Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

ISTITUTO DI RICERCHE FARMACOLOGICHE MARIO NEGRI · IRCCS

Responsabile del Progetto : ***Guido Bertolini***
Nome del Progetto/Iniziativa : ***eCREAM, caso d'uso 1***
Responsabile di business: ***Guido Bertolini***
Responsabile IT: ***Felice Catania***

Identificazione delle parti coinvolte partecipanti alla DPIA		
Nome	**Ruolo**	**Commenti**
Serena Somenzi	DPO	
Raffaella Bertazzi, Veronica Giuliano	Sistema Gestione Privacy	
Guido Bertolini	Referente Privacy	
Felice Catania (ASTIR)	Supporto IT	
Chiara Pandolfini	Referente Operativo Privacy	
Rita Banzi	Altro	

Finalità e base legale del trattamento			
Finalità	**Base legale del trattamento** [NOTA: *La base legale per il trattamento può essere ricondotta ad esempio a 'esecuzione di un contratto', 'legittimo interesse per la Società', 'interesse pubblico' o 'consenso dell'interessato* ']	**Diritto di opposizione / Consenso** [NOTA:*Specificare come si intende rispettare il 'diritto di opposizione' (nel caso in*	**Giustificazione** [NOTA: *Specificare come si considera la finalità legittima. Per esempio fornire argomentazioni per giustificare il 'legittimo interesse' (nel caso si siano usate quelle come legittimazione)* .]
Ricerca Scientifica (analisi dati e creazione modelli predittivi)	Altro - art.110 DL 196/2003		

Necessità e Proporzionalità
[NOTA: *Specificare il motivo per il quale si ritiene che il trattamento sia necessario per i relativi fini, e il motivo per il quale i dati trattati siano considerati proporzionati rispetto ai fini per i quali vengono trattati.* **]**

Il trattamento dei dati, il cui numero e la tipologia sono adeguati e proporzionali al disegno dello studio, è necessario per il raggiungimento degli obiettivi prefissati dallo studio

Fonti di Rischio		
Tipologia		**Esempi**
Individui in malafede che appartengono all'Istituto	☑	Collaboratore in malafede con conoscenza e accesso al sistema (individuo dimissionario / in conflitto con la società, dipendente, azionista, membro del top management, ...)
Individui in malafede al di fuori dell'Istituto	☑	Un hacker o un frodatore, un ex impiegato in conflitto con la società dopo il licenziamento, un competitor, gruppi professionali, una lobby, un sindacato, un giornalista o una organizzazione non governativa, un'organizzazione criminale, un'agenzia governativa oppure un'organizzazione controllata da uno stato estero, spie, un'organizzazione terrorista, ecc.
Individui in buona fede che appartengono all'Istituto	☑	Collaboratore non attento o incosciente, con conoscenze e possibilità di agire sul sistema informativo (staff con scarsa attitudine all'impegno e alla precisione, personale del servizio di manutenzione non attento, stagista, amministratori di sistema o di rete, manager, ...).
Individui in buona fede al di fuori dell'Istituto	☑	Collaboratore esterno non attento o incosciente, con conoscenze e possibilità di agire sul sistema informativo (personale del servizio di manutenzione non attento, fornitore, service provider, subappaltatore, cliente, azionisti, amministratori di sistema o di rete, manager, ...).

Fonti non umane	☑	Emissione di onde elettromagnetiche o radioattive, scosse, attività industriali che producono sostanze tossiche o capaci di arrecare danni minori, traffico stradale o aereo che può generare incidenti, attività che sono causa di eventi disastrosi, virus informatici, disastri naturali, materiali infiammabili, epidemie, roditori, ecc.

Minacce			
Accesso Non Autorizzato			
Minaccia Specifica		**Descrizione**	**Esempi**
Utilizzo di dispositivi / strumenti informatici / hardware non adeguati	☐	Utilizzo di dispositivi elettronici (es. smartphone, laptop, ecc.) e strumenti informatici (chiavette usb, database, ecc.) non adeguati per proteggere i dati trattati o in generale non in linea con gli standard definiti.	Uso di unità USB o strumenti di archiviazione non adeguati rispetto alla sensibilità delle informazioni contenute; utilizzo o trasporto di strumenti di archiviazione contenenti dati sensibili per scopi personali, ecc.
Attività di rilevazione illecita delle informazioni	☐	Rilevazione delle informazioni tramite tecniche tese a sottrarre in maniera illecita i dati trattati	Spiare lo schermo del dispositivo di una persona ad esempio sul treno; scattare una foto di uno schermo; geolocalizzazione di un dispositivo; rilevamento remoto di segnali elettromagnetici, ecc.
Alterazione della configurazione hardware di dispositivi / strumenti informatici	☑	Alterazione della configurazione hardware dei dispositivi elettronici o degli strumenti informatici tramite tecniche di hacking o tramite l'utilizzo di apparecchi volti a violare i dati trattati sul dispositivo / strumento	Rimozione di componenti hardware; connessione di dispositivi (come unità flash USB) per avviare un sistema operativo o recuperare dati; rilevazione dei dati tramite keylogger, ecc.
Malfunzionamento / Alterazione del software	☑	Malfunzionamento o alterazione del software per violare o bypassare i meccanismi di sicurezza implementati per proteggere i dati trattati	Invio di mail con virus/malware; uso improprio delle funzioni di rete; innalzamento dei privilegi; utilizzo illegittimo del cross-referencing dei dati; cancellazione delle registrazioni di utilizzo, ecc.
Perdita di dispositivi / strumenti informatici / hardware	☑	Perdita dei dispositivi elettronici o degli strumenti informatici dal controllo del proprietario e/o dell'azienda e conseguente possibilità di violazione dei dati trattati	Furto di un laptop o di un cellulare; Furto di un dispositivo di memorizzazione o di un terminale dismesso; perdita di un dispositivo di memorizzazione elettronico, ecc.
Analisi dei software	☑	Analisi tecnica del software finalizzata a identificare possibili vulnerabilità da utilizzare per violare i dati trattati	Scansione di indirizzi e porte di rete; raccolta di dati di configurazione; analisi dei codici sorgente al fine di individuare vulnerabilità; test delle vulnerabilità dei database, ecc.
Intercettazione di canali informatici di comunicazione	☑	Intercettazione dei dati trattati durante la comunicazione tra diversi dispositivi elettronici o strumenti informatici, tramite l'utilizzo di sistemi di intercettazione o tecniche di hacking	Intercettazione del traffico di rete; acquisizione di dati inviati tramite una rete Wi-Fi, ecc.
Spionaggio degli individui	☐	Intercettazione dei dati trattati durante comunicazioni verbali tra individui tramite ascolto diretto o utilizzo di sistemi di intercettazione audio	Divulgazione involontaria di informazioni mentre si parla; uso di dispositivi di ascolto per intercettare informazioni durante riunioni, ecc.
Manipolazione degli individui (social engineering)	☐	Attività volta ad ingannare l'individuo o esercitare pressione tali da costringerlo a violare i dati trattati	Utilizzo di tecniche per influenzare gli individui (phishing, social engineering, corruzione, ecc.), o esercitare pressione (ricatto, molestie psicologiche, ecc.), ecc.
Accesso non autorizzato a documenti cartacei	☐	Accesso non autorizzato a documenti cartacei contenenti dati personali	Accesso non autorizzato a documenti cartacei per la lettura, l'esecuzione di fotocopie o fotografie ecc.
Furto di documenti cartacei	☐	Sottrazione non autorizzata di documenti cartacei contenenti dati personali	Furto di documenti dagli uffici; furto di posta; recupero di documenti gettati nei rifiuti, ecc.

Compromissione dei canali di trasmissione cartacei ☐	Compromissione dei dati trattati durante la trasmissione cartacea attraverso la visione o la riproduzione dei dati in transito	Lettura o riproduzione di documenti in transito, ecc.
Controllo sugli individui ☐	Controllo e monitoraggio di individui o gruppi di individui al fine di violare i dati trattati	Rapimento; modifica non autorizzata degli incarichi assegnati; controllo di tutta o parte dell'organizzazione, ecc.
Cambiamenti Indesiderati		
Minaccia Specifica	**Descrizione**	**Esempi**
Alterazione della configurazione hardware di dispositivi / strumenti informatici ☐	Alterazione dei dispositivi elettronici o degli strumenti informatici con compromissione dell'integrità dei dati trattati	Introduzione di hardware incompatibile con conseguenti malfunzionamenti; rimozione di componenti essenziali per il corretto funzionamento di un'applicazione, ecc.
Utilizzo non corretto di dispositivi / strumenti informatici ☐	Utilizzo o gestione di dispositivi elettronici e strumenti informatici in maniera non corretta con la conseguente compromissione dell'integrità dei dati trattati	Errori dell'operatore che modifica i dati; modifiche indesiderate ai dati nei database; cancellazione dei file necessari per il corretto funzionamento del software, ecc.
Alterazioni non previste dei software ☑	Alterazione non prevista del software con violazione dell'integrità dei dati trattati	Errori durante gli aggiornamenti, la configurazione o la manutenzione; introduzione di malware; sostituzione di componenti software, ecc.
Attacchi informatici per l'alterazione dei dati trasmessi ☑	Utilizzo di tecniche di hacking tese a violare la trasmissione dei dati con la possibile modifica dei dati trasmessi	Attacco man-in-the-middle; replay attack (invio di dati intercettati), ecc.
Influenza sull'ambiente lavorativo ☐	Situazioni che possono influenzare il contesto lavorativo mediante aumento dei carichi di lavoro o peggioramento delle condizioni di lavoro, con il conseguente incremento dei possibili errori da parte del personale	Elevato carico di lavoro, stress o cambiamenti negativi nelle condizioni di lavoro; assegnazione al personale di compiti non adeguati rispetto alle competenze, ecc.
Manipolazione di individui ☐	Manipolazione dei soggetti che effettuano il trattamento di dati al fine di indurre a modifiche o errori che compromettano l'integrità dei dati	Utilizzo di tecniche per Influenzare gli individui, diffusione di notizie false o alterate, disinformazione, modifica di istruzioni operative, ecc.
Alterazione di documenti cartacei ☐	Alterazione dei dati su supporti cartacei	Modifiche ai valori riportati in un documento; sostituzione di un originale con un falso, ecc.
Perdita dei Dati		
Minaccia Specifica	**Descrizione**	**Esempi**
Malfunzionamento hardware ☑	Malfunzionamento hardware che determina la compromissione della disponibilità dei dati	Guasto di un server, guasto di un hard disk, ecc.
Sovraccarico hardware ☑	Sovraccarico hardware che determina la compromissione della disponibilità dei supporti necessari all'accesso ai dati	Unità di memoria piena; sovraccarico di capacità di elaborazione; surriscaldamento, ecc.
Alterazione della configurazione hardware ☑	Alterazione hardware che determina la compromissione della disponibilità dei dati	Aggiunta di hardware incompatibili con conseguente malfunzionamento; rimozione di componenti essenziali per il corretto funzionamento del sistema, ecc.

Danneggiamento hardware ☑	Danneggiamento hardware causato da eventi naturali, errori umani o atti dolosi che determina la compromissione della disponibilità dei dati	Inondazioni, incendi, atti vandalici, ecc.
Perdita di hardware ☐	Furto o smarrimento di hardware che determina la compromissione della disponibilità dei dati	Furto o smarrimenti di un laptop o di un cellulare; furto o smarrimento di un supporto di memorizzazione, smaltimento di un dispositivo o hardware, ecc.
Utilizzo anormale del software ☑	Utilizzo di software in maniera erronea o di software errati che determina la compromissione della disponibilità dei dati	Cancellazione di dati; utilizzo di software contraffatto o copiato; errori dell'operatore che cancellano i dati, ecc.
Sovraccarico del software ☑	Sovraccarico delle risorse software che ne impedisce il corretto funzionamento e quindi determina la compromissione della disponibilità dei dati	Superamento della dimensione del database; inserimento di dati al di fuori del normale intervallo di valori, ecc.
Alterazione del software ☑	Malfunzionamento a seguito di alterazione del software con compromissione della disponibilità dei dati	Errori durante gli aggiornamenti, la configurazione o la manutenzione; infezione da codice dannoso; sostituzione di componenti, ecc.
Cancellazione di tutto o parte di un software ☑	Cancellazione di un software utilizzato per accedere ai dati	Cancellazione di un programma o di un codice sorgente in esecuzione, ecc.
Perdita del software ☐	Impossibilità di utilizzo di un software necessario per accedere ai dati	Mancato rinnovo della licenza del software utilizzato per accedere ai dati, ecc.
Saturazione delle connessioni ☐	Sovraccarico della capacità di trasmissione dati che compromette la disponibilità dei dati	Uso improprio della banda di rete; download non autorizzato; perdita di connessione Internet, ecc.
Interruzione delle connessioni ☐	Danneggiamento o malfunzionamento delle infrastrutture necessarie alla trasmissione dei dati che determina la compromissione della disponibilità dei dati	Taglio dei cavi di rete, scarsa ricezione Wi-Fi, ecc.
Condizioni lavorative non adeguate ☐	Aumento dei carichi di lavoro o peggioramento delle condizioni di lavoro con compromissione del corretto accesso e utilizzo dei dati	Elevato carico di lavoro, stress o cambiamenti peggiorativi delle condizioni di lavoro; assegnazione del personale a compiti che vanno oltre le loro capacità; utilizzo di competenze non adeguate, ecc.
Indisponibilità del personale ☐	Indisponibilità del personale che detiene i dati trattati	Incidente professionale, malattia, sciopero, dimissioni, ecc.
Danneggiamento/distruzione di documenti cartacei ☐	Danneggiamento/distruzione dei dati memorizzati su supporti cartacei	Cancellazione graduale nel tempo, distruzione volontaria o per errore di parti di documentazione, incendio, ecc.
Furto o smarrimento di documenti cartacei ☐	Furto o smarrimento dei supporti cartacei su cui sono memorizzati i dati trattati	Furto di documenti, perdita di documenti durante un loro spostamento, ecc.

Impatti

Tipologia	Impatto Specifico	Descrizione
Danni Fisici		
Danni Materiali		
Danni Morali	Violazione dei diritti (discriminazione, violazione delle libertà, ecc.)	Violazione del diritto alla riservatezza dovuta alla perdita o alla diffusione dei dati personali
	Violazione della vita privata	Violazione del diritto alla riservatezza dovuta alla perdita o alla diffusione dei dati personal

Contromisure		
Contromisure Tecniche		
Categoria	**Misure Specifiche**	**Descrizione**
	Vulnerability Assessment e Penetration Testing ☑	In ambito certificazione in corso ISO 27001, analisi periodica dell'infrastruttura dispositivi e networking.
	Revisione del codice sorgente ☑	Nel ciclo di sviluppo vengono utilizzate procedure di code review, supportate da strumenti offerti da piattaforma Atlassian
	Monitoraggio delle utenze amministrative ☑	Utilizzo degli strumenti di monitoraggio AWS
	Log delle infrastrutture ☑	Utilizzo degli strumenti di logging AWS
	Log applicativi ☑	Procedure software di produzione log applicativi per tracciatura eventi

Sicurezza Informatica	Certificazione dei Log	☐	
	SIEM / SOC	☐	
	Difesa perimetrale	☑	Strumenti di AWS
	Anti Virus	☑	Utilizzo antivirus su componenti server
	Anti Malware	☑	Utilizzo antimalware su componenti server
	Anti Advanced Persistent Threat (APT)	☐	
	Crittografia	☑	Utilizzo strumenti AWS
	Data Loss Prevention (DLP)	☐	
	Strong Authentication	☑	Utilizzo procedura autenticazione dual factor
	Identity & Access Management (IAM)	☑	Utilizzo IAM AWS
	Web Application Firewall (WAF)	☐	
	Strumento di gestione degli incidenti	☑	Utilizzo piattaforma Jira secondo procedure di Qualità ISO 9001
	Altro	☑	Ambiente cloud AWS certificato ISO 27018 (definito per garantire che i fornitori di servizi cloud mantengano misure di sicurezza adeguate quando gestiscono i dati personali appartenenti ai loro clienti.
Business Continuity	Backup	☑	Utilizzo strumenti AWS
	Disaster Recovery	☐	
	Altro	☑	Server virtuali in cloud duplicabili da backup
Sicurezza Fisica	Misure di protezione degli asset	☑	Misure di sicurezza del centro di erogazione Amazon Web Services (ISO 27018)
	Altro	☐	

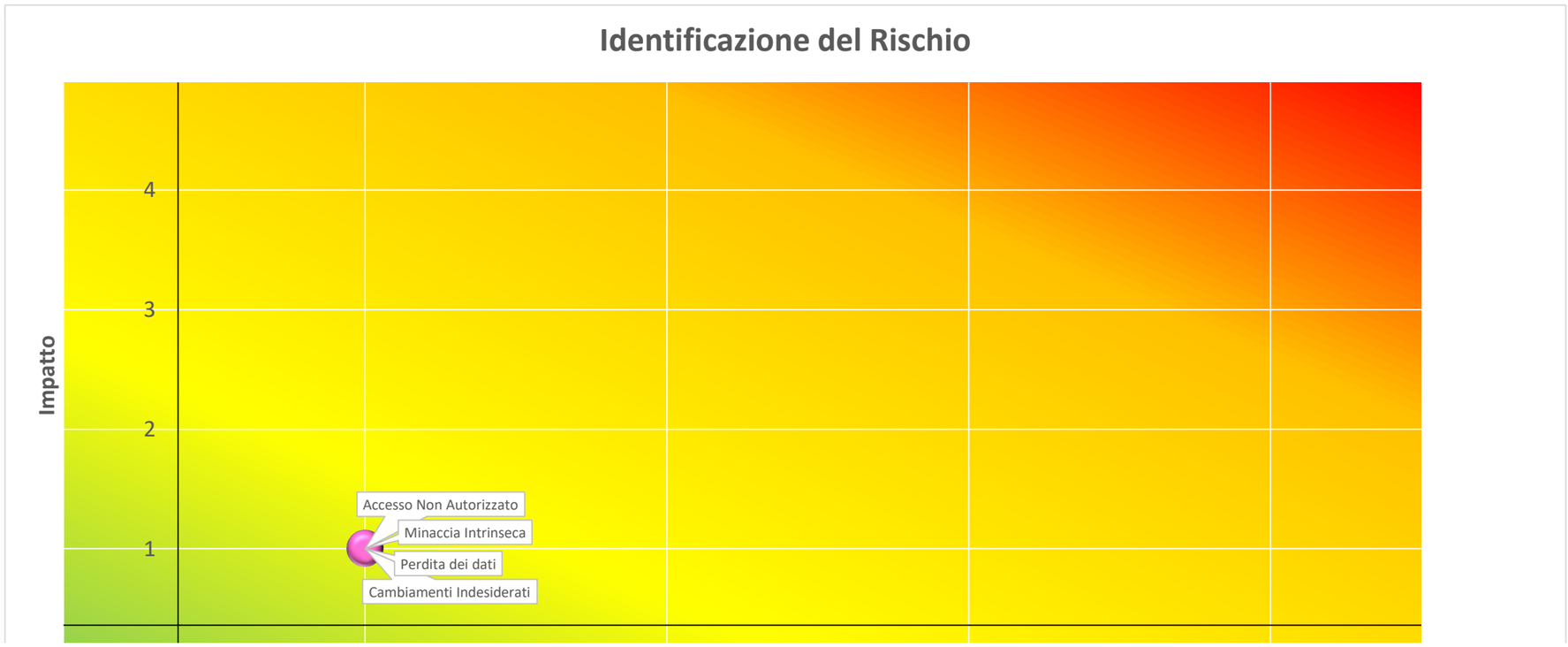
Contromisure Organizzative

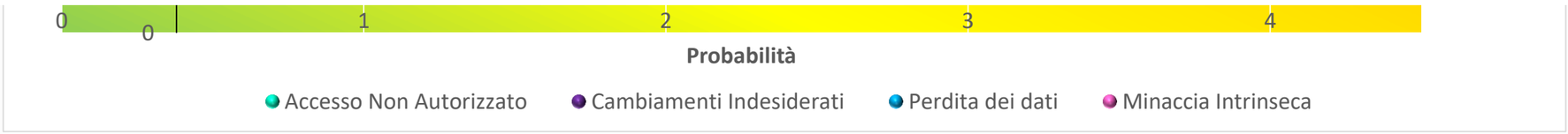
Categoria	Misure Specifiche		Descrizione
Sicurezza Informatica	Policy sulla Sicurezza Informatica	☑	Implementate Policy organizzative per la Sicurezza Informatica nel sistema Qualità ISO 9001. In corso aggiornamento del sistema di Qualità secondo ISO 27001.
	Controllo degli accessi logici	☑	Procedure "Politica controllo accessi" alle macchine di conservazione e trattamento dati. Nomina di amministratori di sistema per ogni ambito di trattamento dati, con responsabilità su sicurezza informatica degli specifici sistemi erogati. Manutenzione elenco del personale con i permessi di accesso ai dati secondo i diversi livelli di
	Sviluppo sicuro del Software	☑	Procedure di sviluppo conformi alle linee guida OWASP. Il Top 10 dell'OWASP è un documento standard di sensibilizzazione per sviluppatori e sicurezza delle applicazioni web che rappresenta un ampio consenso sui rischi di sicurezza più critici per le applicazioni web. In corso aggiornamento del processo produttivo secondo ISO 13485.
	Smaltimento sicuro dei dati e degli asset	☐	
	Gestione della sicurezza delle terze parti	☐	
	Gestione sicura dei dispositivi elettronici	☑	Procedure di requisiti e standard dei dispositivi elettronici utilizzati per l'accesso alle macchine di trattamento dei dati
	Classificazione dei dati	☑	Dati classificati e tracciati nel registro dei trattamenti

	Gestione degli incidenti di sicurezza	☑	Procedura di incident management codificata nel sistema documentale Information Security Management
	Sicurezza Risorse umane	☐	
	Change & Project Management	☐	
	Gestione delle vulnerabilità	☑	Audit periodici, a partire dagli incident report, per estensione delle misure di sicurezza ai sistema in carico.
	Gestione del ciclo di vita dei dati	☑	Rispetto delle policy di data retention secondo GDPR e normativa nazionale.
	Gestione della crittografia	☐	
	Altro	☐	
Business Continuity	Business Continuity Policy	☑	Implementate Policy organizzative per Business Continuity
	Backup Management	☑	Implementate Policy organizzative per Backup in relazione alle diverse tipologie di trattamento
	Piano di Disaster Recovery	☐	
	Altro	☐	
Sicurezza Fisica	Policy sulla sicurezza fisica	☐	
	Controllo accessi fisici	☑	Implementati controlli degli accessi fisici agli uffici dove sono presenti le workstation di accesso alle macchine di trattamento dei dati
	Altro	☐	
Training e Awareness	Sicurezza Informatica	☐	
	Continuità Operativa	☐	
	Sicurezza fisica	☐	
	Altro	☑	Incontri interni di sensibilizzazione su: qualità e sicurezza degli sviluppi software, principi di privacy by design and by default, linee di indirizzo GDPR su trattamento dati, diritti interessato, gestione data

Rischi identificati in riferimento ai diritti e alle libertà degli interessati e misure di mitigazione associate			
Minaccia	**Descrizione dello Scenario**	**Probabilità**	**Descrizione della Probabilità**
Accesso Non Autorizzato	Evento in cui individui che non dovrebbero avere accesso a determinate informazioni sono state tuttavia capaci di entrare in possesso di tali dati, in violazione del principio di confidenzialità.	**1**	La minaccia/rischio non può verificarsi o è remota la possibilità che si realizzi

Cambiamenti Indesiderati	Situazione in cui sono state effettuate modifiche indesiderate ai dati, dunque determinando una violazione alla loro integrità.	**1**	La minaccia/rischio non può verificarsi o è remota la possibilità che si realizzi
Perdita dei dati	Circostanze connesse all'incapacità, da parte di individui autorizzati, di accedere alle informazioni, determinando la mancanza di disponibilità dei dati.	**1**	La minaccia/rischio non può verificarsi o è remota la possibilità che si realizzi
Minaccia Intrinseca	Caso in cui il trattamento stesso minaccia i diritti e le libertà dell'interessato	**2**	E' probabile che la minaccia/rischio si realizzi





VALUTAZIONE FINALE DEL RISCHIO		
Rischio Massimo Identificato	4	*Rischio Basso*
Le misure di sicurezza poste a presidio dei dati personali fanno ritenere che il rischio possa definirsi come BASSO		

Consultazione preventiva con l'autorità competente in materia privacy nel caso in cui sia registrato un elevato rischio del trattamento