ANALISI DEI RISCHI RELATIVA AL TRATTAMENTO DEI DATI PERSONALI
IN CAMMINO CON ROBERTO STRACCIA ODV

PASSAGGI METODOLOGICI

La presente guida per la valutazione dei rischi, che riprende le linee guida dell'ENISA (European Network and Information Security Agency) per le PMI, propone un approccio alla valutazione del rischio che si basa su quattro fasi, come segue:

1. Definizione dell'operazione di trattamento e del suo contesto.
2. Comprensione e valutazione dell'impatto.
3. Definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia).
4. Valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto).

Seguendo la valutazione del rischio, è possibile adottare misure di sicurezza tecniche e organizzative (da un elenco proposto) che sono appropriate al livello di rischio.

DEFINIZIONE DELL'OPERAZIONE DI TRATTAMENTO E IL SUO CONTESTO

Questo è il primo passo della valutazione di impatto del rischio ed è fondamentale per il titolare del trattamento al fine di tracciare i confini del sistema del trattamento dei dati personali (in corso di valutazione) e il relativo contesto. Per supportare le Associazioni nel definire l'operazione di trattamento vengono poste le seguenti domande. Mentre si risponde a tali domande, l'Associazione deve considerare le varie fasi del trattamento del dato (raccolta, conservazione, uso, trasferimento, cessazione, ecc…):

1. Qual è l'operazione di trattamento di dati personali?
2. Quali sono le tipologie di dati personali trattati?
3. Qual è il fine del trattamento?
4. Quali sono i mezzi utilizzati per il trattamento dei dati personali?
5. Dove avviene il trattamento dei dati?
6. Quali sono le categorie degli interessati?
7. Chi sono i destinatari dei dati?

FASE 1: CAPIRE E VALUTARE IL LIVELLO DI IMPATTO DEL TRATTAMENTO

A questo punto il Titolare del trattamento deve valutare l'impatto sui diritti fondamentali e le liberà degli individui che può derivare dalla possibile perdita di dati personali. Vengono presi in considerazione 4 livelli di impatto (basso, medio, alto, molto alto), secondo la tabella che segue.

Tabella 1: Descrizione dei livelli di impatto del trattamento

Livello di impatto	Descrizione
BASSO	Gli interessati possono andare incontro a pochi e minori inconvenienti che supereranno senza alcun problema (tempo speso a fornire nuovamente le informazioni, fastidi, irritazioni, ecc…)
MEDIO	Gli interessati possono andare incontro a significativi inconvenienti che saranno in grado di superare nonostante piccole difficoltà (costi extra, diniego di accesso ai servizi per gli affari, paura, incomprensioni, stress, piccoli disturbi fisici, ecc…)
ALTO	Gli interessati possono andare incontro a inconvenienti significativi, che potrebbero essere in grado di superare, sebbene con serie difficoltà (appropriazioni indebite di capitali, inserimento nella lista nera di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, citazione in giudizio, peggioramento della salute, ecc…)

La valutazione di impatto è un processo qualitativo e debbono essere considerati diversi fattori dal Titolare del trattamento, come ad esempio la tipologia dei dati personali, le criticità delle operazioni di trattamento, il volume dei dati personali raccolti, speciali caratteristiche del Responsabile del trattamento così come speciali categorie di interessati.
Al fine di aiutare il titolare in questo procedimento, può essere utilizzata la Tabella che segue per valutare in modo separato l'impatto derivante dalla perdita di riservatezza, di integrità e disponibilità dei dati.
Dopo tale valutazione, saranno ottenuti tre livelli di impatto (per la perdita di riservatezza, integrità, disponibilità).
Il più alto di questi livelli viene considerato come il risultato finale della valutazione d'impatto, relativamente al trattamento complessivo dei dati.

Tabella 2: valutazione dei tre livelli di impatto

No.	Domanda	Valutazione
I.1	Per cortesia rifletta sull'impatto che una rivelazione non autorizzata (perdita di riservatezza) – nel contesto dove si svolge la sua attività – può avere sull'interessato ed esprima una valutazione	☒ Basso ☐ Medio ☐ Alto
I.2	Per cortesia rifletta sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto dove si svolge la sua attività – può avere sull'interessato ed esprima una valutazione	☒ Basso ☐ Medio ☐ Alto
I.3	Per cortesia rifletta sull'impatto che una distruzione o una perdita non autorizzate (perdita di disponibilità) dei dati personali - nel contesto dove si svolge la sua attività – può avere sull'interessato ed esprima una valutazione	☒ Basso ☐ Medio ☐ Alto

FASE 2: DEFINIZIONE DELLE POSSIBILI MINACCE E VALUTAZIONE DELLA LORO PROBABILITÀ

A questo punto, lo scopo del Titolare del trattamento deve comprendere le minacce correlate alle condizioni in cui vengono trattati i dati personali (internamente ed esternamente all'Associazione) e stabilire le loro probabilità di verificazione.
Per semplificare il procedimento, vengono definite alcune domande che mirano a rendere consapevoli le associazioni e le aziende in genere delle condizioni di trattamento dei dati personali. A tale scopo, le Associazioni devono relazionarsi con quattro principali dimensioni:

A. RISORSE TECNICHE E NETWORK
B. PROCESSI/PROCEDURE CORRELATE AL TRATTAMENTO DEI DATI
C. PERSONE E PARTI DIFFERENTI COINVOLTE NEL TRATTAMENTO
D. SETTORE DI BUSINESS E PESO DEL TRATTAMENTO

La tabella sottostante riassume le domande correlate alla valutazione delle probabilità di avveramento delle minacce.

Tabella 3: valutazione delle probabilità di avveramento delle minacce

A. **RISORSE TECNICHE E NETWORK**		
1	Una parte del trattamento dei dati	Quando il trattamento dei dati viene

	viene realizzata attraverso internet?	totalmente o parzialmente realizzato attraverso Internet, aumentano le possibilità di minacce esterne online, specialmente quando il servizio internet è a disposizione di tutti gli utilizzatori di internet
2	È possibile fornire l'accesso a un sistema di trattamento interno di dati personali tramite Internet?	Quando viene fornito l'accesso a un sistema di trattamento interno di dati personali tramite internet, la probabilità di minacce esterne aumenta. Allo stesso tempo, la probabilità di abuso (volontario o meno) dei dati da parte degli utenti aumenta. Un'attenzione particolare deve essere data ai casi dove è permesso un accesso o un'amministrazione del sistema informatico da remoto
3	Il sistema di trattamento dei dati personali è interconnesso con un altro servizio IT, esterno o interno?	La connessione con un servizio IT esterno può introdurre minacce ulteriori dovute alle minacce inerenti a quei sistemi. Lo stesso dicasi del servizio IT interno, tenendo conto che, se non correttamente configurato, tali connessioni possono permettere l'accesso ai dati personali a più personale dentro l'Azienda, persone non autorizzate al trattamento
4	Persone non autorizzate al trattamento possono avere accesso facilmente al trattamento dei dati?	Nonostante ci si concentri spesso sui sistemi elettronici e digitali, l'0ambiente fisico è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza
5	Il processo del trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le più importanti "*best practice*"?	Componenti hardware e/o software progettati male e/o mantenuti peggio possono determinare seri rischi alla sicurezza delle informazioni. A questo fine, buone o migliori pratiche racchiudono l'esperienza di eventi precedenti e possono essere considerate come pratiche linee guida di come evitare l'esposizione al rischio e ottenere determinati livelli di resilienza
B. **PROCESSI/PROCEDURE CORRELATE AL TRATTAMENTO DEI DATI**		
6	I ruoli e le responsabilità rispetto al trattamento dei dati personali sono vaghi o non chiaramente definiti?	Quando i ruoli e le responsabilità non sono ben definiti, l'accesso ai dati personali può essere incontrollato, determinando un uso non autorizzato delle risorse e compromettendo la sicurezza globale del sistema
7	L'uso della rete, dei sistemi e delle risorse fisiche nell'Azienda è accettabile o non chiaramente definito?	Quando un uso accettabile delle risorse non è chiaramente definito, possono crescere le minacce dovute alle incomprensioni o a abusi intenzionali del sistema. La chiara definizione di politiche della rete, del sistema e delle risorse fisiche possono ridurre i rischi potenziali.
8	I dipendenti hanno il permesso di usare i loro device per connettersi al sistema del trattamento dei dati?	I dipendenti che usano i loro device in Azienda possono aumentare il rischio di perdita dei dati o di accessi non autorizzati al sistema informativo. Inoltre, siccome i device personali non

		sono controllati a livello centrale, possono introdurre bug o virus nel sistema
9	I dipendenti hanno il permesso di trasferire, immagazzinare o altro il procedimento di trattamento dei dati personali fuori dall'Azienda?	Il trattamento dei dati personali al di fuori dell'Azienda può offrire flessibilità ma allo stesso tempo introdurre rischi addizionali, tutti relativi alla trasmissione delle informazioni attraverso canali network non sicuri (open Wi-Fi), così come un uso non autorizzato delle informazioni
10	Il procedimento del trattamento dei dati personali può essere effettuato senza aver prima creato i file di log?	La mancanza di meccanismi di accesso e di monitoraggio appropriati può aumentare eventi di abusi accidentali o intenzionali dei processi/procedure e risorse, ottenendo come risultato l'abuso conseguente dei dati personali
	C. **PERSONE E PARTI DIFFERENTI COINVOLTE NEL TRATTAMENTO**	
11	Il procedimento del trattamento è effettuato da un numero non definito di impiegati?	Quando l'accesso ai, e il successivo trattamento dei, dati personali è aperto a un gran numero di impiegati, le possibilità di abuso dovute al fattore umano aumentano. Definire in maniera chiara chi debba accedere ai dati e limitare l'accesso solo ad alcune persone può contribuire alla sicurezza dei dati personali
12	Parti del trattamento sono svolte da terze parti (responsabili del trattamento esterni)?	Quando il trattamento è effettuato da terze parti esterne, l'Azienda può perdere parzialmente il controllo su questi dati. Inoltre, ulteriori minacce alla sicurezza possono essere introdotte in Azienda a causa delle minacce inerenti a tali terze parti. È importante che l'Azienda selezioni le terze parti che possono offrire un alto livello di sicurezza a che definisca chiaramente quale parte del trattamento è assegnato loro, mantenendo il più possibile un elevato livello di controllo
13	Gli obblighi degli incaricati al trattamento sono ambigui o non chiaramente statuiti?	Quando gli impiegati non sono informati in modo chiaro circa i loro compiti, le minacce derivanti da un abuso accidentale dei dati può aumentare significativamente
14	Il personale coinvolto nel trattamento è all'oscuro della materia della sicurezza delle informazioni?	Quando gli impiegati non sono consapevoli della necessità di applicare misure di sicurezza, essi possono accidentalmente creare future minacce al sistema. La formazione può contribuire molto nel rendere gli impiegati consapevoli sia dei compiti legati alla protezione dei dati sia dell'applicazione di specifiche misure di sicurezza
15	Il personale coinvolto nel trattamento trascura di immagazzinare in modo sicuro e/o distruggere i dati personali?	Molti Data Breach sono dovuti alla mancanza di misure di protezione fisica, come sistemi di chiusura o di distruzione.

D. **SETTORE DI BUSINESS E PESO DEL TRATTAMENTO**		
16	Considera il suo settore di business incline ad essere oggetto di cyber attacchi?	Quando avvengono gli attacchi alla sicurezza in uno specifico settore di business, c'è una indicazione che l'Azienda potrebbe avere bisogno di adottare misure addizionali per evitare eventi similari
17	Ha la sua Azienda sofferto di cyber attacchi o di altri tipi di attacchi negli ultimi due anni?	Se l'Azienda è stata già attaccata o ci sono sospetti che questo potrebbe essere accaduto, misure addizionali devono essere adottate per prevenire in futuro eventi similari
18	Ha ricevuto mai alcuna notificazione e/o citazione riguardante la sicurezza del sistema di informazione usato per il trattamento dei dati personali negli ultimi due anni?	Bug nella sicurezza/vulnerabilità possono essere sfruttati per eseguire attacchi (fisici o digitali) ai sistemi e ai servizi. Dovrebbero essere considerati comunicazioni sulla sicurezza contenenti informazioni importanti circa le vulnerabilità che possono colpire i sopra menzionati sistemi e servizi
19	I trattamenti dei dati personali riguardano un grande volume di interessati e/o di dati personali?	La tipologia e il volume dei dati personali possono fungere da esca agli attaccanti
20	Esistono specifiche "best practice" per il suo settore di affari che non sono state adeguatamente seguite?	Di solito specifiche misure di sicurezza settoriali sono adattate ai bisogni e ai rischi del particolare settore, la mancanza di adeguamento alle "best practice" potrebbe essere un indicatore di un management povero in sicurezza

Seguendo questo approccio, il livello di probabilità di occorrenza della minaccia può essere definito per ciascuna delle aree di valutazione, come segue:

- Basso: è improbabile che la minaccia si materializzi.
- Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
- Alto: la minaccia potrebbe materializzarsi.

Le tabelle 4 e 5 possono quindi essere utilizzate per documentare la probabilità di occorrenza delle minacce per ciascuna area di valutazione e di conseguenza calcolare il suo valore finale.

Tabella 4: Valutazione della probabilità di occorrenza delle minacce per area

AREA DI VALUTAZIONE	**PROBABILITÀ**	
	LIVELLO	**PUNTEGGIO**
RISORSE TECNICHE E NETWORK	☒Basso	1
	☐Medio	2
	☐Alto	3
PROCESSI/PROCEDURE CORRELATE AL TRATTAMENTO DEI DATI	☒Basso	1
	☐Medio	2
	☐Alto	3
PERSONE E PARTI DIFFERENTI	☒Basso	1

COINVOLTE NEL TRATTAMENTO	☐Medio	2
	☐Alto	3
SETTORE DI BUSINESS E PESO DEL TRATTAMENTO	☒Basso	1
	☐Medio	2
	☐Alto	3

Tabella 5: Valutazione della probabilità di occorrenza di una minaccia

SOMMA TOTALE PROBABILITA' DI VERIFICAZIONE DELLA MINACCIA	LIVELLO DI PROBABILITA' VERIFICAZIONE DELLA MINACCIA
4 -5	Basso
6 - 8	Medio
9 - 12	Alto

La probabilità di occorrenza finale della minaccia viene calcolata dopo aver sommato i quattro diversi punteggi ottenuti nella Tabella 4 e associato il risultato complessivo alle somme globali della Tabella 5.

FASE 3: VALUTAZIONE DEL RISCHIO

Dopo aver valutato l'impatto del trattamento dei dati personali e la probabilità di verificazione della minaccia, è possibile effettuare la valutazione del rischio.

	LIVELLO DI IMPATTO		
	BASSO	**MEDIO**	**ALTO**
BASSO			
MEDIO			
ALTO			

PROBABILITA' DI VERIFICAZIONE DELLA MINACCIA

Legenda:
Rischio basso | Rischio medio | Rischio alto

MISURE DI SICUREZZA

A seguito della valutazione del livello di rischio, l'Associazione può procedere con la selezione delle misure di sicurezza appropriate per la protezione dei dati personali.
Le linee guida ENISA considerano due ampie categorie di misure (organizzative e tecniche), ulteriormente suddivise in sottocategorie specifiche. In ogni sottocategoria vengono presentate le misure per livello di rischio (basso: verde, medio: giallo, alto: rosso).
Al fine di ottenere la scalabilità, si assume che tutte le misure descritte nel livello basso (verde) siano applicabili a tutti i livelli. Allo stesso modo, misure presentate nel livello medio (giallo) sono applicabili anche ad alto livello di rischio. Misure presentate nel livello alto (rosso) non sono applicabili a qualsiasi altro livello di rischio.

A.1 **Misure di sicurezza tecniche e organizzative da adottarsi in caso di rischi alla sicurezza qualificati come di valore BASSO.**

	CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	DESCRIZIONE DELLA MISURA DI SICUREZZA
1	Politica di sicurezza e procedure per la protezione dei dati personali	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.
2	Politica di sicurezza e procedure per la protezione dei dati personali	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.
3	Ruoli e responsabilità	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.
4	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.
5	Responsabili del trattamento	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.
6	Responsabili del trattamento	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.
7	Responsabili del trattamento	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.
8	Gestione degli incidenti / Violazione dei dati personali (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.

9	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).
10	Obblighi di riservatezza imposti al 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 preassunzione e / o assunzione.
11	Formazione	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.
12	Controllo degli 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.
13	Controllo degli 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.
14	Controllo degli 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.
15	Controllo degli 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).
16	Sicurezza delle Postazioni di lavoro	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.
17	Sicurezza delle Postazioni di lavoro	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base settimanale.
18	Sicurezza delle Postazioni di lavoro	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.
19	Sicurezza delle Postazioni di	Il sistema dovrebbe attivare il time-out di sessione quando l'utente non è stato attivo per un certo

	lavoro	periodo di tempo.
20	Sicurezza delle Postazioni di lavoro	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.
21	Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).
22	Back-up	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.
23	Back-up	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
24	Back-up	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
25	Back-up	I backup completi devono essere eseguiti regolarmente.
26	Dispositivi mobili / portatili	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
27	Dispositivi mobili / portatili	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere preregistrati e preautorizzati.
28	Dispositivi mobili / portatili	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.
29	Sicurezza del ciclo di vita delle applicazioni	Dovrebbero essere seguiti standard e pratiche di codifica sicure.
30	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.
31	Cancellazione / eliminazione dei dati	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.
32	Sicurezza fisica	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.

A.2 Misure di sicurezza tecniche e organizzative da adottarsi in caso di rischi alla sicurezza qualificati come di valore MEDIO.

	CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	DESCRIZIONE DELLA MISURA DI SICUREZZA
1	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.
2	Politica di controllo degli accessi	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.
3	Gestione risorse / asset	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.
4	Gestione delle modifiche	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.
5	Responsabili del trattamento	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.
6	Gestione degli 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.
7	Obblighi di riservatezza imposti al 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.
8	Formazione	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.

9	Controllo degli 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.
10	Controllo degli accessi e autenticazione	Le password degli utenti devono essere memorizzate in una forma "hash".
11	Generazione di file di log e monitoraggio	Dovrebbe essere necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.
12	Generazione dei file di log 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.
13	Generazione dei file di log e monitoraggio	Un sistema di monitoraggio dovrebbe generare i file log e produrre report sullo stato del sistema e notificare potenziali allarmi.
14	Sicurezza del server / database	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.
15	Sicurezza del server / database	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.
16	Sicurezza del server / database	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
17	Sicurezza della Postazione di lavoro	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.
18	Sicurezza della rete / comunicazione	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.
19	Sicurezza della rete / comunicazione	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.
20	Sicurezza della rete / comunicazione	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.
21	Back-up	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.
22	Back-up	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.
23	Back-up	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.

24	Back-up	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.
25	Dispositivi mobili / portatili	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.
26	Dispositivi mobili / portatili	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.
27	Dispositivi mobili / portatili	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.
28	Dispositivi mobili / portatili	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
29	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.
30	Sicurezza del ciclo di vita delle applicazioni	Devono essere eseguiti test periodici di penetrazione.
31	Sicurezza del ciclo di vita delle applicazioni	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.
32	Sicurezza del ciclo di vita delle applicazioni	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.
33	Cancellazione / eliminazione dei dati	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.
34	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.
35	Sicurezza fisica	Identificazione chiara, 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.
36	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
37	Sicurezza fisica	I sistemi di rilevamento antintrusione dovrebbero essere installati in tutte le zone di sicurezza.

38	Sicurezza fisica	Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.
39	Sicurezza fisica	Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere attivati nella sala server.
40	Sicurezza fisica	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.

A.3 Misure di sicurezza tecniche e organizzative da adottarsi in caso di rischi alla sicurezza qualificati come di valore ALTO.

	CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	DESCRIZIONE DELLA MISURA DI SICUREZZA
1	Procedure e policy di sicurezza per la protezione dei dati personali	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.
2	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.
3	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.
4	Policy di controllo degli accessi	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff
5	Gestione risorse / asset	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.
6	Responsabili del trattamento	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.
7	Gestione degli incidenti / Violazione dei dati personali (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.
8	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.
9	Business continuity	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.

10	Obblighi di riservatezza imposti al 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).
11	Formazione	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.
12	Controllo degli 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.
13	Controllo degli accessi e autenticazione	Dovrebbe essere soggetto ad autenticazione ogni dispositivo (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale
14	Sicurezza Server/Database	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.
15	Sicurezza della postazione di lavoro	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).
16	Sicurezza della postazione di lavoro	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.
17	Sicurezza della postazione di lavoro	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.
18	Sicurezza della rete / comunicazioni	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.

INDICAZIONI FINALI
(leggere attentamente)

Preso atto delle misure di sicurezza corrispondenti (A1, A2, A3), l'Organizzazione dovrà posizionarsi sulle misure di sicurezza corrispondenti al rischio e, valutati i costi di implementazione delle stesse nonché la loro fattibilità tecnica nel caso concreto, determinare quali misure attivare e quali no (anche

questa scelta rientra nel principio di responsabilizzazione del Titolare o del Responsabile del trattamento).

In caso di controllo, l'organizzazione dovrà dimostrare perché ha scelto determinate misure e non altre. Se vi è un *data breach*, la stessa dovrà dimostrare che la violazione dei dati si è verificata "nonostante" le misure prescelte (quindi, che la violazione non era prevedibile ed evitabile e che le misure erano adeguate ad evitare o mitigare il rischio).

Non implementare alcuna misura di sicurezza conduce l'organizzazione ad una inevitabile sanzione.

ATTENZIONE:

Le misure che l'Organizzazione adotterà vanno riportate nei Registri delle Attività di Trattamento, nella colonna "MISURE TECNICHE ED ORGANIZZATIVE ADOTTATE (E RIMANDI AD EVENTUALI ALLEGATI DI DETTAGLIO)", dove dovrà riportarsi la Sezione e il numero delle misure di sicurezza adottate (Es. A1, 1-2-3-5-8; oppure A2, 3-6-8 ecc.).