Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

ISTITUTO DI RICERCHE FARMACOLOGICHE MARIO NEGRI · IRCCS

Responsabile del Progetto :	**Roldano Fossati**
Nome del Progetto/Iniziativa :	**Citoriduzione secondaria k ovaio**
Responsabile di business:	**Roldano Fossati**
Responsabile IT:	**Elda Caccia**

Identificazione delle parti coinvolte partecipanti alla DPIA		
Nome	**Ruolo**	**Commenti**
CDR - Cattaneo Dall'Olio Rho & Partners - Tax & Legal	DPO	
Raffaella Bertazzi, Veronica Giuliano	Sistema Gestione Privacy	
Valter Torri	Referente Privacy	
Lorenzo Rossi	Centro Ingegneria Informatica	
Elda Caccia	Supporto IT	
Monica Carsenzuola	Referente Operativo Privacy	
	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 cui il trattamento sia basato su un legittimo interesse per la Societa' o su un pubblico interesse), oppure come si intende gestire il consenso (nel caso in cui il trattamento sia basato sul consenso).*]	**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).*]
Analisi Statistica	Consenso dell'individuo	Revoca mediante comunicazione scritta al Titolare	
Ricerca Scientifica / Sperimentazione Clinica	Consenso dell'individuo	Revoca mediante comunicazione scritta al Titolare	
Ricerca Scientifica / Sperimentazione Clinica	Altro	-	Art. 110 C.P. per pazienti decedute o non rintracciabili
Analisi dei Dati	Consenso dell'individuo	Revoca mediante comunicazione scritta al Titolare	

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

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 confgurazione 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 ditto all riservateza dovuta alla perdita o alla diffusione dei dati personali
	Violazione della vita privata	Violazione del ditto all riservateza dovuta alla perdita o alla diffusione dei dati personali

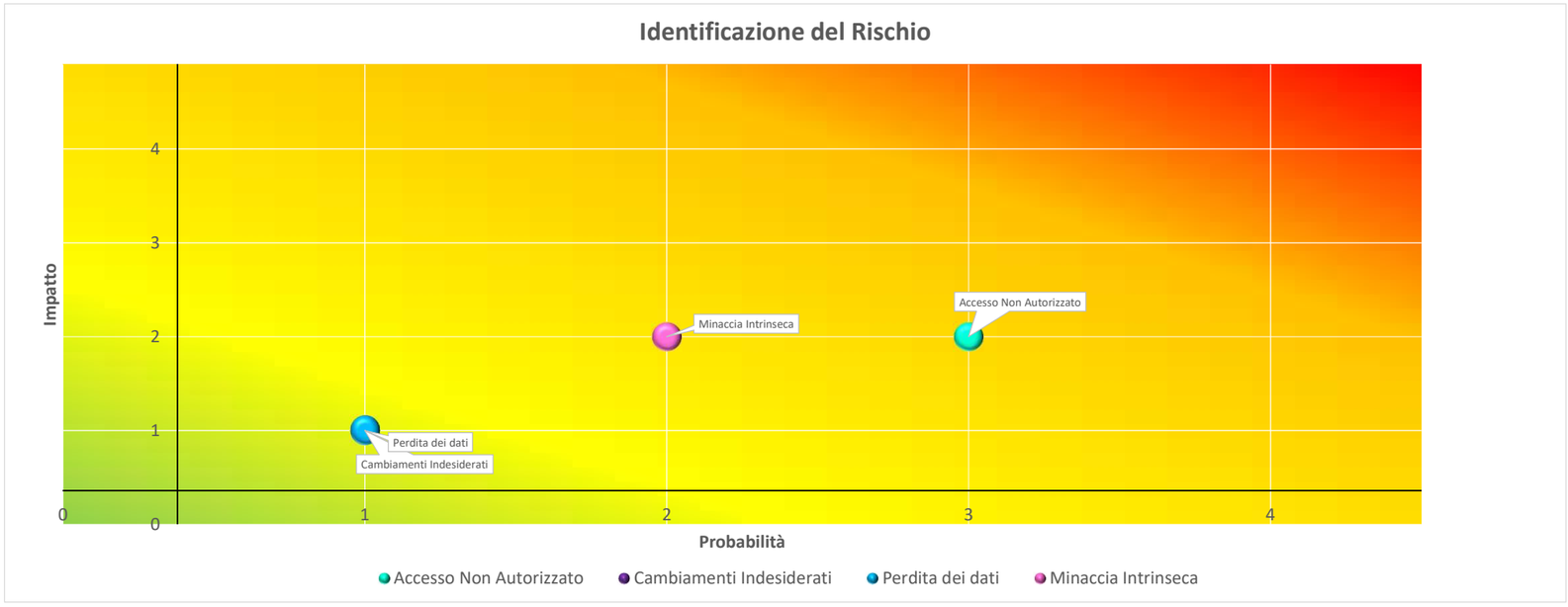
Contromisure		
Contromisure Tecniche		
Categoria	**Misure Specifiche**	**Descrizione**
Sicurezza Informatica	Vulnerability Assessment e Penetration Testing ☑	Vengono effettuate periodicamente delle attività di Vulnerability Assessment sui sistemi più critici della rete informatica dell'Istituto
	Revisione del codice sorgente ☐	
	Monitoraggio delle utenze amministrative ☐	
	Log delle infrastrutture ☑	Gli accessi alle infrastrutture (server, postazioni di lavoro, ecc.) da parte dei preposti al trattamento dei dati sono nominativi e sono registrati in appositi files (c.d. "files di log") con indicazione di data, ora e provenienza dell'accesso
	Log applicativi ☑	Gli accessi agli applicativi che trattano dati personali e/o particolari da parte degli incaricati sono protetti da credenziali personali e sono registrati in appositi files
	Certificazione dei Log ☐	
	SIEM / SOC ☐	
	Difesa perimetrale ☑	La difesa perimetrale dell'infrastruttura informatica è realizzata con una coppia di Next-Generation Firewall FORCEPOINT
	Anti Virus ☑	La protezione delle Postazioni di Lavoro è realizzata con l'antivirus/antimalware ESET Endpoint Security gestito centralmente e mantenuto costantemente aggiornato
	Anti Malware ☑	La protezione delle Postazioni di Lavoro è realizzata con l'antivirus/antimalware ESET Endpoint Security gestito centralmente e mantenuto costantemente aggiornato
	Anti Advanced Persistent Threat (APT) ☐	
	Crittografia ☑	Gli applicativi che gestiscono dati particolari prevedono sistemi di crittografia utilizzati per la memorizzazione di tali informazioni all'interno delle basi dati. Inoltre le connessioni VPN e tutte le comunicazioni fra sistemi u
	Data Loss Prevention (DLP) ☐	
	Strong Authentication ☐	
	Identity & Access Management (IAM) ☐	
	Web Application Firewall (WAF) ☑	E' presente un Web Application Firewall integrato nel sistema di firewall perimetrale FORCEPOINT
	Strumento di gestione degli incidenti ☐	
	Altro ☐	
Business Continuity	Backup ☑	Backup eseguito giornalmente
	Disaster Recovery ☑	La copia dei dati sottoposti a backup viene conservata su aree di storage dedicate ubicate in un edificio del Campus separato da quello dove risiede la Server Farm. Non sono attualmente previsti né siti di DR secondari né strategie di Business Continuity
	Altro ☐	
Sicurezza Fisica	Misure di protezione degli asset ☐	
	Altro ☐	
Contromisure Organizzative		
Categoria	**Misure Specifiche**	**Descrizione**
	Policy sulla Sicurezza Informatica ☑	L'Istituto è dotato di una policy di sicurezza informatica che prevede l'informazione, la formazione degli utenti e la presenza di credenziali personali autorizzate
	Controllo degli accessi logici ☑	E' garantito l'iuso di account personali con politica di qualificazione, lunghezza e complessità della password (minimo 12 caratteri con almeno 1 lettera maiuscola, 1 lettera minuscola e un carattere numerico). Richiesta periodica automatica di cambio password.
	Sviluppo sicuro del Software ☑	La piattaforma REDCAP possiede differenti standard di ricurezza per la gestione di dati sensibili, incluso lo standard HIPAA (Health Insurance Portability and Accountability Act)

Sicurezza Informatica	Smaltimento sicuro dei dati e degli asset	☐		
	Gestione della sicurezza delle terze parti	☑	Le terze parti esterne (fornitori, collaboratori esterni ecc.) possono accedere unicamente alle risorse di competenza previa richiesta scritta delle credenziali di accesso e utilizzo di strumenti sicuri (collegamento VPN)	
	Gestione sicura dei dispositivi elettronici	☑	I dispositivi elettronici (computer, tablet, cellulari ecc.) possono collegarsi alla rete dell'Istituto ed accedere a dati e servizi solo se gestiti dal personale dell'Istituto ed equipaggiati con tutte le dotazioni di sicurezza (antivirus, sistema operativo costantemente aggiornato con le patches di sicurezza, ecc.). Ai dispositivi non gestiti dall'Istituto è inibito l'accesso a tutte le risorse fruibili dalla rete dell'Istituto, ad eccezione dell'accesso	
	Classificazione dei dati	☐		
	Gestione degli incidenti di sicurezza	☐		
	Sicurezza Risorse umane	☑	Il personale coinvolto nel trattamento dei dati personali è adeguatamente formato e informato in merito ai requisiti in materia di protezione dei dati e agli obblighi legali attraverso regolari campagne di formazione e sensibilizzazione.	*Specificare la descrizione*
	Change & Project Management	☐		
	Gestione delle vulnerabilità	☑	I sistemi operativi dei computer vengono mantenuti costantemente aggiornati per eliminare le vulnerabilità di sicurezza	
	Gestione del ciclo di vita dei dati	☑	E' previsto che i dati raccolti siano inquadrati in un trattamento regolamentato dal punto di vista Privacy incluso il periodo di conservazione	
	Gestione della crittografia	☑	Applicazione di protocolli crittografici (TLS/SSL)	
	Altro	☐		
Business Continuity	Business Continuity Policy	☑		
	Backup Management	☑	Le procedure di backup e ripristino dei dati sono definite, documentate e chiaramente collegate a ruoli e responsabilità. I backup completi sono eseguiti giornalmente.	
	Piano di Disaster Recovery	☑		
	Altro	☐		
Sicurezza Fisica	Policy sulla sicurezza fisica	☑	E' previsto un accesso regolamentato ai locali che ospitano i server, gli storage e gli apparati di rete, con possibilità di ingresso al solo personale preposto, oltre alla registrazione di tutti gli accessi e ad un sistema di sorveglianza remota tramite telecontrollo attivo 24 ore su 24	
	Controllo accessi fisici	☑	L'accesso fisico alla Server Farm aziendale è controllato tramite badge e consentito solo alle persone esplicitamente abilitate. Tutti gli accessi sono registrati.	
	Altro	☐		
Training e Awareness	Sicurezza Informatica	☑	E' prevista la formazione sulle regole per accedere alle infrastrutture informatiche dell'Istituto. Inoltre ogni persona abilitata all'utilizzo delle risorse informatiche deve prendere visione dell'apposito regolamento informatico	
	Continuità Operativa	☐		
	Sicurezza fisica	☑	E' prevista una formazione per le regole che riguardano gli accessi fisici all'Istituto	
	Altro	☐		

Rischi identificati in riferimento ai diritti e alle libertà degli interessati e misure di mitigazione associate

Minaccia	Descrizione dello Scenario	Probabilità	Descrizione della Probabilità	Impatto	Descrizione dell'Impatto	Rischio	Note
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.	**3**	La minaccia/rischio sicuramente prima o poi si verificherà	**2**	Limitato - I Soggetti Interessati potrebbero incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, negazione dell'accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).	**6**	
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	**1**	Trascurabile - I Soggetti Interessati non subiranno conseguenze o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso a reinserire informazioni, seccature, irritazioni, ecc.).	**1**	
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	**1**	Trascurabile - I Soggetti Interessati non subiranno conseguenze o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso a reinserire informazioni, seccature, irritazioni, ecc.).	**1**	

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	**2**	Limitato - I Soggetti Interessati potrebbero incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, negazione dell'accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).	**4**	



VALUTAZIONE FINALE DEL RISCHIO		
Rischio Massimo Identificato	6	*Rischio Basso*
[Commentare la valutazione effettuata]		

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