	Ruoli e responsabilità relative al trattamento dei				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	onsabilità	dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale												
B.2	B - Ruoli e Responsabilità	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
B.3	B - Ruoli e Responsabilità	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
B.4	B - Ruoli e Responsabilità	Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
B.5	B - Ruoli e Responsabilità	Compiti e responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
C.1	C- Access Control Policy	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
C.2	C- Access Control Policy	Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. L'organizzazione dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure relative ai dati personali.				Sì	Sì	No	Medio	Sì	Trasversale	Trasversale	Non Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
C.3	C-Access Control Policy	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
C.4	C-Access Control Policy	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
D.1	D-Resource and asset management	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
D.2	D-Resource and asset management	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.				Sì	Sì	Sì	Basso		Trasversale	Trasversale	Conforme	
D.3	D-Resource and asset management	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
D.4	D-Resource and asset management	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Non Applicabile	
E.1	E - Change Management	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
E.2	E - Change Man	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	agement	non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.												
E.3	E - Change Management	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
F.1	F - Data Processor (responsabile	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	esterno)	dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.												
F.2	F - Data Processor (responsabile esterno)	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
F.3	F - Data Processor (responsabile esterno)	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Azienda le	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.												
F.4	F - Data Processor (responsabile esterno)	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
F.5	F - Data Processor (responsabile esterno)	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.				Sì	No	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
G.1	G - Gestione Incidenti/ Personal Data breaches	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
G.2	G - Gestione Incidenti/ Personal Data breaches	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Conforme	
G.3	G - Gestione Incidenti/ Personal Data breaches	Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Non Conforme	
G.4	G - Gestione Incidenti/ Personal Data breaches	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione intraprese.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
H.1	H - Business Continuity	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello				No	No	Sì	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).												
H.2	H - Business Continuity	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.				No	No	Sì	Medio	Sì	Trasversale	Verticale	Non Conforme	
H.3	H - Business Continuity	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.				No	No	Sì	Medio	Sì	Trasversale	Verticale	Non Conforme	
H.4	H - Business Continuity	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.				No	No	Sì	Alto	Sì	Trasversale	Verticale	Non Conforme	
H.5	H - Business	Si dovrebbe prendere in considerazione una struttura IT alternativa				No	No	Sì	Alto	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	Continuity	(disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.												
I.1	I - Riservatezza del personale	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
I.2	I - Riservatezza del personale	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Conforme	
I.3	I - Riservatez	I dipendenti coinvolti nel trattamento dei				Sì	No	No	Alto	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	za del personale	dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).												
J.1	J - Training	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
J.2	J - Training	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale,				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati.												
J.3	J - Training	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
K.1	K - Controllo Accessi e autenticazione	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
K.2	K - Controllo Accessi e autenticazione	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
K.3	K - Controllo Accessi e aute	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ntica zione	sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.												
K.4	K - Controllo Accessi e autenticazione	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Conforme	
K.5	K - Controllo Accessi e autenticazione	Dovrebbe essere definita e documentata una policy specifica per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.				Sì	Sì	No	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
K.6	K - Controllo Accessi e autenticazione	Le password degli utenti devono essere memorizzate in una forma "hash".				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
K.7	K - Controllo Acce	L'autenticazione a due fattori (autenticazione forte) dovrebbe				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ssi e autenticazione	preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.											Conforme	
K.8	K - Controllo Accessi e autenticazione	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
L.1	L - Logging e Monitoraggio	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
L.2	L - Logging e Monitoraggio	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.												
L.3	L - Logging e Monitoraggio	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
L.4	L - Logging e Monitoraggio	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
L.5	L - Logging e Monitoraggio	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
M.1	M - Server/Database security - crittografia	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		per funzionare correttamente.												
M.2	M - Server/Database security - crittografia	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
M.3	M - Server/Database security - crittografia	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.4	M - Server/Database security - crittografia	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.5	M - Server/Database security - crittografia	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.6	M - Server/Dat	Dovrebbero essere considerate le				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	abase security - crittografia	tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.											Conforme	
N.1	N - Workstation security	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
N.2	N - Workstation security	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
N.3	N - Workstation security	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
N.4	N - Workstation security	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.5	N - Workstation security	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
N.6	N - Workstation security	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
N.7	N - Workstation security	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.8	N - Workstation security	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.				Sì	Sì	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.9	N - Workstation security	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.1	O - Sicurezza del network e delle	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	comunicazioni	tramite protocolli crittografici (TLS / SSL).												
O.2	O - Sicurezza del network e delle comunicazioni	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Conforme	
O.3	O - Sicurezza del network e delle comunicazioni	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Conforme	
O.4	O - Sicurezza del network e delle comunicazioni	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
O.5	O - Sicurezza del network e delle comu	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Non Applicabile	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	nicazioni	per il trattamento dei dati personali.												
O.6	O - Sicurezza del network e delle comunicazioni	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.7	O - Sicurezza del network e delle comunicazioni	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
P.1	P - Back up dati	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.				No	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
P.2	P - Back up dati	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Conforme	
P.3	P - Back up dati	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.				No	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
P.4	P - Back up dati	I backup completi devono essere eseguiti regolarmente.				No	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
P.5	P - Back up dati	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.6	P - Back up dati	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.7	P - Back up dati	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.8	P - Back up dati	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare del trattamento.				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Non Applicabile	
P.9	P - Back up dati	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.				Sì	Sì	Sì	Alto	Sì	Verticale	Verticale	Conforme	
Q.1	Q - Mobile/Portable Devices	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
Q.2	Q - Mobile/Portable Devices	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Conforme	
Q.3	Q - Mobile/Portable Devices	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
Q.4	Q - Mobile/Portable Devices	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
Q.5	Q - Mobile/Portable Devices	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.6	Q - Mobile/Portable Devices	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
Q.7	Q - Mobile/Portable Devices	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.				Sì	No	Sì	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.8	Q - Mobile/Portable Devices	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).				Sì	Sì	No	Alto	Sì	Trasversale	Verticale	Non Conforme	
Q.9	Q - Mobile/Portable Devices	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
R.1	R - Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.2	R - Sicurezza del ciclo di vita delle applicazioni	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.3	R - Sicurezza del ciclo	Le tecnologie e le tecniche specifiche progettate per supportare la				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	di vita delle applicazioni	privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.												
R.4	R - Sicurezza del ciclo di vita delle applicazioni	Dovrebbero essere seguiti standard e pratiche di codifica sicure.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.5	R - Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.6	R - Sicurezza del ciclo di vita delle applicazioni	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		di sicurezza richiesto.												
R.7	R - Sicurezza del ciclo di vita delle applicazioni	Devono essere eseguiti test periodici di penetrazione.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.8	R - Sicurezza del ciclo di vita delle applicazioni	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.9	R - Sicurezza del ciclo di vita delle applicazioni	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
S.1	S - Cancellazione/ Eliminazione dei Dati	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Conforme	
S.2	S - Cancellazione/ Elimi	È necessario eseguire la triturazione della carta e dei supporti portatili				Sì	No	No	Basso		Trasversale	Verticale	Non Applicabile	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	nazione dei Dati	utilizzati per memorizzare i dati personali.												
S.3	S - Cancellazione/ Eliminazione dei Dati	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Non Applicabile	
S.4	S - Cancellazione/ Eliminazione dei Dati	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Conforme	
S.5	S - Cancellazione/ Eliminazione dei Dati	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Conforme	
S.6	S - Cancellazione/ Eliminazione dei Dati	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare				Sì	No	No	Alto	Sì	Trasversale	Verticale	Non Applicabile	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		del trattamento (ed evitare il trasferimento all'esterno dei dati personali.												
T.1	T - Sicurezza Fisica	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Conforme	
T.2	T - Sicurezza Fisica	Meccanismi di identificazione tramite mezzi appropriati, ad es. i badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.3	T - Sicurezza Fisica	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.4	T - Sicurezza Fisica	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.5	T - Sicurezza Fisica	Se del caso, dovrebbero essere costruite barriere fisiche per impedire				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		l'accesso fisico non autorizzato.												
T.6	T - Sicurezza Fisica	Le aree protette vuote dovrebbero essere bloccate fisicamente e controllate periodicamente.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.7	T - Sicurezza Fisica	Ddovrebbero essere attivati nella sala server un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS).				No	No	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.8	T - Sicurezza Fisica	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	

Misure Non Utilizzate

Misure Non Utilizzate

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
			Formazione						Basso		Trasversale			
A.1	A - Security Policy e Procedure Protezione PII	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
A.2	A - Security Policy e Procedure Protezione PII	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.3	A - Security Policy e Procedure Protezione PII	L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.4	A - Security Policy e Procedure Protezione PII	La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
A.5	A - Security Policy e Proc	Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	edure Protezione PII	alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.												
A.6	A - Security Policy e Procedure Protezione PII	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	"
B.1	B - Ruoli e Responsabilità	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
B.2	B - Ruoli e Responsabilità	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
B.3	B - Ruoli e Responsabilità	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza,				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		compresa la nomina di un responsabile della sicurezza.												
B.4	B - Ruoli e Responsabilità	Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
B.5	B - Ruoli e Responsabilità	Compiti e responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
C.1	C- Access Control Policy	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
C.2	C-Access Control Policy	Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. L'organizzazione dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure relative ai dati personali.				Sì	Sì	No	Medio	Sì	Trasversale	Trasversale	Non Conforme	
C.3	C-Access Control Policy	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
C.4	C-Access Control Policy	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
D.1	D-Resource and asset management	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		(hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).												
D.2	D-Resource and asset management	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.				Sì	Sì	Sì	Basso		Trasversale	Trasversale	Conforme	
D.3	D-Resource and asset management	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
D.4	D-Resource and asset management	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Non Applicabile	
E.1	E - Change Management	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.												
E.2	E - Change Management	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
E.3	E - Change Management	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.												
F.1	F - Data Processor (responsabile esterno)	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
F.2	F - Data Processor (responsabile esterno)	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		senza indebiti ritardi.												
F.3	F - Data Processor (responsabile esterno)	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
F.4	F - Data Processor (responsabile esterno)	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
F.5	F - Data Processor (responsabile	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici				Sì	No	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	esterno)	accordi documentati di riservatezza / non divulgazione.												
G.1	G - Gestione Incidenti/ Personal Data breaches	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	
G.2	G - Gestione Incidenti/ Personal Data breaches	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Conforme	
G.3	G - Gestione Incidenti/ Personal Data breaches	Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Non Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
G.4	G - Gestione Incidenti/ Personal Data breaches	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione intraprese.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
H.1	H - Business Continuity	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).				No	No	Sì	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
H.2	H - Business Continuity	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.				No	No	Sì	Medio	Sì	Trasversale	Verticale	Non Conforme	
H.3	H - Business Continuity	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla				No	No	Sì	Medio	Sì	Trasversale	Verticale	Non Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		sicurezza dei dati personali.												
H.4	H - Business Continuity	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.				No	No	Sì	Alto	Sì	Trasversale	Verticale	Non Conforme	
H.5	H - Business Continuity	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.				No	No	Sì	Alto	Sì	Trasversale	Verticale	Conforme	
I.1	I - Riservatezza del personale	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
I.2	I - Riservatezza del personale	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Conforme	
I.3	I - Riservatezza del personale	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).				Sì	No	No	Alto	Sì	Trasversale	Verticale	Conforme	
J.1	J - Training	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.												
J.2	J - Training	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Parzialmente Conforme	
J.3	J - Training	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.				Sì	Sì	Sì	Alto	Sì	Trasversale	Trasversale	Parzialmente Conforme	
K.1	K - Controllo Accessi e autenticazione	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
K.2	K - Controllo Accessi e autenticazione	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
K.3	K - Controllo Accessi e autenticazione	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
K.4	K - Controllo Accessi e autenticazione	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Conforme	
K.5	K - Controllo Acce	Dovrebbe essere definita e documentata una policy specifica				Sì	Sì	No	Medio	Sì	Trasversale	Trasversale	Parzialmente	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	ssi e autenticazione	per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.											Conforme	
K.6	K - Controllo Accessi e autenticazione	Le password degli utenti devono essere memorizzate in una forma "hash".				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
K.7	K - Controllo Accessi e autenticazione	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
K.8	K - Controllo Accessi e autenticazione	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
L.1	L - Logging e Monitoraggio	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
L.2	L - Logging e Monitoraggio	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
L.3	L - Logging e Monitoraggio	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
L.4	L - Logging e Monitoraggio	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		monitoraggio per rilevare attività insolite.												
L.5	L - Logging e Monitoraggio	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
M.1	M - Server/Database security - crittografia	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
M.2	M - Server/Database security - crittografia	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Parzialmente Conforme	
M.3	M - Server/Database security - crittografia	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
M.4	M - Server/Database security - crittografia	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.5	M - Server/Database security - crittografia	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.				Sì	No	No	Medio	Sì	Verticale	Verticale	Parzialmente Conforme	
M.6	M - Server/Database security - crittografia	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.				Sì	Sì	No	Alto	Sì	Verticale	Verticale	Parzialmente Conforme	
N.1	N - Workstation security	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
N.2	N - Workstation security	Le applicazioni anti-virus e le firme di rilevamento devono essere				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Azienda le	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		configurate su base settimanale.												
N.3	N - Workstation security	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
N.4	N - Workstation security	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.5	N - Workstation security	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
N.6	N - Workstation security	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
N.7	N - Workstation security	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
N.8	N - Workstation security	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a				Sì	Sì	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.												
N.9	N - Workstation security	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.1	O - Sicurezza del network e delle comunicazioni	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.2	O - Sicurezza del network e delle comunicazioni	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Conforme	
O.3	O - Sicurezza del network e delle comunicazioni	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazion				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		e (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.												
O.4	O - Sicurezza del network e delle comunicazioni	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	
O.5	O - Sicurezza del network e delle comunicazioni	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Non Applicabile	
O.6	O - Sicurezza del network e delle comunicazioni	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
O.7	O - Sicurezza del network e delle comunicazioni	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).				Sì	Sì	Sì	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
P.1	P - Back up dati	Le procedure di backup e ripristino dei dati devono essere definite,				No	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		documentate e chiaramente collegate a ruoli e responsabilità.												
P.2	P - Back up dati	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.				Sì	Sì	No	Basso	Sì	Verticale	Verticale	Conforme	
P.3	P - Back up dati	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.				No	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
P.4	P - Back up dati	I backup completi devono essere eseguiti regolarmente.				No	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
P.5	P - Back up dati	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.6	P - Back up dati	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.7	P - Back up dati	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.				No	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
P.8	P - Back up dati	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere				Sì	Sì	No	Medio	Sì	Verticale	Verticale	Non Applicabile	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		trasmessa dal titolare del trattamento.												
P.9	P - Back up dati	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.				Sì	Sì	Sì	Alto	Sì	Verticale	Verticale	Conforme	
Q.1	Q - Mobile/Portable Devices	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.				Sì	Sì	Sì	Basso	Sì	Trasversale	Verticale	Conforme	
Q.2	Q - Mobile/Portable Devices	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Conforme	
Q.3	Q - Mobile/Portable Devices	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.				Sì	Sì	No	Basso	Sì	Trasversale	Verticale	Conforme	
Q.4	Q - Mobile/Portable Devices	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.				Sì	Sì	Sì	Medio	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
Q.5	Q - Mobile/Portable Devices	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.6	Q - Mobile/Portable Devices	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.				Sì	Sì	No	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.7	Q - Mobile/Portable Devices	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.				Sì	No	Sì	Medio	Sì	Trasversale	Verticale	Parzialmente Conforme	
Q.8	Q - Mobile/Portable Devices	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).				Sì	Sì	No	Alto	Sì	Trasversale	Verticale	Non Conforme	
Q.9	Q - Mobile/Portable Devices	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Parzialmente Conforme	
R.1	R - Sicurezza del ciclo di vita	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	delle applicazioni	sviluppo, framework o standard di protezione sicuri ben noti.												
R.2	R - Sicurezza del ciclo di vita delle applicazioni	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.3	R - Sicurezza del ciclo di vita delle applicazioni	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.4	R - Sicurezza del ciclo di vita delle applicazioni	Dovrebbero essere seguiti standard e pratiche di codifica sicure.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	
R.5	R - Sicurezza del ciclo di vita delle appli	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.				Sì	Sì	Sì	Basso	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	cazioni													
R.6	R - Sicurezza del ciclo di vita delle applicazioni	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.7	R - Sicurezza del ciclo di vita delle applicazioni	Devono essere eseguiti test periodici di penetrazione.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.8	R - Sicurezza del ciclo di vita delle applicazioni	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	
R.9	R - Sicurezza del ciclo di vita delle	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.				Sì	Sì	Sì	Medio	Sì	Verticale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	applicazioni													
S.1	S - Cancellazione/ Eliminazione dei Dati	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.				Sì	No	No	Basso	Sì	Trasversale	Verticale	Conforme	
S.2	S - Cancellazione/ Eliminazione dei Dati	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.				Sì	No	No	Basso		Trasversale	Verticale	Non Applicabile	
S.3	S - Cancellazione/ Eliminazione dei Dati	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Non Applicabile	
S.4	S - Cancellazione/ Eliminazione dei Dati	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.				Sì	No	No	Medio	Sì	Trasversale	Verticale	Conforme	
S.5	S - Cancellazione/	Dopo la cancellazione del software, dovrebbero				Sì	No	No	Alto	Sì	Trasversale	Verticale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
	Eliminazione dei Dati	essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.												
S.6	S - Cancellazione/ Eliminazione dei Dati	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali.				Sì	No	No	Alto	Sì	Trasversale	Verticale	Non Applicabile	
T.1	T - Sicurezza Fisica	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.				Sì	Sì	Sì	Basso	Sì	Trasversale	Trasversale	Conforme	
T.2	T - Sicurezza Fisica	Meccanismi di identificazione tramite mezzi appropriati, ad es. i badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.3	T - Sicurezza Fisica	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	

Identificatore	Categoria - ENISA	Misura - ENISA	Categoria - Gruppo	Misura - Gruppo	Misura Aziendale	R	I	D	Livello di Rischio	Utilizzo	Perimetro (Gruppo)	Perimetro	Conformità	Note
		registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro.												
T.4	T - Sicurezza Fisica	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.5	T - Sicurezza Fisica	Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.6	T - Sicurezza Fisica	Le aree protette vuote dovrebbero essere bloccate fisicamente e controllate periodicamente.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.7	T - Sicurezza Fisica	Ddovrebbero essere attivati nella sala server un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS).				No	No	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	
T.8	T - Sicurezza Fisica	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.				Sì	Sì	Sì	Medio	Sì	Trasversale	Trasversale	Conforme	

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti Potenziali
Perdita di controllo dei propri dati
Utilizzo da parte di terzi di dati dell'interessato

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia
Comportamenti sleali/fraudolenti
Attacco informatico (es. social engineering, man in the middel, denial of ervice, brute force, etc.)
Furto e/o perdita di dispositivi, supporti di memorizzazione, documenti

Quali sono le fonti di rischio?

Fonte
Fonti umane esterne (es. criminali informatici, fornitori, utenti)
Fonti umane interne accidentali (es. collaboratori negligenti)

Misure Applicate

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
	Secure Web Application (RedCap)	No	Sì	Sì	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
	Secure Web Application (RedCap)	No	Sì	Sì	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.
	Secure Web Application (RedCap)	No	Sì	Sì	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.
	Secure Web Application (RedCap)	Sì	No	No	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
	Secure Web Application (RedCap)	No	Sì	Sì	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.
	Secure Web Application (RedCap)	Sì	No	No	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	No	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup completi devono essere eseguiti regolarmente.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.
	Secure Web Application (RedCap)	Sì	Sì	No	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
	Secure Web Application (RedCap)	Sì	Sì	No	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Devono essere eseguiti test periodici di penetrazione.
	Secure Web Application (RedCap)	Sì	No	No	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere seguiti standard e pratiche di codifica sicure.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.
	Secure Web Application (RedCap)	Sì	No	No	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.
	Secure Web Application (RedCap)	Sì	Sì	No	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.
	Secure Web Application (RedCap)	No	No	Sì	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

Misure da Applicare

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.
	Secure Web Application (RedCap)	Sì	No	No	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
	Secure Web Application (RedCap)	Sì	No	No	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).
	Secure Web Application (RedCap)	Sì	Sì	No	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.
	Secure Web Application (RedCap)	Sì	Sì	No	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.
	Secure Web Application (RedCap)	Sì	Sì	No	Le password degli utenti devono essere memorizzate in una forma "hash".
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.
	Secure Web Application (RedCap)	Sì	No	No	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
	Secure Web Application (RedCap)	Sì	No	Sì	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
	Secure Web Application (RedCap)	No	No	Sì	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.
	Secure Web Application (RedCap)	Sì	Sì	No	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.
	Secure Web Application (RedCap)	Sì	No	No	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	Secure Web Application (RedCap)	Sì	Sì	No	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	Secure Web Application (RedCap)	Sì	No	No	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.
	Secure Web Application (RedCap)	Sì	No	No	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
	Secure Web Application (RedCap)	No	No	Sì	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? Importante

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? Limitato

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatti Potenziali
Dati non esatti e/o non aggiornati

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Minaccia
Errore operativo

Quali sono le fonti di rischio?

Fonte
Fonti umane interne accidentali (es. collaboratori negligenti)

Misure Applicate

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
	Secure Web Application (RedCap)	No	Sì	Sì	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
	Secure Web Application (RedCap)	No	Sì	Sì	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.
	Secure Web Application (RedCap)	No	Sì	Sì	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.
	Secure Web Application (RedCap)	Sì	No	No	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
	Secure Web Application (RedCap)	No	Sì	Sì	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.
	Secure Web Application (RedCap)	Sì	No	No	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	No	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup completi devono essere eseguiti regolarmente.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.
	Secure Web Application (RedCap)	Sì	Sì	No	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
	Secure Web Application (RedCap)	Sì	Sì	No	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Devono essere eseguiti test periodici di penetrazione.
	Secure Web Application (RedCap)	Sì	No	No	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere seguiti standard e pratiche di codifica sicure.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.
	Secure Web Application (RedCap)	Sì	No	No	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.
	Secure Web Application (RedCap)	Sì	Sì	No	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.
	Secure Web Application (RedCap)	No	No	Sì	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

Misure da Applicare

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.
	Secure Web Application (RedCap)	Sì	No	No	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
	Secure Web Application (RedCap)	Sì	No	No	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).
	Secure Web Application (RedCap)	Sì	Sì	No	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.
	Secure Web Application (RedCap)	Sì	Sì	No	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.
	Secure Web Application (RedCap)	Sì	Sì	No	Le password degli utenti devono essere memorizzate in una forma "hash".
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.
	Secure Web Application (RedCap)	Sì	No	No	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
	Secure Web Application (RedCap)	Sì	No	Sì	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
	Secure Web Application (RedCap)	No	No	Sì	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.
	Secure Web Application (RedCap)	Sì	Sì	No	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.
	Secure Web Application (RedCap)	Sì	No	No	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	Secure Web Application (RedCap)	Sì	Sì	No	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	Secure Web Application (RedCap)	Sì	No	No	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.
	Secure Web Application (RedCap)	Sì	No	No	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
	Secure Web Application (RedCap)	No	No	Sì	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate? Limitato

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate? Trascurabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Impatti Potenziali
Costi aggiuntivi

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Minaccia
Errore operativo

Quali sono le fonti di rischio?

Fonte
Eventi tecnologici (es. guasti, malfunzionamenti, etc.)
Fonti umane interne accidentali (es. collaboratori negligenti)

Misure Applicate

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Ruoli e responsabilità relative al trattamento dei dati personali sono chiaramente definite e allocate in accordo con la security policy aziendale
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
	Secure Web Application (RedCap)	No	Sì	Sì	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
	Secure Web Application (RedCap)	No	Sì	Sì	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.
	Secure Web Application (RedCap)	No	Sì	Sì	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.
	Secure Web Application (RedCap)	Sì	No	No	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.
	Secure Web Application (RedCap)	No	Sì	Sì	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.
	Secure Web Application (RedCap)	Sì	No	No	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	No	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup completi devono essere eseguiti regolarmente.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	Sì	Un sistema di monitoraggio dovrebbe generare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.
	Secure Web Application (RedCap)	Sì	Sì	No	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.
	Secure Web Application (RedCap)	Sì	Sì	No	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Devono essere eseguiti test periodici di penetrazione.
	Secure Web Application (RedCap)	Sì	No	No	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere seguiti standard e pratiche di codifica sicure.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.
	Secure Web Application (RedCap)	Sì	Sì	Sì	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.
	Secure Web Application (RedCap)	Sì	No	No	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.
	Secure Web Application (RedCap)	Sì	Sì	No	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
	Secure Web Application (RedCap)	Sì	Sì	Sì	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
	Secure Web Application (RedCap)	No	Sì	Sì	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.
	Secure Web Application (RedCap)	No	No	Sì	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

Misure da Applicare

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.
	Secure Web Application (RedCap)	Sì	No	No	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.
	Secure Web Application (RedCap)	Sì	No	No	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.

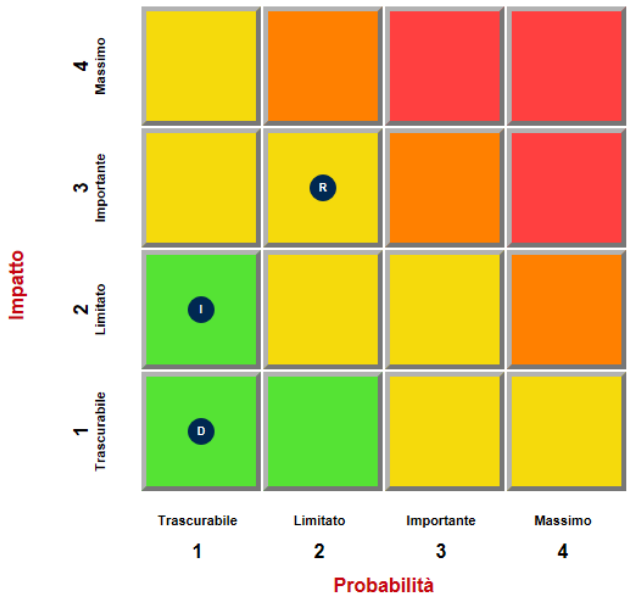
Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	Sì	No	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).
	Secure Web Application (RedCap)	Sì	Sì	No	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.
	Secure Web Application (RedCap)	Sì	Sì	No	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.
	Secure Web Application (RedCap)	Sì	Sì	No	Le password degli utenti devono essere memorizzate in una forma "hash".
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.
	Secure Web Application (RedCap)	Sì	No	No	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.
	Secure Web Application (RedCap)	Sì	No	No	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
	Secure Web Application (RedCap)	Sì	No	Sì	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
	Secure Web Application (RedCap)	No	No	Sì	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.
	Secure Web Application (RedCap)	Sì	Sì	Sì	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.
	Secure Web Application (RedCap)	Sì	Sì	No	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.
	Secure Web Application (RedCap)	No	No	Sì	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbe essere registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.

Categoria Asset	Asset	R	I	D	Misura di Sicurezza
	Secure Web Application (RedCap)	Sì	No	No	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.
	Secure Web Application (RedCap)	Sì	Sì	No	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.
	Secure Web Application (RedCap)	Sì	No	No	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
	Secure Web Application (RedCap)	Sì	Sì	Sì	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	Secure Web Application (RedCap)	Sì	Sì	No	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.
	Secure Web Application (RedCap)	Sì	Sì	No	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	Secure Web Application (RedCap)	Sì	No	No	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).
	Secure Web Application (RedCap)	Sì	Sì	No	Ogni dispositivo dovrebbe essere soggetto ad autenticazione (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale.
	Secure Web Application (RedCap)	Sì	No	No	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
	Secure Web Application (RedCap)	No	No	Sì	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).
	Secure Web Application (RedCap)	Sì	Sì	No	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	Secure Web Application (RedCap)	Sì	Sì	No	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
	Secure Web Application (RedCap)	Sì	Sì	Sì	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? Trascurabile

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Trascurabile

Mappatura del rischio



		Probabilità	Impatto
R	Riservatezza	Limitato	Importante
I	Integrità	Trascurabile	Limitato
D	Disponibilità	Trascurabile	Trascurabile

Pareri DPO/RDP e interessati

Nome/i DPO/RDP	Giorgio Presepio
Tenuto conto di quanto segue	Il trattamento può essere implementato
Specifichi le motivazioni della sua scelta	Ho esaminato la Valutazione d'Impatto sulla Protezione dei Dati (DPIA) relativa al protocollo AI-HOPE. Considerando quanto segue: La conformità del trattamento dei dati ai requisiti del GDPR, in particolare in merito ai principi di liceità, minimizzazione, sicurezza, esattezza e limitazione della conservazione. L'adozione di misure tecniche e organizzative adeguate per garantire la protezione dei dati personali trattati, inclusi la pseudonimizzazione, l'anonimizzazione ove applicabile e il rispetto dei diritti degli interessati. La valutazione dei rischi residui e le azioni messe in atto per ridurre al minimo i rischi per i diritti e le libertà degli interessati. Dichiaro che la presente DPIA è stata valutata positivamente e che le misure proposte sono ritenute sufficienti per garantire un trattamento dei dati conforme al GDPR. Pertanto, esprimo parere favorevole alla prosecuzione delle attività di trattamento dei dati descritte nella DPIA per il progetto AI-HOPE.
Parere degli Interessati	Non è stato chiesto il parere degli interessati
Motivare la mancata richiesta del parere degli interessati	Difficoltà Pratiche e Proporzionalità: La raccolta del parere di tutti gli interessati (pazienti coinvolti nello studio) sarebbe impraticabile e sproporzionata, considerata la numerosità degli interessati e la natura dello studio, che prevede l'analisi di dati retrospettivi raccolti presso varie strutture sanitarie. Molti dei dati trattati riguardano pazienti che potrebbero non essere più reperibili o che hanno concluso il percorso di cura, rendendo impossibile un contatto diretto. Pseudonimizzazione e Misure di Sicurezza: I dati dei pazienti sono trattati in forma pseudonimizzata o anonima, garantendo che non siano direttamente identificabili da parte del personale che esegue l'analisi. Questa misura riduce significativamente i rischi per i diritti e le libertà degli interessati. La gestione sicura dei dati, la limitazione dell'accesso al personale autorizzato e l'adozione di misure tecniche e organizzative adeguate (come il sistema CRF elettronico e la segregazione dei dati) contribuiscono a minimizzare l'impatto del trattamento sui pazienti. Finalità di Ricerca Scientifica e Interesse Pubblico: Lo studio si basa su finalità di ricerca scientifica nell'ambito sanitario, volte a migliorare i trattamenti terapeutici per il carcinoma polmonare metastatico, con potenziali benefici per la salute pubblica e l'avanzamento delle conoscenze mediche. In base all'art. 89 del GDPR, il trattamento dei dati personali per scopi di ricerca scientifica può avvenire anche in assenza del parere diretto degli interessati, purché siano adottate misure di sicurezza adeguate e il trattamento rispetti i principi di minimizzazione dei dati e proporzionalità. Rispetto della Normativa e dell'Accountability del Titolare: L'intero trattamento è stato oggetto di una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) e il protocollo è stato sottoposto a valutazione e approvazione da parte del Comitato Etico competente. Questo garantisce che tutte le

	misure siano state attentamente valutate per proteggere i diritti degli interessati. La trasparenza del trattamento è comunque garantita mediante l'informativa pubblicata sul sito web delle strutture coinvolte per gli interessati ai dati retrospettivi e la raccolta del consenso informato per i pazienti inclusi nella parte prospettica dello studio. Conclusione: La mancata raccolta del parere degli interessati è giustificata dalla difficoltà pratica di contattare gli interessati, dalle misure di sicurezza adottate per garantire la protezione dei loro dati personali, dalla natura scientifica e di interesse pubblico del trattamento, e dal rispetto delle procedure di conformità alla normativa vigente.
Scheda Completata	Sì

Dichiaro che la descrizione del contesto del mio trattamento corrisponde alla realtà.

Dichiaro di essere consapevole dei rischi esistenti in funzione delle misure attualmente implementate o previste.

Convalido le misure correttive indicate.

Mi impegno a implementare quanto prima le misure correttive indicate.