Valutazione d'impatto sulla protezione dei dati (DPIA) sullo Studio clinico osservazionale ALX-TMA-502.

ai sensi dell'art. 35 GDPR.

La revisione è stata redatta dal dipartimento societario competente in materia e concordata con la funzione responsabile della protezione dei dati personali e con il DPO ("Data Protection Officer").

Storico delle revisioni			
Vers.	Data	Motivo della revisione	Autore
1.0	10/02/2025	Prima Emessa	Ufficio compliance

L'ultima revisione sostituisce qualsiasi revisione precedente.

Distribuzione	

INDICE

0 PREMESSA 3

0.1 TITOLARE DEL TRATTAMENTO 3
0.2 PARERE DEL DPO 3
0.3 PARERE DEGLI INTERESSATI 3

1 CONTESTO - PANORAMICA DEL TRATTAMENTO 4

1.1 PANORAMICA DEL TRATTAMENTO 4

2 CONTESTO - DATI, PROCESSI E RISORSE DI SUPPORTO 6

2.1 QUALI DATI SONO TRATTATI 6
2.2 CICLO DI VITA DEL TRATTAMENTO DEI DATI (DESCRIZIONE FUNZIONALE) 7
2.3 QUALI SONO LE RISORSE DI SUPPORTO AI DATI 7

3 PRINCIPI FONDAMENTALI 8

3.1 PROPORZIONALITÀ E NECESSITÀ 8
3.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI 9

4 ANALISI DEL RISCHIO 13

4.1 MISURE ESISTENTI O PIANIFICATE 13
4.2 ACCESSO ILLEGITTIMO AI DATI - VIOLAZIONE DI RISERVATEZZA 17
4.3 MODIFICHE INDESIDERATE DEI DATI 17
4.4 PERDITA DI DATI 18

5 VALUTAZIONE DEL RISCHIO 19

5.1 PANORAMICA DEI RISCHI 19
5.2 GRAVITÀ DEL RISCHIO 20
5.3 VALUTAZIONE RESIDUA DEL RISCHIO 21

6 PIANO AZIONE DI RIMEDIO 22

0 PREMESSA

0.1 Titolare del trattamento

La società Alexion è titolare del trattamento oggetto della presente DPIA. Nel rispetto dell'art. 35 del GDPR, quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

0.2 Parere del DPO

La DPIA è stata svolta conformemente all'articolo 35 del GDPR. Le conclusioni raggiunte danno un profilo di rischio basso. La società dimostra un livello di conformità al GDPR molto soddisfacente. Si raccomandano le azioni seguenti:

-Aggiornamento della valutazione d'impatto su base periodica, ogni 24 mesi, o prima in caso di evoluzione organizzativa del processo o dell'evoluzione della normativa.

-Realizzazione della formazione ai dipendenti coinvolti nel processo con periodicità annuale.

0.3 Parere degli interessati

Non è stato chiesto il parere degli interessati. Lo studio è realizzato per una finalità di ricerca scientifica e prevede la raccolta dei dati personali in maniera retrospettiva. A tale riguardo certi pazienti possono essere deceduti o risultare non reperibili.

1 CONTESTO - PANORAMICA DEL TRATTAMENTO

1.1 Panoramica del trattamento

1.1.1 Descrizione del settore di attività

La presente DPIA è svolta da Alexion Pharma Italy Srl (di seguito "**Alexion**" o "**Società**") ed ha ad oggetto lo studio clinico osservazionale multicentrico ALX-TMA-502, uno studio globale secondario sull'utilizzo dei dati nel mondo reale su partecipanti pediatrici e adulti affetti da microangiopatia trombotica (TMA) dopo trapianto di cellule staminali ematopoietiche (HSCT).

Alexion è parte di un gruppo multinazionale ed opera sul territorio italiano. La società è impegnata nella ricerca di soluzioni in diverse malattie rare attraverso la scoperta, lo sviluppo e l'accesso a farmaci in grado di cambiare la vita dei pazienti. A tale proposito, promuove studi clinici rigorosi, allo scopo di ottenere l'approvazione all'utilizzo di farmaci a cura di malattie rare da parte delle autorità regolatorie di tutto il mondo.

1.1.2 Descrizione dello studio clinico e del trattamento in considerazione.

Lo scopo del presente studio è valutare i risultati di sopravvivenza globale nei partecipanti con diagnosi di HSCT-TMA che non hanno ricevuto terapia con inibitori del complemento e nei pazienti trattati con eculizumab. Questo studio fornirà dati di controllo storici sul farmaco ravulizumab nel trattamento di partecipanti pediatrici affetti da TMA. Lo studio si rivolge a pazienti adulti e minorenni, 60 pazienti in totale in Italy, circa 25 pazienti pediatrici e 35 adulti.

Questo studio è necessario per il titolare del trattamento al fine di confrontare i risultati di pazienti affetti dalla malattia che hanno seguito una terapia definita e di altri pazienti affetti dalla stessa malattia che non hanno beneficiato di tale terapia.

I risultati della ricerca saranno utilizzati per fornire dati di controllo storici per lo studio ALXN1210-TMA-314 e la contestualizzazione nel mondo reale per la fase 2 dello studio ALXN1210-TMA-313. I risultati potrebbero anche essere pubblicati su riviste scientifiche o utilizzati per scopi didattici. Inoltre, lo studio retrospettivo verrà utilizzata per la costruzione del dossier di registrazione del farmaco ravulizumab.

Lo studio si svolge a livello globale nel modo seguente:

Due gruppi di partecipanti provenienti da circa 70 centri studio in 11 paesi e/o dal repository di dati TriNetX partecipano allo studio. I partecipanti devono avere ≥ 28 giorni di età al momento della diagnosi HSCT-TMA.

1a coorte: 250 partecipanti (150 partecipanti adulti e 100 partecipanti pediatrici) che non hanno ricevuto terapia con inibitori del complemento.

2a coorte: 100 partecipanti che hanno ricevuto il medicinale eculizumab off-label per HSCT-TMA.

In Italia, lo studio coinvolge 9 centri, con la seguente previsione di partecipanti:

CENTRI	1 COORTE PREVISIONE DI 35 PARTECIPANTI	2 COORTE PREVISIONE DI 25 PARTECIPANTI

Firenze	5	0
Brescia	1	4
Torino	0	6
Napoli	6	4
Roma	0	4
Torrette di Ancona	7	0
Genova	6	4
Lazio	4	2
Pavia	6	1

Il trattamento in oggetto prevede la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, la modifica, l'estrazione, la consultazione, l'analisi, la comunicazione, l'uso, il raffronto, la cancellazione e la distruzione del dato.

Il trattamento prevede anche la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, la modifica, l'estrazione, la consultazione dei dati personali dei pazienti, medici, infermieri e altri professionisti inclusi nello studio clinico oltre che di dipendenti dei fornitori delle varie parti interessate allo studio clinico, come la CRO.

In sintesi, le operazioni di elaborazione dei dati sono: analisi, archiviazione, reporting, monitoraggio, condivisione, riutilizzo tramite anonimizzazione, conservazione, archiviazione ed eliminazione.

1.1.3 Distribuzione delle responsabilità connesse al trattamento

Alexion, in qualità di sponsor dello studio, è titolare del trattamento dei dati personali in oggetto; nonostante parte delle attività venga affidata a fornitori di servizi esterni, la determinazione delle modalità e degli scopi del trattamento è in capo a Alexion, che determina l'oggetto e l'ambito dello studio clinico e ne valuta gli esiti.

Il dipartimento aziendale maggiormente coinvolto nelle operazioni di trattamento è il dipartimento R&D.

Lo studio è di portata globale, ma ogni paese gestisce la partecipazione locale di Alexion.

I fornitori terzi come la CRO (Clinical Research Organizations) agiscono come Responsabili del trattamento dei dati.

Gli ospedali/siti di studio: sono titolari autonomi del trattamento dei dati.

1.1.4 Standard applicabili al trattamento

- Prescrizioni e delle Regole deontologiche, che costituiscono condizione essenziale di liceità e correttezza dei trattamenti (art. 2-quater del Codice e art. 21, comma 5, del d.lgs. 10 agosto 2018, n. 101).
- Codice privacy art. 110 e successive modifiche: “Ricerca medica, biomedica ed epidemiologica”.
- Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019 [9091942]
- Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21 comma 1 del d.lgs. 10 agosto 2018 n. 101 e successive modifiche.
- Autorizzazione n. 9/2016 - Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica - 15 dicembre 2016 [5805552]. Garante della Privacy.

Valutazione: Accettabile

2 CONTESTO - DATI, PROCESSI E RISORSE DI SUPPORTO

2.1 Quali dati sono trattati

2.1.1 Categorie di dati trattati

Gli interessati al trattamento sono in primo luogo i pazienti coinvolti nello studio, i cui dati vengono raccolti per verificare la sicurezza e l'efficacia del farmaco oggetto dello studio.

Vengono altresì trattati i dati riferiti al personale medico e ai professionisti incaricati di svolgere lo studio attraverso società incaricate. Inoltre, il trattamento riguarda anche i dati personali dei dipendenti o collaboratori dei fornitori coinvolti.

Le categorie di dati personali coinvolti sono le seguenti:

• Alexion e i dati di contatto dei dipendenti dei fornitori terzi applicabili: condivisi con gli operatori sanitari (HCP) secondo necessità per lo studio.

• Informazioni di contatto degli HCP: utilizzate per facilitare lo studio.

• Dati codificati del paziente: dati sanitari dei partecipanti allo studio.

I partecipanti allo studio devono essere considerati “soggetti vulnerabili” (ai fini della disciplina sulla protezione dei dati personali e del GDPR), in quanto la particolare patologia da cui sono afflitti li espone a rischi maggiori soprattutto nei confronti del titolare del trattamento con il quale sussiste un rapporto

asimmetrico, giustificato dalla possibilità di guarigione o miglioramento delle proprie condizioni fornita dal farmaco sperimentale.

Il programma clinico in esame coinvolge soggetti minorenni.

Con riferimento ai professionisti e collaboratori coinvolti a vario titolo vengono trattati i dati anagrafici, quelli di contatto, quelli relativi alla formazione e alla competenza professionale (es. CV) e dati professionali.

Il titolare del trattamento tratta dati relativi alla salute e allo stile di vita dei soggetti. In particolare, viene raccolta l'anamnesi del soggetto coinvolto e viene tenuta traccia dell'evoluzione del quadro clinico. Il set di dati è costituito da dati clinici come delineato nel protocollo dello studio clinico. Si tratta di: Codici paziente, informazioni demografiche (tra cui sesso, anno di nascita, razza, gruppo etnico), storia medica, segni vitali (altezza, peso).

2.2 Ciclo di vita del trattamento dei dati (descrizione funzionale)

Il protocollo dello studio, la gestione dei dati (incluso lo sviluppo dell'Electronic Data Capture (EDC) utilizzando l'applicazione Medidata Rave), l'analisi dei dati e il rapporto finale dello studio saranno gestiti dal team Alexion, con il supporto di Fortrea Inc, contratto come fornitore di terze parti CRO clinico.

Alexion raccoglierà e utilizzerà i dati personali dei pazienti (partecipanti allo studio), degli operatori sanitari e di terze parti (personale).

Lo studio e la raccolta di tutti i dati saranno condotti in modo da garantire la riservatezza e la privacy, la protezione della reputazione e la non stigmatizzazione dei partecipanti allo studio e che nessuna informazione verrà utilizzata a danno di queste persone, in conformità con la normativa sulla protezione dei dati personali europea e specifica ad ogni paese incluso, il codice Farmindustria e la normativa sugli studi clinici. Le informazioni relative ai partecipanti allo studio verranno comunicate ai soggetti autorizzati solo se anonimi, senza l'uso di iniziali o altre indicazioni che possano identificarli e nel rigoroso rispetto della normativa locale sulla protezione dei dati in vigore.

I dati verranno poi conservati per venti cinque anni dopo il termine dello studio per finalità di verifica della qualità della ricerca, al termine del quale lo sponsor provvederà alla loro distruzione.

2.3 Quali sono le risorse di supporto ai dati

- Email aziendale
- eTMF and Clinical Trial Management System (CTMS): electronic Master File : Veeva Clinica Vault
- Software Medidata utilizzabile dai siti

Valutazione: Accettabile

3 PRINCIPI FONDAMENTALI

3.1 Proporzionalità e necessità

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

I dati sono trattati per finalità di ricerca scientifica. Alexion persegue legittimamente finalità di ricerca scientifica come da statuto e oggetto sociale. Le finalità sono rese esplicite perché dichiarate nelle informative e nei documenti predisposti per la ricerca clinica.

Valutazione: Accettabile

3.1.2 Quali sono le basi legali che rendono lecito il trattamento?

Trattamento di dati personali	Base giuridica
L'elaborazione delle informazioni di contatto di lavoro e delle qualifiche necessarie per lo svolgimento dello studio del personale Alexion.	Base contrattuale Art. 6 1) b) GDPR
L'elaborazione delle informazioni di contatto di lavoro di base necessarie per consentire lo svolgimento dello studio e per l'adempimento degli obblighi contrattuali del personale delle terze parti coinvolte.	Interesse legittimo Art. 6 1) f) GDPR
L'elaborazione delle informazioni di contatto e delle qualifiche necessarie per lo svolgimento dello studio del personale medicale.	Interesse legittimo Art. 6 1) f) GDPR
L'elaborazione dei dati sanitari codificati/pseudonimizzati dei partecipanti allo studio è necessaria per lo svolgimento dello studio. Non verranno raccolti o elaborati dati personali identificabili del paziente.	Consenso dell'interessato Art. 6 1) a) GDPR quando possibile Interesse legittimo Art. 6 1) f) GDPR

Valutazione: Accettabile

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

I dati utilizzati seguono un protocollo di ricerca rigido che ne definisce gli obiettivi e il disegno, pertinenti con il perimetro dello studio.

Valutazione: Accettabile

3.1.4 I dati sono esatti e aggiornati?

I dati verranno raccolti in ciascun sito di studio dagli investigatori del sito e quindi registrati nella eCRF dal personale del sito delegato. La robustezza, l'accuratezza e l'integrità dei dati raccolti saranno monitorate dal personale specializzato secondo un piano di monitoraggio definito. La qualità dei dati sarà inoltre valutata dal data manager secondo un Piano di gestione dei dati predefinito.

Valutazione: Accettabile

3.1.5 Qual è il periodo di conservazione dei dati?

I dati saranno conservati per il tempo necessario allo svolgimento della ricerca clinica e poi per un periodo non superiore a venti cinque anni dal suo termine.

Valutazione: Accettabile

3.2 Misure a tutela dei diritti degli interessati

3.2.1 Come sono informati del trattamento gli interessati?

Le diverse categorie di interessati sono informate tramite le seguenti informative privacy:

1) Informativa rivolta al Partecipante alla Sperimentazione Clinica (per Adulti e Bambini)

2) Informativa rivolta a professionisti dell'ambiente medico (investigatore principale (PI) e operatori sanitari (HCP)

3) Informativa rivolta ai dipendenti interni di Alexion

I siti che conducono gli studi clinici globali contengono una propria Informativa sulla privacy per il trattamento dei dati personali.

In caso di impossibilità di comunicare l'informativa privacy e raccogliere il relativo consenso per partecipanti deceduti o che non sono più rintracciabili si farà ricorso alle procedure dell'Art 110 del D. Lgs. 196/2003 e all'autorizzazione del Garante della Privacy : Autorizzazione n. 9/2016 - Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica - 15 dicembre 2016 [5805552].

Per l'insieme dei partecipanti, l'informativa privacy è disponibile sul sito internet di Alexion.

Valutazione: Accettabile

3.2.2 Ove applicabile come si ottiene il consenso degli interessati?

L'informativa privacy e il consenso al trattamento dei dati personali viene comunicato al paziente da parte del personale del centro ospedaliero che partecipa allo studio retrospettivo.

Per i pazienti pediatrici, i genitori o il tutore forniscono il consenso. Il paziente pediatrico riceve anche tutte le informazioni pertinenti e riceve un documento di "assenso", che include informazioni comprensibili per la sua età.

I dati dei pazienti saranno trattati sulla base giuridica del consenso ai sensi degli artt. 6(1)(a) e 9(2)(a) GDPR. Il consenso è facoltativo e il suo diniego comporterà l'impossibilità di partecipare allo Studio Clinico.

Il paziente potrà revocare il consenso, in qualsiasi momento ed interrompere la sua partecipazione allo Studio Clinico senza dover fornire alcuna giustificazione. In tal caso, non saranno raccolti ulteriori dati. I dati raccolti prima della revoca del consenso saranno conservati in quanto trattati con una base giuridica valida.

Nel caso in cui risultasse "impossibile" o implicasse "uno sforzo sproporzionato" o rischiasse di "rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca" (cfr. art. 110, comma 1, secondo periodo, del Codice Privacy) informare gli interessati e raccogliere il loro consenso, la modifica dell'art. 110 del Codice Privacy – rubricato "Ricerca medica, biomedica ed epidemiologica" – in vigore dal 23 aprile 2024, prevede in questi casi che il consenso non costituisce la base giuridica del trattamento anche senza approvazione preventiva del Garante.

Ai sensi dell'autorizzazione n. 9/2016 del Garante della Privacy: "VISTI gli specifici provvedimenti di autorizzazione rilasciati dall´Autorità, ai sensi degli artt. 110, comma 1 (ultima parte) e 41 del Codice Privacy, con i quali è stata autorizzata, anche in assenza del consenso degli interessati, la conduzione di studi, non aventi significativa ricaduta personalizzata sull´interessato, effettuati con dati raccolti in precedenza per finalità di tutela della salute degli interessati o ricavati da campioni biologici prelevati in precedenza per le stesse finalità; ciò, in quanto, a causa di comprovate particolari ragioni, è stata documentata l´impossibilità di fornire loro l´informativa sul trattamento dei dati e il relativo programma di ricerca ha ricevuto un motivato parere favorevole del comitato etico territorialmente competente".

Nel contesto dello studio, la popolazione di pazienti potrebbero comprendere pazienti con malattia allo stadio terminale. Una parte dei pazienti potrebbe essere deceduta al momento dell'estrazione dei dati. In questo contesto il paziente potrebbe non essere raggiungibile.

A tale riguardo poiché numerosi pazienti potrebbero essere deceduti o risultatare non reperibili, non essendo possibile informarli e raccogliere il relativo consenso si farà ricorso alle procedure dell'Art 110 del D. Lgs. 196/2003 e all'autorizzazione generale del Garante.

Per motivi di completezza, è stato realizzato ogni ragionevole sforzo per contattare i partecipanti allo studio, ad esempio verificando se ancora in vita, consultando la sua cartella clinica, contattando i numeri telefonici eventualmente disponibili o ottenendo informazioni di contatto da registri anagrafici e/o sanitari, se risulti deceduta o con informazioni di contatto non raggiungibili al momento dell'iscrizione allo studio in questione.

Se gli sforzi ragionevoli di ricerca compiuti per verificare se la persona è ancora in vita o raggiungibile al momento dell'iscrizione allo studio in questione non hanno reso possibile mettersi in contatto con il paziente per informarlo e raccogliere il suo consenso, i dati del paziente in questione verranno utilizzati senza raccogliere un consenso privacy come previsto dai testi di legge citati sopra.

Valutazione: Accettabile

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

Gli interessati possono esercitare il diritto di accesso scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy di Alexion, reperibile sia nell'informativa privacy che nel sito web istituzionale.

Il diritto alla portabilità non è applicabile per tale attività di trattamento. Alexion ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

Valutazione: Accettabile

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

Gli interessati possono esercitare il diritto di accesso scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy di Alexion, reperibile sia nell'informativa privacy che nel sito web istituzionale.

In caso di richiesta di esercizio di diritto GDPR, Alexion ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

Valutazione: Accettabile

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

Gli interessati possono esercitare il diritto di accesso scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy di Alexion, reperibile sia nell'informativa privacy che nel sito web istituzionale.

In caso di richiesta di esercizio di diritto GDPR, Alexion ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

Valutazione: Accettabile

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

Il trattamento in esame prevede il coinvolgimento di numerosi soggetti esterni. Il titolare del trattamento si avvale di una o più CRO, individuate sulla base delle specifiche competenze di ognuna e delle esigenze dello studio. Le terze parti coinvolte nel trattamento sono state contrattualizzate con accordi ai sensi dell'art. 28 GDPR. Nel trattamento sono coinvolti i seguenti responsabili:

Nome terza parte	Attività	Categorie di dati trattati
IQVIA RDS Inc	CRO. Conduce le attività di studio: gestione TMF, gestione del sito, monitoraggio clinico, invii EC/IRB	Dipendenti CRO e Alexion, operatori sanitari e partecipanti allo studio.

Fortrea Inc	La finalizzazione del protocollo dello studio, la gestione dei dati (incluso lo sviluppo di un modulo elettronico per la segnalazione dei casi [eCRF]), l'analisi dei dati, la preparazione delle pubblicazioni e il rapporto finale dello studio.	Dipendenti Alexion, operatori sanitari e partecipanti allo studio.
Parexel International LLC	Attività di redazione di materiale medico.	Dipendenti Alexion, e informazioni aggregate dei partecipanti allo studio.
Medidata Solutions Inc	Elaboratore dati, elabora i dati personali solo dietro istruzioni dirette dello Sponsor, in conformità con le leggi locali applicabili e i protocolli approvati dallo Sponsor.	Dipendenti CRO e Alexion, operatori sanitari e partecipanti allo studio.

Alexion condivide i dati codificati con i suoi partner di ricerca e fornitori di servizi per scopi di sviluppo dello studio, i quali sono vincolati da accordi contrattuali ad agire in qualità di Responsabili del trattamento dei dati.

Valutazione: Accettabile

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

Il trattamento oggetto di analisi comporta il trasferimento di dati oltre lo Spazio Economico Europeo e verso gli Stati Uniti dove sono ospitati i sistemi. Allo stato, i paesi destinatari dei dati personali risultano essere:

Le società IQVIA RDS Inc, Parexel International LLC e Medidata Solutions Inc sono iscritte al programma di garanzia Data Privacy Framework che regola il trasferimento dei dati personali tra l'Unione Europea e gli Stati Uniti. La sede della società capo gruppo di Alexion è sita negli USA.
La società Fortrea Inc. non è iscritta al programma di garanzia Data Privacy Framework. Ha valutato che non è necessario completare una valutazione d'impatto sul trasferimento di dati poiché il personale di Fortrea Inc. utilizza i sistemi e gli strumenti di Alexion e non "ospita" dati al di fuori dei sistemi e degli strumenti di Alexion.

I siti si trovano nei seguenti paesi: Brasile, Belgio, Francia, Grecia, Italia, Israele, Giappone, Spagna, Corea del Sud, Regno Unito, Stati Uniti

Tuttavia, la presente valutazione d'impatto è specificatamente realizzata per l'Italia.

Valutazione: Accettabile

4 ANALISI DEL RISCHIO

4.1 Misure esistenti o pianificate

Misura di sicurezza	Descrizione	Valutazione
Crittografia	Le politiche di crittografia e trasferimento di Medidata si applicano a tutti gli scenari, garantendo la protezione dei dati sul dispositivo e in transito, indipendentemente dall'hardware di cui si tratta. Le cartelle cliniche usano di crittografia. Tutti i dati vengono crittografati quando sono al riposo e in transito tramite TLS v 1.2 con AES-256 (al livello di crittografia più alto consentito dalla legge).	Accettabile
Controllo accessi logici	Tutte le applicazioni/sistemi chiave utilizzati per la conduzione di studi/sperimentazioni cliniche sono registrati nell'inventario delle risorse aziendali e dispongono della necessaria valutazione del rischio aziendale. I dati personali dei pazienti verranno raccolti nella eCRF. L'accesso alla eCRF sarà possibile solo con account personali e tali account saranno concessi solo al personale dello studio che ha firmato un accordo di riservatezza, lavora sotto la clausola sulla privacy del contratto di servizio tra Alexion e la CRO e ha una reale necessità di accedere al sistema (es. Alexion CRA, gestori dei dati). Gli accessi sono autorizzati dalla funzione che coordina lo studio. Nel sito dello studio, il nome e i dettagli di contatto del partecipante allo studio clinico saranno accessibili al medico dello studio e al team di studio per condurre lo studio. Il personale non medico che opera per conto dello sponsor ed è vincolato da un obbligo di riservatezza nonché le Autorità sanitarie e i Comitati etici a cui potrà essere dato accesso anche a tali dati solo per verificare che lo studio sia condotto nel rispetto dei requisiti legali e di qualità.	Accettabile

	I dati personali dei pazienti verranno inoltre archiviati nell'Investigator Site File [ISF], come previsto dalle normative vigenti e dagli standard di ricerca clinica; l'ISF è cartaceo ed è accessibile solo al personale dello studio presso la sede dello studio e alle CRA (ai fini delle attività di monitoraggio, come richiesto dagli attuali standard per la ricerca clinica e dettagliato in un Piano di monitoraggio). I dati personali del personale dello studio (operatori sanitari e personale della CRO) saranno trattati solo dalle persone coinvolte nello studio all'interno di Alexion e della CRO.	
Tracciabilità	Gli accessi alle cartelle cliniche elettroniche sono registrati in automatico con l'indicazione dell'orario, del giorno, dell'unità operativa e dell'operatore che vi ha avuto accesso.	Accettabile
Archiviazione	Veeva Clinica Vault (VCV) che è il Trial Master File elettronico (eTMF) + Clinical Trial Management System (CTMS) Altri sistemi/applicazioni chiave sono identificati nell'"Inventario dei sistemi informatici di ricerca e sviluppo" - a cui è possibile accedere tramite procedura interna.	Accettabile
Minimizzazione dei dati	Il protocollo condiviso e autorizzato con il Comitato Etico stabilisce sia il set di informazioni cui si può accedere, sia o il dataset di informazioni che devono essere poi successivamente raccolte, catalogate e valutate, oltre anche all'arco temporale di analisi. I dati trattati sono soltanto quelli strettamente necessari per le finalità perseguite.	Accettabile
Lotta contro il malware	L'intranet è protetta da sistemi di firewall aziendale: gli unici dispositivi autorizzati a poter aprire canali di comunicazione nell'intranet aziendale sono quelli preventivamente registrati e autorizzati (solamente dispositivi aziendali).	Accettabile
Gestione postazioni	Le postazioni utilizzate sono principalmente in dominio aziendale e le misure adottate sono quelle previste da regolamenti e policy aziendali. I dispositivi esterni e personali non possono ottenere l'accesso all'intranet aziendale.	Accettabile
Backup	Tutti i principali tipi di sistemi/applicazioni utilizzati presso Alexion per la gestione degli studi dispongono di sistemi	Accettabile

	di housing e di backup controllati e approvati. Sono in vigore contratti con fornitori/venditori di sistemi e applicazioni che delineano le modalità di sicurezza delle informazioni come l'accesso all'hosting/ accordi di backup e disaster recovery. Il sistema di gestione Medidata effettua un backup del data base dello studio clinico. Il backup per il ripristino di emergenza si trova a Francoforte, in Germania.	
Sicurezza dei canali informatici	La rete aziendale è protetta da sistemi di firewall. Solo i dispositivi registrati possono accedere alla rete aziendale. Alexion utilizza meccanismi di trasferimento sicuri per condividere o fornire l'accesso ai dati a terzi come autorità esterne/comitati esterni. Tali meccanismi di trasferimento/accesso vengono esaminati dalla Sicurezza IT a seguito del processo di Valutazione della Sicurezza IT. Lo sponsor può condividere solo dati codificati con i suoi partner di ricerca e fornitori di servizi ai fini del programma di sviluppo del farmaco. Le politiche di accesso controllato e autenticazione fanno parte delle misure tecniche e organizzative richieste e concordate (per contratto) che devono essere applicate da queste parti. Al fine di garantire una corretta condotta e risultati accurati dello studio e ottenere l'autorizzazione alla commercializzazione del farmaco, lo sponsor condividerà i dati codificati con le autorità e i comitati etici utilizzando metodi di trasferimento sicuri.	Accettabile
Controllo degli accessi fisici	L'accesso ai locali protetto con chiusura a chiave e con personale di reception. Nel sito dello studio, il nome e i dettagli di contatto del partecipante allo studio clinico saranno accessibili al medico dello studio e al team di studio per condurre lo studio. Il personale non medico che opera per conto dello sponsor ed è vincolato da un obbligo di riservatezza nonché le Autorità sanitarie e i Comitati etici a cui potrà essere dato accesso anche a tali dati solo per verificare che lo studio sia condotto nel rispetto dei requisiti legali e di qualità.	Accettabile
Politica di tutela della Privacy	Alexion è dotata di una politica generale sulla tutela dei dati personali che stabilisce in maniera chiara ruoli, regole e responsabilità per il trattamento dei dati personali all'interno dell'azienda e del gruppo.	Accettabile

	Il personale non medico che opera per conto dello sponsor ed è vincolato da un obbligo di riservatezza nonché le Autorità sanitarie e i Comitati etici a cui potrà essere dato accesso anche a tali dati solo per verificare che lo studio sia condotto nel rispetto dei requisiti legali e di qualità.	
Integrare la protezione della privacy nei progetti	Alexion applica il principio di protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita. Per impostazione predefinita, i dati vengono trasmessi non appena vengono inviati e i dati trasmessi con successo vengono cancellati dal dispositivo.	Accettabile
Gestire gli incidenti di sicurezza e le violazioni di dati personali	Esiste un'organizzazione operativa al riguardo (procedura interna, definizione delle responsabilità, piano di reazione, informazione ai dipendenti, registro delle violazioni). Sono in place i sistemi di resilienza aziendale per prevenire eventuali attacchi informatici.	Accettabile
Gestione del personale	Il personale è debitamente formato con cadenza periodica sulla normativa in materia di protezione dei dati personali, con un focus specifico in funzione dei trattamenti svolti e dei sistemi di sicurezza da osservare. Il personale dei siti che utilizza Medidata Rave per la raccolta e l'elaborazione dei dati degli studi clinici è formato su come utilizzarlo e i diritti di accesso sono rigorosamente controllati. Un accordo di riservatezza è stato stipulato tra Alexion e i fornitori terzi e sarà stipulato tra la CRO (per conto di Alexion) e gli investigatori.	Accettabile
Pseudonimizzazione	The Study Site shares participant clinical data with Alexion but only after it has been coded: a correlating patient number is created through Medidata. Each participant is provided with a unique identifier code known as patient code. This is done by the study doctor who keeps the link between the name/ contact details and the code to ensure patient confidentiality.	Accettabile
Vigilanza sulla protezione dei dati	Il consiglio di amministrazione della società ha designato un DPO che svolge attività di vigilanza e controllo dell'applicazione della normativa sulla protezione dei dati. Il gruppo Alexion ha un ufficio Privacy che coordina i DPO dei diversi paesi.	Accettabile

4.2 Accesso illegittimo ai dati - Violazione di riservatezza

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

Gli impatti principali sono alti e corrispondono alla perdita di riservatezza, di controllo sull'utilizzo dei dati e il rischio di re-identificazione.

4.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le minacce possono essere di diversi tipi, come la perdita o il furto di dispositivo elettronico utilizzato per la gestione dello studio, il recupero dei codici e della relativa identità dei partecipanti allo studio. Il recupero delle chiave di crittografia.

4.2.3 Quali sono le fonti di rischio?

Le fonti di rischio sono di tipo umano e potrebbero consistere in un attacco informatico, un comportamento inappropriato del personale coinvolto.

4.2.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Le misure di sicurezza e i fondamenti di liceità individuati sono idonei a ridurre il rischio di un accesso da parte di soggetti non autorizzati ai dati. La cifratura delle informazioni, la protezione degli archivi sia cartacei che digitali, la gestione postazioni, la sicurezza dei canali informatici, il controllo degli accessi fisici, la vigilanza sulla protezione dei dati e la pseudonimizzazione mitigano il potenziale rischio.

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

Limitata, in merito alle misure di minimizzazione, di pseudonimizzazione e di crittografia implementate.

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

Limitata, Date le misure di minimizzazione, di pseudonimizzazione, date le politiche privacy, la politica degli accessi logici il rischio di perdita della riservatezza nonché di perdita di controllo sull'utilizzo dei dati, il rischio risulta limitato.

Valutazione: Accettabile

4.3 Modifiche indesiderate dei dati

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

Nessun impatto individuato per l'interessato, trattandosi di studio retrospettivo.

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

Le minacce potrebbero essere ricondotte ad un'errata compilazione della CRF o un'errata elaborazione del dataset.

4.3.3 Quali sono le fonti di rischio?

Comportamento inappropriato del personale esterno, accesso ai dati da parte di personale che non ha ricevuto una formazione adeguata.

4.3.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Le misure di sicurezza come il backup, il controllo degli accessi e la gestione del personale possono mitigare il potenziale rischio.

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

Trascurabile, un eventuale modifica indesiderata dei dati della ricerca avrebbe un impatto sullo studio nel suo insieme ma nessuno sugli interessati.

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

Trascurabile. Date le misure di gestione del personale, le politiche privacy e il controllo degli accessi logici, la probabilità di accadimento è improbabile.

Valutazione: Accettabile

4.4 Perdita di dati

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

Gli impatti principali sono alti e corrispondono alla perdita di riservatezza, di controllo sull'utilizzo dei dati e il rischio potenziale di re-identificazione.

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

Le minacce possono essere di diversi tipi, come la perdita o il furto di dispositivo elettronico utilizzato per la gestione dello studio, il recupero dei codici e della relativa identità dei partecipanti allo studio. Il furto delle chiave di crittografia.

4.4.3 Quali sono le fonti di rischio?

Le fonti di rischio sono di tipo umano o naturali. Essi potrebbero consistere in un attacco informatico, un comportamento inappropriato del personale coinvolto oppure un virus informatico. Le fonti di rischio naturali potrebbero essere un incendio o un'alluvione.

4.4.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Le misure di sicurezza e i fondamenti di liceità individuati sono idonei a ridurre il rischio di un accesso da parte di soggetti non autorizzati ai dati. La cifratura e la pseudonimizzazione delle informazioni, la protezione degli archivi sia cartacei che digitali, la gestione postazioni, la sicurezza dei canali informatici, la lotta contro il malware, il controllo degli accessi fisici, la vigilanza sulla protezione dei dati e la gestione degli incidenti di sicurezza e le violazioni dei dati personali mitigano fortemente il potenziale rischio.

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

Limitata, Data la natura retrospettiva degli studi, le misure di minimizzazione, di archiviazione, di sicurezza dei canali informatici e fisiche, delle politiche di tutela della privacy, delle politiche di gestione degli incidenti di sicurezza e violazione dei dati personali.

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

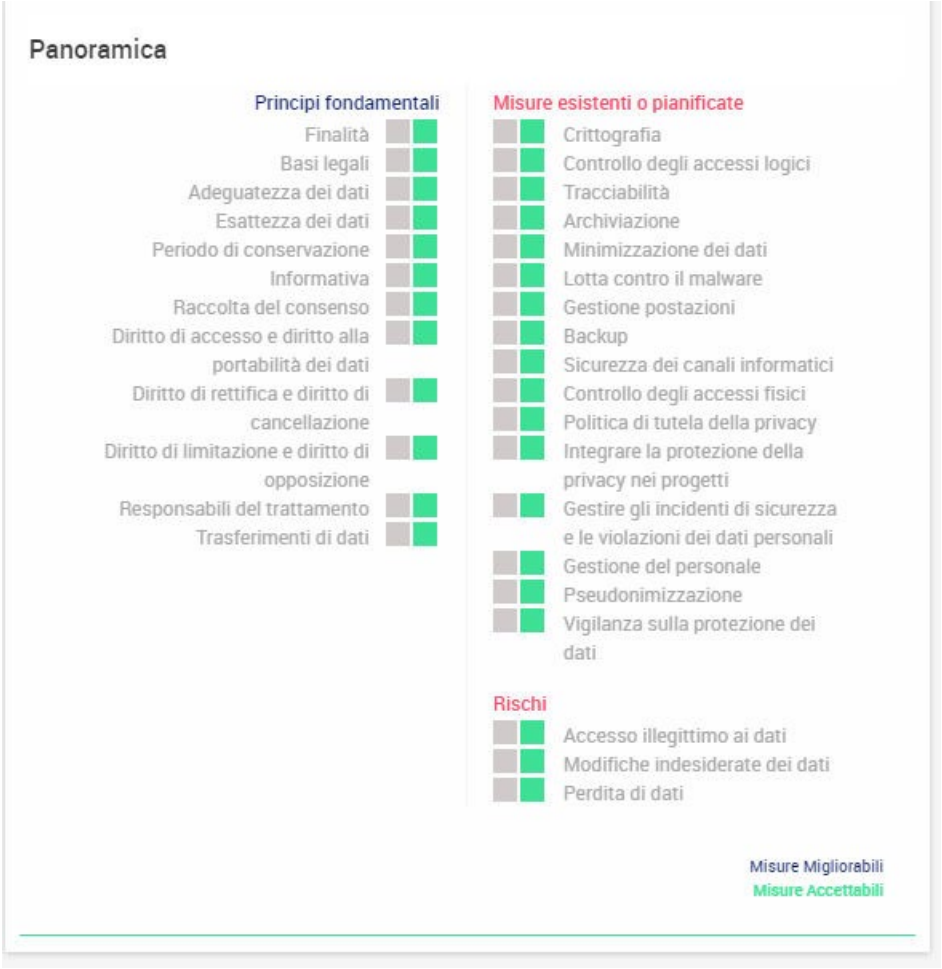
Limitata, Date le misure di minimizzazione, le politiche privacy, la procedura di gestione degli incidenti di sicurezza e la politica degli accessi logici e fisici, il rischio di perdita di dati risulta limitato anche se si raccomanda di porre molta attenzione al processo di gestione degli incidenti di sicurezza e di gestione degli accessi fisici e logici.

Valutazione: Accettabile

5 VALUTAZIONE DEL RISCHIO

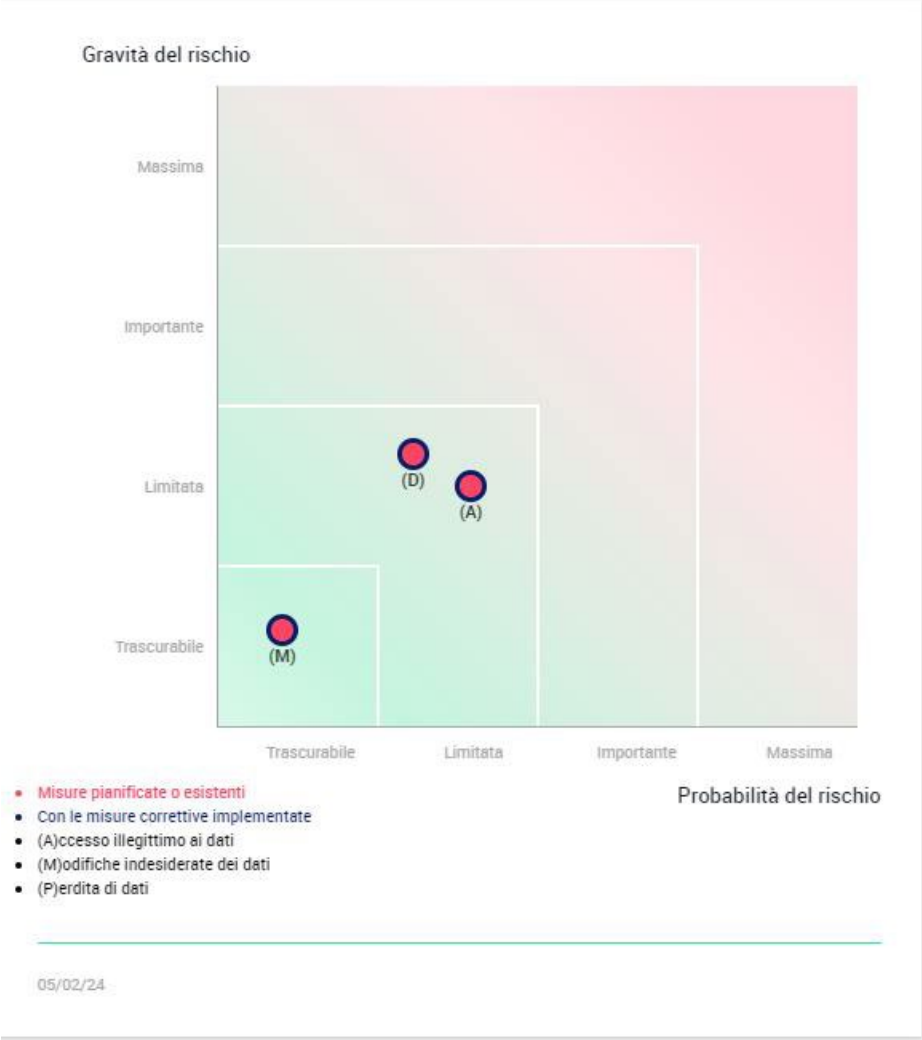
5.1 Panoramica dei rischi

L'analisi realizzata indica il rispetto dei principi e l'applicazione di idonee misure di sicurezza per la protezione dei dati personali coinvolti nello studio da parte dell'azienda sponsor dello studio clinico.



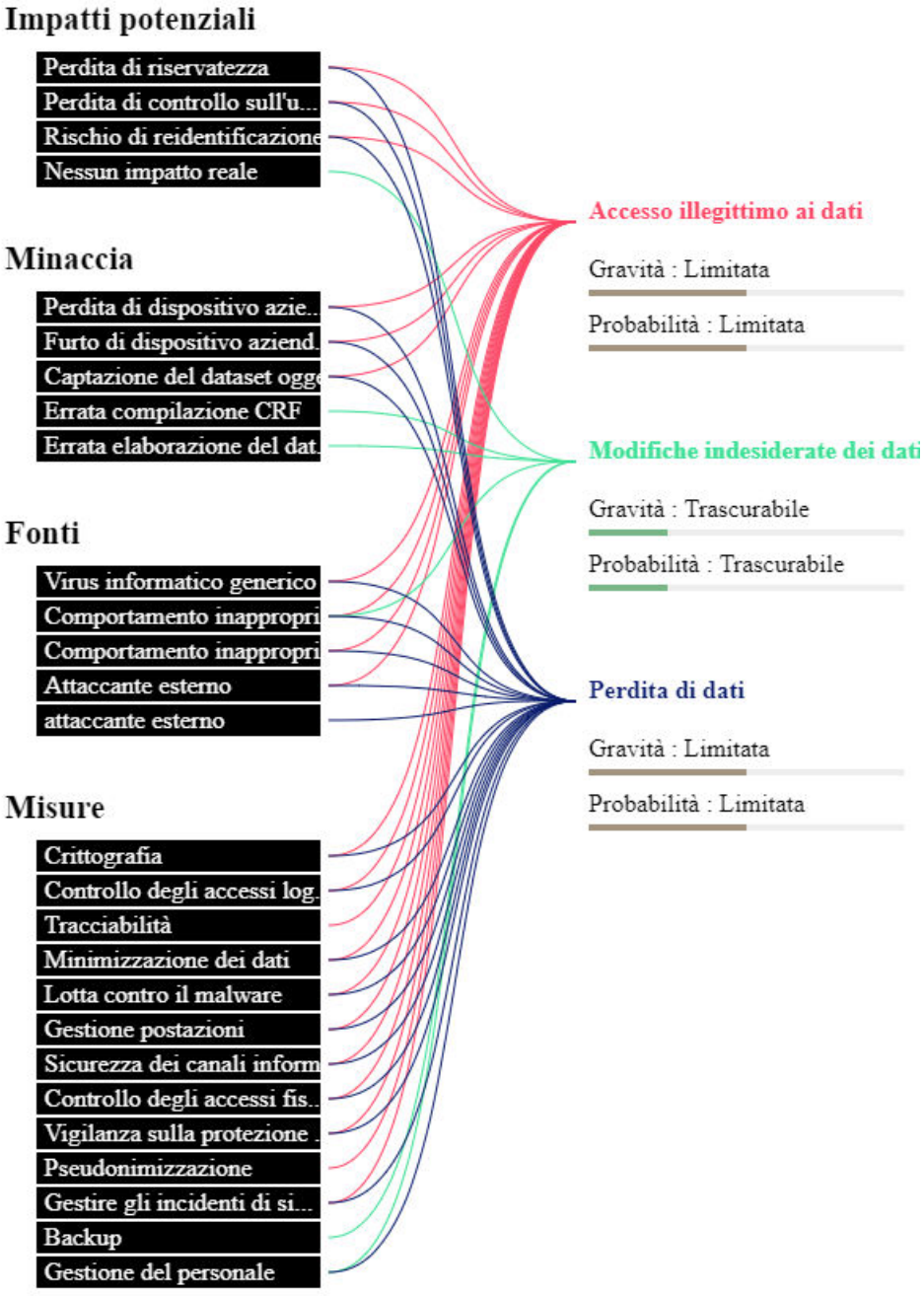
5.2 Gravità del rischio

Sia la gravità che la probabilità dei rischi individuati sono circoscritti come limitati e trascurabili.



5.3 Valutazione residua del rischio

Alla luce delle analisi svolte, il rischio viene individuato come limitato riguardo i rischi di accesso illegittimo ai dati e di perdita di dati. Invece, riguardo al rischio di modifiche indesiderate dei dati, quest'ultimo risulta trascurabile in quanto trattandosi di studio retrospettivo un eventuale modifica avrebbe un impatto sullo studio nel suo insieme ma nessuno sugli interessati.



6 PIANO AZIONE DI RIMEDIO

Il rischio relativo al trattamento dei dati risulta correttamente indirizzato.

(Fine documento)