Manuale sulla Sicurezza nel trattamento dei dati personali

DICEMBRE 2017

Sommario

Disclaimer

Il presente documento è riservato ad un uso strettamente privato. Esso costituisce una traduzione non ufficiale della pubblicazione "Handbook on Security of Personal Data Processing" elaborato dall'ENISA (European Union Agency for Network and Information Security), alla quale sono riservati tutti i diritti. Non si fornisce alcuna garanzia in merito all'affidabilità ed all'esattezza delle notizie riportate, ovvero della esattezza delle traduzioni.

Si declina pertanto ogni responsabilità per qualsiasi danno, diretto, indiretto, incidentale e consequenziale legato all'uso, proprio o improprio delle informazioni contenute in questo documento, ivi inclusi, senza alcuna limitazione, la perdita di profitto, l'interruzione di attività aziendale o professionale, la perdita di programmi o altro tipo di dati ubicati sul sistema informatico dell'utente o altro sistema, e ciò anche qualora gli Autori del documento fossero stati espressamente messi al corrente della possibilità del verificarsi di tali danni.

Curatori del progetto di traduzione

(in ordine alfabetico)

Coordinamento e Revisione

Rosario Mauro Catanzaro

Alessandro del Ninno

Traduzioni

Rino Cannizzaro

Giacomo Conti

Vittoria Diotallevi

Alessandro Feltrin

Alessandro Flacco

Roberto Formigoni

Fabiana Lo Sicco

Claudia Ogriseg

Giulia Spinoglio

Floriana Tagliaferro

Luca Visconti

Executive Summary

Il Regolamento generale sulla protezione dei dati (UE) 679/2016 ("GDPR") sarà, dal 25 maggio 2018, il principale testo normativo sulla la protezione dei dati nell'UE. Esso sarà direttamente applicabile a tutti gli Stati membri e abrogherà l'attuale direttiva sulla protezione dei dati 95/46/CE. Attualmente, le imprese nella UE devono conformarsi a 28 diverse legislazioni nazionali i sulla protezione dei dati. Tale frammentazione rappresenta un costoso onere amministrativo che rende difficoltoso per molte aziende, in particolare le PMI, l'accesso a nuovi mercati.

Ai sensi del Regolamento, uno degli obblighi fondamentali per tutte le imprese, comprese le PMI, che agiscono in qualità di Titolari o di Responsabili del trattamento , è quello della sicurezza nel trattamento dei dati personali. In particolare, secondo il GDPR, la sicurezza è una tematica che include anche quelle della riservatezza, integrità e disponibilità dei dati e dovrebbe essere considerata seguendo un approccio basato sul rischio: più alto è il rischio e più rigorose devono essere le misure che il Titolare o il Responsabile del trattamento devono considerare (per gestire il rischio). Anche se questo approccio basato sul rischio non è un nuovo concetto, sono stati presentati solo alcuni specifici quadri di valutazione del rischio per la privacy, focalizzandosi principalmente sulla valutazione del rischio sui dati personali e sull'adozione di adeguate misure di sicurezza pertinenti.

Su questa base e come parte del suo continuo supporto sull'implementazione delle policy EU, ENISA ha pubblicato nel 2016 una serie di linee guida per le PMI, che agiscono come Titolare o come Responsabile del trattamento, il cui scopo era di essere d'aiuto nell'analisi dei rischi di sicurezza e nella conseguente adozione di contromisure di sicurezza per la protezione dei dati personali. Tali linee guida possono anche essere utili in tutti i casi in cui è prevista la valutazione del rischio ai sensi del Regolamento (ad esempio la Valutazione dell'impatto sulla protezione dei dati (DPIA), la notifica di violazioni di dati personali, etc).

Nel corso del 2017 l'Agenzia ha continuato le sue attività nell'area e si è concentrata sulla fornitura di ulteriori indicazioni sull'applicazione delle sopradescritte linee guida attraverso casi di utilizzo specifici. In stretta collaborazione con gli esperti delle autorità nazionali per la protezione dei dati, ciascun caso pratico corrisponde ad una specifica operazione di trattamento dei dati personali e porta a specifiche considerazioni sull'ambiente di trattamento dei dati e su tutto il contesto del trattamento. Gli esempi forniti si focalizzano solo sulle misure di sicurezza e non mirano a fornire alcuna analisi di tipo legale e nemmeno alcuna valutazione di conformità al GDPR per la specifica operazione di trattamento dei dati. Durante l'esecuzione delle analisi, sono state tratte una serie di conclusioni e raccomandazioni pertinenti, rivolte a diversi soggetti interessati, presentate di seguito.

- Gli organismi competenti dell'UE, i responsabili delle politiche e i regolatori dell'UE (ad esempio il Garante per la Protezione dei Dati) dovrebbero definire e promuovere dei modelli di certificazione scalabili per la Protezione dei dati, che siano in grado di supportare e assistere diversi tipi di responsabili del trattamento dei dati e affrontare le comunità di stakeholder specifici.
- Gli organismi competenti dell'UE, i responsabili delle politiche e i regolatori dell'UE (ad esempio le autorità per la protezione dei dati) dovrebbero individuare una serie di competenze e requisiti professionali di base che i Titolari e Responsabili della protezione dei dati dovrebbero soddisfare.
- La comunità di ricerca e gli organismi competenti, in stretta collaborazione con i regolatori (ad esempio il Garante per la Protezione dei Dati), dovrebbero proporre metodologie che armonizzino

la gestione dei rischi inerenti la sicurezza dei dati e delle informazioni e la gestione del rischio per i dati personali.

- le associazioni di PMI, in stretta collaborazione con gli Organismi competenti dell'UE e con i regolatori (ad esempio il Garante per la Protezione dei Dati), dovrebbero informare e incoraggiare i Titolari del trattamento ad intraprendere azioni nella direzione della Security e della compliance alla Privacy come un vantaggio competitivo oltre che per rispettare i soli obblighi di legge.

1. Introduzione

1.1 Background

Il Regolamento Generale per la Protezione dei dati (EU) 679/2016[1] ('GDPR') sarà, a far data dal 25 Maggio 2018, il principale testo normativo sulla protezione dei dati nella Unione Europea , direttamente applicabile a tutti gli Stati membri, in revoca all'attuale Direttiva sulla Protezione dei dati 95/46/EC[2]. Ai sensi del Regolamento, uno dei principali obblighi per tutte le imprese, sia che agiscano come Titolare che come Responsabile del trattamento, è finalizzato alla sicurezza delle operazioni di trattamento dei dati personali.

Sebbene la sicurezza dei dati personali sia già un obbligo giuridico per i Titolari del trattamento dei dati ai sensi della Direttiva per la Protezione dei dati, il GDPR rafforza le disposizioni normative (sia nella sostanza che nel contesto), estendendo direttamente anche ai Responsabili del trattamento gli obblighi in materia di sicurezza..

In particolare la sicurezza nel trattamento dei dati personali è in via primaria regolata dall'articolo 32 del GDPR, il quale afferma che:

"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento."

Tale articolo stabilisce inoltre che "*Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".* Viene inoltre indicato che l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 41 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di sicurezza nel trattamento . Infine, l'articolo 32 prescrive che il Titolare del trattamento e il Responsabile del trattamento *"fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".*

[1] http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679
[2] http://eur-lex.europa.eu/eli/dir/1995/46/oj

Secondo quanto sopra riportato, nel GDPR la sicurezza è tematica che include in modo omogeneo quelle relative alla riservatezza, integrità e disponibilità dei dati e dovrebbe essere considerata nella prospettiva dell'approccio basato sul rischio (*risk-based approach*) e cioè: tanto più elevato è il livello di rischio (per i diritti e la libertà degli interessati), tanto più stringenti devono essere le misure che il Titolare o il Responsabile necessitano di considerare (per la gestione del rischio). Ancora, la sicurezza nel trattamento dovrebbe essere considerata nel complessivo contesto della *accountability* ("*documentabilità*") degli adempimenti e della conformità ai principi del GDPR dal momento che l'accountability è altresì da considerarsi nella prospettiva *risk-based* ed *impact-based* ed è finalizzata ad applicarsi in ogni specifico contesto operativo e nei processi di un'organizzazione.

Tenendo conto delle considerazioni sopra esposte, l'ENISA ha emanato nel 2016 una serie di linee guida per le PMI che agiscono come Titolari o Responsabili del trattamento finalizzate a fornire elementi di supporto per la valutazione dei rischi per la sicurezza e a indicare conseguenti misure di sicurezza per la protezione dei dati personali. Nell'ambito del suo programma di lavoro 2017, l'ENISA ha deciso di continuare questo lavoro fornendo esempi pratici sull'applicazione delle linee guida da parte delle PMI.

1.2 Ambito di applicazione e obiettivi

La finalità generale di questo Manuale è quella di fornire esempi concreti e criteri interpretativi delle linee guida 2016 dell'ENISA per le PMI[3] relative alla sicurezza nel trattamento dei dati personali. Questo obiettivo viene perseguito attraverso l'esame di casi pratici e di prassi operative comuni a tutte le PMI.

Per ogni ipotesi esaminata, le linee guida dell'ENISA vengono applicate al fine di valutare il rischio concreto (per i diritti e le libertà degli interessati) e nell'ottica di adottare le misure tecniche e organizzative adeguate al rischio presentato.

Il presente Manuale si rivolge principalmente alle PMI che agiscono come Titolari o Responsabili del Trattamento e che possono utilizzare gli esempi pratici forniti in questa sede come supporto pratico di riferimento per svolgere la propria valutazione dei rischi connessi al trattamento dei dati personali e per valutare l'adozione di adeguate misure di sicurezza, nell'ambito del più ampio contesto di attuazione di misure volte a garantire la conformità dei trattamenti al GDPR. Peraltro, anche le Autorità per la Protezione dei Dati potrebbero trovare d'interesse i casi in esame, sia nell'ambito del quadro di riferimento per i propri audit relativi alla protezione dei dati, che nelle proprie raccomandazioni sulla sicurezza.

Si evidenzia come mentre le linee guida ENISA del 2016 ricomprendono ogni ipotesi di trattamento di dati personali, il presente Manuale si concentra principalmente sui processi di elaborazione elettronica dei dati personali posti in essere dalle PMI, laddove questi si basino su reti e sistemi informatici, nonché su nuove tecnologie digitali (ad esempio cloud computing, dispositivi mobili, ecc).

relazione Infine, il Manuale si concentra esplicitamente sulle misure di sicurezza e non ha l'obiettivo di effettuare alcuna analisi legale o valutazione della conformità di specifiche operazioni di trattamento dei dati.

1.3 Metodologia

Il presente Manuale è stato redatto da un gruppo di esperti, composto da Georgia Panagopoulou (Autorità Garante della Protezione dei Dati Ellenica) e Giuseppe D'Acquisto (Autorità Garante della Protezione dei Dati Italiana).

3 https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Un certo numero di operazioni di trattamento sono state identificate come le più tipiche o, comunque, come quelle che risultano più frequenti nella prassi per la maggior parte delle PMI. Tali tipologie di trattamento sono state quindi convalidate, per quanto possibile, con i Titolari del trattamento interessati.

1.4 Struttura

Il presente documento è strutturato come segue:

- Il capitolo 2 fornisce una panoramica delle fasi metodologiche relative alla valutazione dei rischi per la sicurezza all'interno delle PMI, alla luce di quanto già proposto nel 2016.
- I capitoli da 3 a 7 presentano casi pratici selezionati, corredati da un'analisi di ciascuna operazione di trattamento e del calcolo del livello generale di rischio, sulla base delle fasi metodologiche descritte in precedenza.
- Il capitolo 8 riporta una serie di osservazioni e conclusioni finali in merito all'attuazione dell'approccio proposto da parte delle PMI.

Il rapporto integra il precedente lavoro dell'ENISA nei settori della privacy e della sicurezza dei dati personali[4].

[4] Per ulteriori informazioni, consulta: https://www.enisa.europa.eu/topics/data-protection

2. Valutazione del rischio e misure di sicurezza per i dati personali

L'ENISA, nelle sue linee guida per il 2016[5], ha illustrato un approccio semplificato che può guidare le PMI (operanti come titolari o responsabili) attraverso le loro specifiche operazioni di trattamento dei dati, supportandole nella valutazione dei rischi rilevanti per la sicurezza e adottando, di conseguenza, misure di sicurezza.

In questo capitolo si fornisce una breve panoramica delle linee guida 2016 dell'ENISA che verranno utilizzate nel resto del Manuale per fornire esempi pratici. Si evidenzia altresì la nozione di "Scenari pratici" su cui saranno costruiti esempi di scenari di trattamento dati.

2.1 Panoramica dei passaggi metodologici

Le linee guida dell'ENISA per le PMI propongono 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, le PMI possono adottare misure di sicurezza tecniche e organizzative (da un elenco proposto) che sono appropriate al livello di rischio.

2.1.1 Step 1: Definizione dell'operazione di trattamento e del suo contesto

Questo passaggio è il punto di partenza della valutazione del rischio ed è fondamentale per il Titolare del trattamento al fine di definire i confini del sistema di trattamento dei dati oggetto di valutazione e *assessment* e del relativo contesto. Per supportare le PMI nella definizione dell'operazione di trattamento viene fornita una serie di domande.

1. Cos'è l'operazione di trattamento dei dati personali?
2. Quali sono le tipologie di dati personali trattati?
3. Qual è la finalità del trattamento?
4. Quali sono gli strumenti utilizzati per il trattamento dei dati personali?
5. Dove avviene il trattamento dei dati personali?
6. Quali sono le categorie di soggetti interessate?
7. Chi sono i destinatari dei dati?

Rispondendo a queste domande, una PMI deve considerare le varie fasi del trattamento dei dati (raccolta, conservazione, utilizzo, trasferimento, comunicazione, ecc.) e dei loro successivi parametri.

2.1.2 Step 2: Comprensione e valutazione dell'impatto

Sulla base dell'analisi dello Step 1, il Titolare del trattamento in questa fase deve valutare l'impatto sui diritti e sulle libertà fondamentali delle persone fisiche derivanti dalla possibile perdita di sicurezza dei dati

[5] https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

personali. Vengono considerati quattro livelli di impatto (Basso, Medio, Alto, Molto alto) come mostrato nella Tabella 1 di seguito.

LIVELLO DI IMPATTO	DESCRIZIONE
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Tabella 1: descrizione dei livelli di impatto

La valutazione d'impatto è un processo qualitativo e il Titolare del trattamento deve considerare una serie di fattori quali la tipologia di dati personali, la criticità dell'operazione di trattamento, il volume dei dati personali, le caratteristiche speciali del Titolare del trattamento, come anche le speciali categorie di interessati.

Per supportare il Titolare del trattamento in questo processo, la Tabella 2 può essere utilizzata per valutare separatamente l'impatto dalla perdita di riservatezza, integrità e disponibilità dei dati.

Dopo questa valutazione, saranno ottenuti tre diversi livelli di impatto (per la perdita di riservatezza, integrità e disponibilità). Il più alto di questi livelli è considerato come il risultato finale della valutazione dell'impatto, relativo al trattamento complessivo dei dati personali.

N.	DOMANDA	VALUTAZIONE
I.1.	**Si prega di riflettere sull'impatto che una divulgazione non autorizzata (perdita di riservatezza) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.**	☐ Basso ☐ Medio ☐ Alto ☐ Molto Alto
I.2.	**Si prega di riflettere sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.**	☐ Basso ☐ Medio ☐ Alto ☐ Molto Alto
I.3.	**Si prega di riflettere sull'impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.**	☐ Basso ☐ Medio ☐ Alto ☐ Molto Alto

Tabella 2: domande di valutazione d'impatto

2.1.3 Step 3: Definizione di possibili minacce e valutazione della loro probabilità

In questa fase, lo scopo del Titolare del trattamento è comprendere le minacce correlate al contesto complessivo del trattamento dei dati personali (esterno o interno) e valutare la loro probabilità (probabilità di accadimento della minaccia).

Per semplificare questo processo, sono state definite una serie di domande di valutazione che mirano a sensibilizzare le PMI sull'ambiente di elaborazione dei dati (che è direttamente rilevante per le minacce). In tale prospettiva, le domande sono relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati , vale a dire:

- Risorse di rete e tecniche (hardware e software)
- Processi / procedure relativi all'operazione di trattamento dei dati
- Diverse parti e persone coinvolte nell'operazione di trattamento
- Settore di operatività e scala del trattamento

La Tabella 3 riassume le domande relative alla valutazione della probabilità di occorrenza di una minaccia.

A. RISORSE DI RETE E TECNICHE		
1.	**Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?**	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.
2.	**È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?**	Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.
3.	**Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?**	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate a tale accesso).
4.	**Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?**	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).
5.	**Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?**	Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.

- **B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI**

6.	**I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?**	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema.
7.	**L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?**	Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.
8.	**I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?**	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.
9.	**I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?**	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni.
10.	**Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?**	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali.
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI		
11.	**Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?**	Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.
12.	**Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?**	Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.

13.	**Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?**	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.
14.	**Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?**	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.
15.	**Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?**	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO		
16.	**Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?**	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento , questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile.
17.	**La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?**	Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.
18.	**Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?**	Bug di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.
19.	**Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?**	Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).
20.	**Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?**	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della 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.

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
RETE E RISORSE TECNICHE	Basso	1
	Medio	2
	Alto	3
PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto	3
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto	3
SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Basso	1
	Medio	2
	Alto	3

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

Somma globale della probabilità di occorrenza di una minaccia	LIVELLO DI PROBABILITÀ DELLE MINACCE
4 - 5	Basso
6 - 8	Medio
9 -12	Alto

Tabella 5: Valutazione della probabilità di occorrenza di una minaccia

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.

2.1.4 Step 4: Valutazione del rischio

Dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la probabilità di accadimento della minaccia rilavante, la valutazione finale del rischio è possibile (Tabella 6).

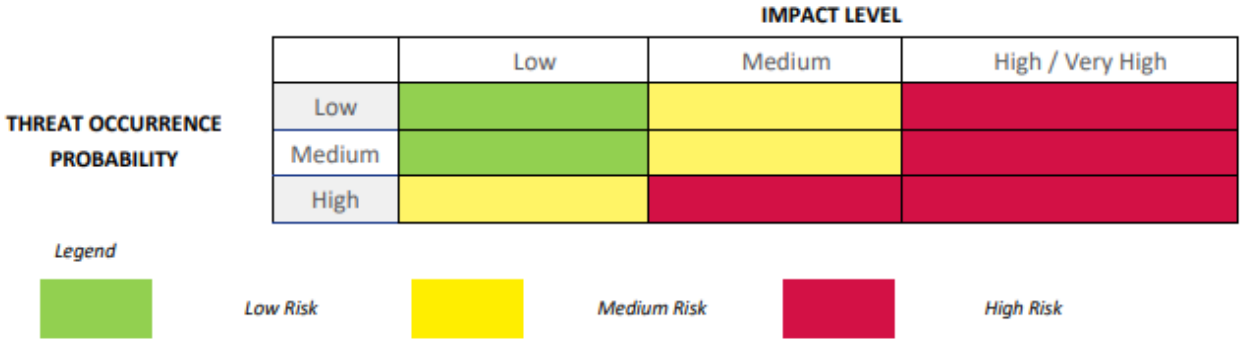

Tabella 6: Valutazione del rischio

Indipendentemente dal risultato finale di questo esercizio, la PMI dovrebbe sentirsi libera di adeguare il livello di rischio ottenuto, tenendo conto delle caratteristiche specifiche dell'operazione di trattamento dei dati (che sono state omesse durante il processo di valutazione) e fornendo un'adeguata giustificazione per tale adeguamento.

2.1.5 Step 5: Misure di sicurezza

A seguito della valutazione del livello di rischio, la PMI 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.

Si veda l'Allegato A che riporta l'elenco delle misure tecniche e organizzative proposte per livello di rischio.

Va notato che l'abbinamento di misure a specifici livelli di rischio non dovrebbe essere percepito come assoluto. A seconda del contesto del trattamento dei dati personali, l'organizzazione può considerare l'adozione di misure aggiuntive, anche se sono assegnate a un livello di rischio più elevato. Inoltre, l'elenco proposto di misure non tiene conto di altri requisiti di sicurezza specifici settoriali aggiuntivi, nonché di obblighi normativi specifici, derivanti ad esempio dalla direttiva e-privacy[6] o dalla direttiva NIS[7]. Nel tentativo di facilitare ulteriormente questa procedura è inclusa anche una mappatura del gruppo di misure proposto con i controlli di sicurezza ISO/IEC 27001: 2013[8].

[6] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche): http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32002L0058&from=IT : http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A32002L0058

[7] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L1148&from=IT http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1481193515962&uri=CELEX:32016L1148

[8] ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements http://www.iso.org/iso/catalogue_detail?csnumber=54534

2.2 Scenari pratici e approccio utilizzato nel Manuale

Come già accennato, il presente Manuale fornisce ulteriori indicazioni sull'applicazione delle linee guida dell'ENISA (sezione 2.1) basate su scenari pratici Ogni scenario pratico corrisponde a una specifica operazione di trattamento dei dati personali e formula ipotesi specifiche sull'ambiente di trattamento dei dati e sul contesto generale del trattamento.

A tal fine, nel contesto delle PMI dell'UE, sono state identificate diverse operazioni di trattamento. Queste operazioni di trattamento variano da processi relativi alle risorse umane (HR), fornitura di beni, a marketing e sicurezza fisica / controllo degli accessi. Oltre a queste categorie generali, vengono presi in considerazione alcuni specifici Scenari pratici nei settori della salute e dell'istruzione.

Per ogni scenario pratico viene fornita una descrizione dell'operazione di trattamento, ivi inclusa l'analisi dei presupposti e delle specifiche condizioni che sono state prese in considerazione. Viene quindi effettuata la valutazione del rischio, sulla base dei presupposti dello specifico trattamento e delle varie fasi del trattamento. In alcuni scenari pratici presi in considerazione sono altresì menzionati specifici parametri che potrebbero modificare il rischio complessivo. A seguito della valutazione del rischio, è possibile adottare le misure di sicurezza appropriate (al livello di rischio identificato) in base all'Allegato A al presente Manuale:

Il calcolo del rischio per ciascuno scenario pratico dovrebbe essere considerato solo come un esempio dell'applicazione delle line guida dell'ENISA nell'ambito dello specifico scenario.

Non può essere considerato applicabile a priori alle relative operazioni di trattamento dei dati.

Si consiglia al Titolare del trattamento di iniziare con gli esempi forniti e di eseguire ulteriormente la valutazione in base al contesto e allo specifico ambiente di trattamento dei dati.

Gli Scenari Pratici si concentrano unicamente sulle misure di sicurezza e non mirano a fornire alcuna analisi legale o valutazione della conformità a GDPR per le specifiche operazioni di elaborazione dei dati.

A tal fine, tutte le ipotesi formulate nell'ambito degli Scenari pratici hanno il solo scopo di illustrare operativamente taluni esempi pratici e non forniscono alcuna indicazione in merito alla legalità / conformità di specifiche operazioni di trattamento dei dati.

3. Scenario pratico: Processi relativi alle Risorse Umane

Una tipica PMI tratta i dati personali dei propri lavoratori in quanto parte delle attività di gestione delle Risorse Umane (HR). A seconda della natura delle attività svolte dal Titolare del trattamento , delle dimensioni e dell'organizzazione interna di una PMI, le attività di gestione delle Risorse Umane possono prevedere procedure aggiuntive che implicano il trattamento di ulteriori dati personali o semplicemente implicano il perseguimento di diverse finalità . I trattamenti di dati personali più ricorrenti che vengono in tale sede presi in considerazione con riferimento alla gestione delle Risorse Umane sono: a) Gestione delle retribuzioni/stipendi, b) Gestione delle dimissioni/assenze, c) Reclutamento e d) Valutazione del personale. Altre operazioni potrebbero includere i dati sanitari del personale (ad esempio i controlli medici dei dipendenti, la formazione del personale, etc).

3.1 Gestione degli stipendi

All'interno di questo scenario si consideri una PMI di vendita al dettaglio che tratta dati personali dei suoi lavoratori a fini salariali, di corresponsione di benefit e a fini previdenziali . I dati personali oggetto di trattamento considerati sono: informazioni di contatto (come cognome, nome, indirizzo e telefono), numero della Previdenza Sociale, codice fiscale, data di assunzione, livello di inquadramento lavorativo e informazioni salariali. Il trattamento è svolto mediante il sistema IT del Dipartimento Risorse Umane, che è allocato presso la sede della PMI e viene utilizzato dal Responsabile del Dipartimento delle Risorse Umane . Sempre inquadrando gli elementi dello scenario pratico qui considerato, va evidenziato che esiste una specifica policy in vigore per regolare l'utilizzo dei sistemi IT. Tuttavia, non vi sono policies specifiche relative alla conservazione dei dati né relative alla loro distruzione. Il trattamento dei dati personali è limitato ai locali della società. Verso la fine di ogni mese, il Responsabile HR invia all'Amministrazione Finanziaria e agli enti pubblici proposti a fini previdenziali le dichiarazioni per tutti i lavoratori . Sebbene il Responsabile HR abbia firmato un accordo di riservatezza, non è stata recentemente eseguita alcuna formazione in materia di sicurezza o protezione dei dati per i dipendenti della PMI.

L'attività di trattamento dei dati può essere descritta come segue:

DESCRIZIONE ATTIVITA' DI TRATTAMENTO	GESTIONE DELLE PAGHE DEI DIPENDENTI	
Dati Personali oggetto di trattamento	**Informazioni generali (Cognome, nome, indirizzo, numero di telefono), Codice di previdenza sociale, Codice Fiscale, data di assunzione, informazioni salariali**	
Finalità del trattamento	**Gestione paghe e stipendi (pagamento del salario, emolumenti, benefits e contributi previdenziali)**	
Soggetti interessati	**Lavoratori**	
Strumenti impiegati nel trattamento	**Sistemi IT dell'Ufficio Risorse Umane**	
Destinatari dei dati	**Esterno**	**Amministrazione Finanziaria**
	Esterno	**Istituti Previdenziali**
Responsabile del Trattamento	**Interno (nessun Responsabile esterno del trattamento)**	

3.1.1 Valutazione d'impatto

Facendo seguito alle modalità di approccio evidenziate alla sezione 2.1.2, la successiva analisi sarà effettuata nel seguente modo:

Perdita di riservatezza

Nell'ambito della finalità del trattamento rappresentata dalla gestione di paghe e stipendi dei lavoratori , come descritto sopra, l'impatto dovuto alla eventuale perdita di riservatezza è legato principalmente ad una potenziale divulgazione involontaria del reddito (e di altri dati rilevanti) a terze parti. Ciò potrebbe esporre l'interessato a conseguenze che vanno dal disagio derivante dalla conoscenza pubblica dei propri dati personali relativi alla retribuzione e, in casi limite, al rischio potenziale di attacchi mirati, furti e ricatti. Un risultato di questo tipo potrebbe quindi trasformarsi in più di un semplice disagio. L'impatto della perdita di informazioni andrebbe quindi impostato su **MEDIO.**

Perdita di Integrità e di disponibilità

La perdita di integrità e/o quella della disponibilità dei dati personali possono essere generalmente considerate su un valore **BASSO,** dal momento che i soggetti interessati si aspettano già di dover avere a che fare con inconvenienti come il dover rinviare le informazioni oppure di non ricevere i bonifici del proprio salario nei tempi concordati, a patto che i problemi possano essere rapidamente superati. Un impatto più importante rispetto alla perdita di riservatezza potrebbe spostare la valorizzazione a **MEDIO** qualora le conseguenze sui soggetti interessati fossero persistenti nel tempo (come ad esempio un ripetuto ritardo nel pagamento del salario). Tale scenario però non è considerato nel presente scenario pratico esemplificativo.

La Tabella che segue riassume analisi appena sopra svolta:

ANALISI D'IMPATTO		
Riservatezza	Integrità	Disponibilità
Medio	**Basso**	**Basso**
	Valutazione di impatto Globale	**Medio**

Il risultato complessivo della valutazione dell'impatto è il più alto identificato. Pertanto, l'impatto complessivo in questo caso particolare viene valutato come **MEDIO**.

Oltre alle ipotesi formulate nello scenario pratico appena sopra esaminato potrebbero darsi ipotesi di impatto complessivo superiore a quello calcolato nello scenario analizzato. . Una tale ipotesi potrebbe darsi nei seguenti scenari:

- trattamento sistematico di dati di particolare natura relativi a specifici stati sanitari o a dati sulla salute / disabilità (ad esempio dovuti a privilegi/accordi di lavoro, come permessi straordinari assegnati a dipendenti disabili o svantaggiati). In tali casi il Titolare del trattamento dovrebbe considerare se il livello di impatto possa essere alzato a **ALTO**

3.1.2 Probabilità di occorrenza di una minaccia

Sulla base delle domande e delle modalità di approccio esposte alla Sezione 2.1.3, la seguente verifica può essere svolta per ciascuna area dell'ambiente specifico di trattamento dei dati (cioè il sistema IT delle Risorse Umane) che è stato portato come esempio nel presente scenario pratico :

- **Risorse tecniche e di rete:** la probabilità di accadimento della minaccia è **BASSA**, visto che il Sistema non è connesso a Internet e non permette accesso da Internet alle risorse interne di altri Sistemi IT. Viene assunto per questo scenario pratico che l'accesso non autorizzato sia gestito come rischio seguendo delle adeguate linee guida di sicurezza interne e buone prassi. .
- **Processi/Procedure relativi alla operazione di trattamento dei dati personali:** la probabilità di accadimento della minaccia è BASSA, assumendo che ruoli e responsabilità del responsabile della funzione HR siano chiaramente definiti ed allineati alle policies interne del Titolare del trattamento e che il trattamento dei dati personali sia ristretto alla sede dell'organizzazione e che vengano prodotti files di log per ciascuna attività di trattamento.
- **Gruppi/Persone coinvolte nel trattamento di dati personali:** la probabilità di accadimento della minaccia è **MEDIO** visto che gli addetti HR non hanno ricevuto una appropriata formazione sulla sicurezza dei dati e non vi è certezza che i dati personali vengano sempre trattati e/o distrutti in modalità sicura (a fronte di policy non definite in modo completo/appropriato -).
- **Settori di operatività e scala del trattamento :** la probabilità di accadimento della minaccia è **BASSA** visto che il settore di operatività della PMI non è, in generale, considerato a rischio di cyber attacchi. Viene assunto che nessuna violazione o furto di dati sia nota o accaduta in passato e che le operazioni di trattamento siano eseguite unicamente dal personale della PMI.

AREA DI VALUTAZIONE	PROBABILITA	
	LIVELLO	PUNTEGGIO
Rete e risorse tecnologiche	Basso	1
Processi/Procedure collegate all'elaborazione dei dati personali	Basso	1
Terze parti / persone coinvolte nell'elaborazione dei dati personali	Medio	2
Settori di Business e loro peso nei processi di elaborazione	Basso	1
Probabilità di accadimento	Basso (5)	

3.1.3 Valutazione del rischio e adozione di misure di Sicurezza

Facendo uso dei risultati dalla valutazione di impatto e della probabilità di accadimento delle minacce, il rischio è calcolato sulla base di quanto indicato alla Sezione 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low		X	
	Medium			
	High			

Il rischio globale per questo caso particolare viene generalmente considerato come MEDIO. Gli Allegato A (A.1 e A.2) possono essere utilizzati per l'adozione delle misure appropriate al rischio da trattare.

Si tenga conto che il rischio potrebbe essere differente (più elevato) in presenza di condizioni particolari del trattamento o in rapporto a particolari dati personali trattati con la conseguenza di diverse valutazioni (sul rischio più elevato) che potrebbero interessare l'impatto del trattamento sulla sfera

personale degli interessati e la probabilità di accadimento delle minacce (si prega di fare riferimento alle relative considerazioni riportate nella sezione 3.1.2).

3.2 Selezione del Personale

All'interno di questo scenario si consideri la medesima PMI descritta nella sezione 3.1. La selezione del personale è un processo gestito dalle Risorse Umane e consiste in numerose attività organizzative che hanno lo scopo di selezionare persone che possiedono specifiche capacità oppure che siano in grado di portare a termine determinati compiti. Successivamente alla pubblicazione dell'avviso che informa i candidati della presenza di un posto vacante, questi sono invitati a presentare la loro candidatura elettronica accompagnata da un curriculum vitae dettagliato, nel quale saranno indicati la formazione accademica, le esperienze lavorative, un'ulteriore formazione professionale o accademica, lo stato civile e dettagli personali come nome e cognome, indirizzo, numeri di telefono, data di nascita. Il comitato di selezione, dopo aver esaminato e valutato le candidature, redige una lista di candidati che saranno invitati a fare un colloquio. Durante il colloquio, i membri del comitato di selezione prendono appunti sulla performance del candidato e alla fine abbozzano un resoconto dettagliato che sarà presentato all'alta direzione. Il trattamento dei dati avviene in modo semplice ed intuitivo grazie ad un sistema IT che supporta la presentazione delle candidature, la preselezione dei candidati e i resoconti dei colloqui, e che è gestito da un incaricato delle Risorse Umane.

3.2.1 Definizione di operazione di trattamento e del suo contesto

DESCRIZIONE DELL'OPERAZIONE DI TRATTAMENTO	SELEZIONE	
Dati personali oggetto del trattamento	**Formazione accademica, esperienza lavorativa, ulteriore formazione professionale o accademica, stato civile, nome e cognome, indirizzo, numero di telefono, data di nascita, resoconto/appunti del colloquio**	
Finalità del trattamento	**Gestione dei candidati selezionati per la selezione**	
Interessati	**Candidati alla procedura selettiva**	
Strumenti impiegati per il trattamento	**Piattaforma IT per la selezione**	
Destinatari dei dati	**Interni**	**direzione Senior Management**
Responsabile dei dati	**In-house (nessun responsabile dei dati)**	

3.2.2 Valutazione d'impatto

Seguendo l'approccio presentato nella sezione 2.1.2, è dunque possibile procedere alla seguente analisi :

Perdita di riservatezza

Nel contesto della selezione del personale, come descritto sopra, la perdita di riservatezza potrebbe comportare la diffusione dei dati dei candidati causando loro imbarazzo quando non lesione della reputazione . Tali conseguenze della illecita diffusione potrebbero essere per lo più riconducibili ai risultati finali che potrebbero fornire una valutazione dell'esperienza lavorativa e delle capacità professionali del candidato ed anche di altre qualità personali (ad esempio capacità comunicative o capacità di esprimersi chiaramente). In questo scenario pratico utilizzato come esempio per condurre la valutazione di sicurezza

si è preso in considerazione il presupposto che la piattaforma di selezione preveda una valutazione strutturata del candidato, basata su criteri professionali specifici, e non includa altri tipi di valutazioni della personalità o delle caratteristiche del candidato (ad esempio, profilo psicologico). Seguendo la sopra menzionata impostazione , può prevedersi che in conseguenza della perdita di riservatezza l'interessato possa andare incontro a disagi che possono qualificarsi da minimi a gravi fino ad influenzare la stessa possibilità del candidato di essere assunto. Di conseguenza, in questo caso pratico, l'impatto può in generale essere considerato MEDIO.

Perdita di integrità

L'impatto derivante dalla perdita di integrità dei dati va considerato MEDIO, dato che modifiche non autorizzate dei dati personali trattati potrebbero sia ostacolare il positivo completamento della procedura di selezione, sia modificare l'idoneità/il resoconto del colloquio del candidato (di conseguenza, anche la possibilità che il candidato sia assunto).

Perdita di disponibilità

L'impatto della perdita di disponibilità va considerato BASSO, dato che si prevede che gli interessati vadano incontro a disagi minori, semplicemente dovuti al ritardo del processo di selezione che però non viene invalidato. La tabella sotto riassume la suddetta analisi.

VALUTAZIONE DELL'IMPATTO		
Riservatezza	Integrità	Disponibilità
Medio	Medio	Basso
Valutazione complessiva dell'impatto		**Medio**

Il risultato complessivo della valutazione dell'impatto è il più elevato individuato in questa analisi e, di conseguenza, l'impatto complessivo rilevato è MEDIO.

Inoltre, considerando i presupposti dello scenario pratico presentato come esempio , ci potrebbero essere ipotesi di impatto complessivo persino più elevato rispetto a quello calcolato sopra. Per esempio, questo potrebbe essere il caso di un processo di valutazione che include test psicologici o psicoattitudinali oppure caratteristiche comportamentali specifiche dei candidati. Un tale risultato si potrebbe presentare nel caso in cui siano stati trattati anche i dati personali relativi a disabilità, origine etnica ecc.

3.2.3 Probabilità di occorrenza di una minaccia

Sulla base delle domande presentate nella sezione 2.1.3, è stata sviluppata la seguente valutazione per ogni aspetto dell'ambiente delle operazioni del trattamento:

- **Risorse di rete e tecniche:** la probabilità che una minaccia si verifichi è BASSA, dato che il trattamento non è eseguito attraverso internet e la piattaforma IT impiegata per la valutazione è un sistema dedicato non è connesso a nessun altro sistema IT della PMI. Come negli esempi precedenti, l'assunzione di partenza è che presso tale PMI siano applicate best practices per evitare accessi non autorizzati e, di conseguenza, si assume che esse siano atte a garantire la protezione dei dati.
- **Processi/Procedure relativi alla operazione di trattamento dei dati personali:** la probabilità di accadimento della minaccia è BASSA, assumendo che ruoli e responsabilità del responsabile della funzione HR siano chiaramente definiti ed allineati alle policies interne del Titolare del trattamento

e che il trattamento dei dati personali sia ristretto alla sede dell'organizzazione e che vengano prodotti files di log per ciascuna attività di trattamento.

- **Parti/persone coinvolte nel trattamento dei dati personali:** la probabilità che si verifichi una minaccia è MEDIA, in quanto comprende un grande numero di impiegati coinvolti nel trattamento (l'uffici delle risorse umane, il comitato di selezione, il senior management). Inoltre, si presuppone che non tutti gli impiegati coinvolti nel trattamento abbiano ricevuto un'adeguata formazione sulla sicurezza delle informazioni.
- **Settori di operatività e scala del trattamento:** la probabilità di accadimento della minaccia è **BASSA** visto che il settore di operatività della PMI non è, in generale, considerato a rischio di cyber attacchi. Viene assunto che nessuna violazione o furto di dati sia nota o accaduta in passato e che le operazioni di trattamento siano eseguite unicamente dal personale della PMI.

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
Risorse di rete e tecniche	Basso	1
Trattamenti/Procedure relative al trattamento dei dati personali	Basso	1
Parti/Persone coinvolte nel trattamento dei dati personali	Medio	2
Settore di operatività e scala/dimensione del trattamento	Basso	1
Probabilità complessiva di occorrenza di una minaccia	**Basso (5)**	

Data la suddetta valutazione, la probabilità complessiva che una minaccia si verifichi è **BASSA.**

3.2.4 Valutazione del rischio

Dati i risultati della valutazione dell'impatto e della probabilità che una minaccia si verifichi, il rischio è calcolato basandosi sulla sezione 2.1.4.

Livello d'impatto

Probabilità che si verifichi una minaccia

	Basso	Medio	Alto / Molto Alto
Basso		X	
Medio			
Alto			

Il rischio complessivo per questo caso particolare è generalmente considerato **MEDIO**. Allegato A: (A.1 & A.2) può essere utilizzato per adottare misure adeguate al rischio che il trattamento presenta.

Si dovrebbe prendere atto del fatto che il livello di rischio potrebbe essere differente (più alto) in condizioni direttamente connesse a specifici trattamenti di dati che potrebbero influenzare sia l'impatto che la probabilità che una minaccia si verifichi. Per esempio, se i candidati hanno accesso ai loro

resoconti di valutazione direttamente attraverso la piattaforma di selezione IT, la probabilità che la minaccia si verifichi aumenterà fino a diventare ALTA. Per quanto riguarda la valutazione dell'impatto, si considerino anche le pertinenti considerazioni esposte nella sezione 3.3.2.

3.3 Valutazione dei dipendenti

All'interno di questo ulteriore scenario si consideri come esempio una PMI specializzata in prodotti IT e relativi servizi di consulenza. Una volta all'anno, ogni dipendente viene valutato dal proprio responsabile in base a criteri predefiniti e concordati, relativi alla sua prestazione e alle sue doti professionali, che includono affidabilità, orientamento verso gli utenti / clienti, tempestività / prontezza, abilità interpersonali, flessibilità, autonomia, capacità di comunicazione scritta e orale e spirito di squadra. Il trattamento viene eseguito da un funzionario delle Risorse Umane e dai dirigenti con strumenti elettronici e documentazione cartacea. Il manager produce una prima versione del rapporto su carta e discute i risultati con il dipendente. La versione finale del rapporto è debitamente firmata e inoltrata elettronicamente al dipartimento risorse umane, cosi come il sommario e le conclusioni/risultati del rapporto.

3.3.1 Definizione del trattamento e del suo contesto

DESCRIZIONE DELL'OPERAZIONE DI TRATTAMENTO	EVALUATION OF STAFF	
Dati personali oggetto del trattamento	**Nome e Cognome, posizione nella PMI, data di impiego, storia in azienda, skill tecniche, conoscenze ed abitudini (report di valutazione di performance lavorativa)**	
Finalità del trattamento	**Valutazione della performance e delle caratteristiche professionali inerenti al lavoro**	
Interessati	**Dipendenti**	
Strumenti impiegati per il trattamento	**Sistemi IT del Dipartimento Risorse Umane**	
Destinatari dei dati	**Interni**	**Line Managers**
Responsabile dei dati	**In-house (nessun Responsabile dei dati)**	

3.3.2 Valutazione di impatto

Seguendo l'approccio presentato nella sezione 2.1.2, è dunque possibile procedere alla seguente analisi.

Perdita di riservatezza

Nell'ambito della finalità di questo trattamento, si dovrebbe considerare che la valutazione del personale fornisce un dettagliato profilo professionale del dipendente, attribuendo valori qualitativi e quantitativi alle sue prestazioni lavorative. Sebbene la valutazione possa essere limitata alle prestazioni lavorative, nel corso della valutazione possono emergere altre caratteristiche del dipendente, creando il rischio che vengano elaborate anche le informazioni relative al comportamento e alla personalità dei dipendenti. La perdita di riservatezza di questi dati potrebbe andare dal semplice imbarazzo, alla lesione dell'onore fino addirittura alla limitazione di possibilità per il dipendente, ad es. ove cercasse un nuovo lavoro. Pertanto, l'impatto della perdita di riservatezza deve essere considerato come MEDIO.

Perdita di Integrità

La perdita di integrità potrebbe essere in generale considerata con il valore **MEDIO** poiché ci si aspetta che i soggetti interessati incontrino inconvenienti significativi, tra cui una valutazione sbagliata o la mancanza o il ritardo nel beneficiare dei risultati della valutazione.

Perdita di disponibilità

L'impatto della perdita di disponibilità va considerato **BASSO**, dato che si prevede che gli interessati vadano incontro a disagi minori, semplicemente dovuti al ritardo del processo di valutazione che però non viene invalidato. La tabella sotto riassume la suddetta analisi.

VALUTAZIONE DI IMPATTO		
Riservatezza	Integrità	Disponibilità
Medium	Medium	Low
	Valutazione di Impatto complessiva	MEDIUM

Il risultato complessivo della valutazione di impatto è il più alto identificato e pertanto l'impatto complessivo valutato è **MEDIO**.

Oltre alle ipotesi formulate in questo esempio, potrebbero esserci casi in cui l'impatto complessivo potrebbe essere superiore a quello calcolato sopra. Un esempio di tale caso potrebbe essere quando:

- Il contesto lavorativo specifico richiede una valutazione delle caratteristiche psicologiche dei dipendenti o quando vengono inclusi dati di particolare natura (sensibili) nel corso del processo di valutazione (ad esempio in relazione alle persone con disabilità).

3.3.3 Probabilità di occorrenza di una minaccia

In base alle domande e all'approccio presentati nella sezione 2.1.3, è possibile effettuare la seguente valutazione per ciascuna dimensione dell'ambiente specifico di elaborazione dei dati di questo Scenario pratico:

- **Risorse di rete e tecniche:** la probabilità che si verifichi una minaccia è **BASSA**, in quanto il sistema IT non è connesso a Internet e non consente l'accesso da Internet a risorse interne e altri sistemi IT della PMI. Come negli esempi precedenti, l'assunzione di partenza è che presso tale PMI siano applicate best practices per evitare accessi non autorizzati e, di conseguenza, si assume che esse siano atte a garantire la protezione dei dati.
- **Processi/Procedure relativi alla operazione di trattamento dei dati personali:** La probabilità che si verifichi una minaccia è di valore **MEDIO**, presupponendo che la "policy"interna sul processo di valutazione non sia chiaramente definita e che il trattamento non sia necessariamente limitato ai locali dell'organizzazione (es: la parte del processo basato su documenti/report cartacei).
- **Parti / Persone coinvolte nel trattamento dei dati personali:** La probabilità che si verifichi una minaccia è di valore **MEDIO** poiché si presuppone (dalla descrizione del caso) che non ci siano "policy" specifiche riguardanti la memorizzazione sicura e la cancellazione dei dati (specialmente quando una parte del processo è basata su carta).
- **Settori di operatività e scala del trattamento:** la probabilità che si verifichi una minaccia è **BASSA**, in quanto il settore di attività della PMI non è generalmente considerato soggetto agli attacchi informatici e si presume che in passato non si sia verificata alcuna violazione dei dati personali. Il trattamento è limitato solo ai dipendenti della PMI.

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
Rete e dispositivi tecnici	Low	1
Processi/Procedure relative al trattamento di dati personali	Medium	2
Parti/Persone coinvolte nel trattamento di dati personali	Medium	2
Settore di attività e portata del trattamento	Low	1
Probabilità di accadimento di minaccia globale	Medium (6)	

Seguendo i criteri di cui sopra, la probabilità di accadimento complessiva della minaccia viene calcolata con valore **MEDIO**.

3.3.4 Valutazione del Rischio

Utilizzando i risultati della valutazione di impatto e della probabilità di accadimento di minacce, il rischio viene calcolato in base ai parametri indicati nella Sezione 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low			
	Medium		X	
	High			

In particolare, il rischio globale per questo caso particolare è generalmente considerato come **MEDIO**. L'allegato A(A.1 & A.2) può essere utilizzato per adottare misure adeguate al rischio che il trattamento presenta.

Anche in questo scenario pratico si dovrebbe prendere atto del fatto che il livello di rischio potrebbe essere differente (più alto) in condizioni direttamente connesse a specifici trattamenti di dati che potrebbero influenzare sia l'impatto che la probabilità che una minaccia si verifichi. Per quanto riguarda la valutazione dell'impatto, si considerino anche le pertinenti considerazioni esposte nella sezione 3.3.2.

4. Scenario pratico: gestione clienti, marketing e fornitori

Una PMI, per svolgere le proprie attività, tratta i dati personali dei propri clienti e svolge attività di marketing per acquisire nuova clientela . Queste attività potrebbero comportare anche il trattamento di dati personali relativi ai suoi fornitori.

In base alla natura e alla quantità dei prodotti e servizi offerti da tale PMI , nonché del mercato di riferimento, le sue attività potrebbero essere diversificate e includere il trattamento di diversi tipi di dati personali anche per scopi diversi da quelli originari.

4.1 Ordini e consegna dei prodotti

Nell'ambito dello scenario pratico esemplificativo sopra delineato, si consideri una PMI al dettaglio che offre beni attraverso un negozio elettronico specificatamente dedicato.
Il cliente può navigare tra i prodotti disponibili, aggiungerli al carrello e controllare i propri ordini. Per

consentirgli di completare l'ordine, gli viene chiesto di registrarsi alla piattaforma (qualora non sia già registrato) fornendo i propri dettagli di contatto (nome e cognome, indirizzo di consegna, numero di telefono e indirizzo e-mail). Durante la procedura di checkout, all'utente registrato viene anche chiesto di fornire i dettagli di pagamento in un modulo separato predisposto dal fornitore dei servizi di pagamento.

Dopo il completamento dell'ordine di acquisto e la conferma da parte del fornitore del servizio di pagamento dell'avvenuta transazione economica, i dettagli dell'ordine effettuato dall'utente vengono trasmessi al Sistema ERP (Enterprise Resource Planning), al sistema CRM (Customer Relation Management) e al fornitore dei servizi di consegna.

Questa procedura, implementata e utilizzata sulla base di una specifica policy di utilizzo e corredata da best practice riconosciute, non è tuttavia accompagnata da policy specifiche circa la conservazione e la distruzione dei dati. A ciò si aggiunga che non tutti i dipendenti dell'azienda coinvolti in questa procedura hanno ricevuto una formazione specifica a proposito del livello di sicurezza necessario sul trattamento dei dati personali effettuato.

4.1.1 Definizione del trattamento e del relativo contesto

La specifica operazione di trattamento dei dati personali considerata nello scenario pratico può essere dettagliata come segue:

TIPO DI TRATTAMENTO	DESCRIZIONE ORDINE E CONSEGNA MERCE
Dati personali oggetto di trattamento	Informazioni di contatto (cognome e nome, indirizzo, numero di telefono) dati di pagamento (carta di credito, informazioni sul conto bancario)
Finalità del trattamento	Ordine e consegna della merce
Soggetti interessati	Clienti
Strumenti del trattamento	Sistema di gestione degli ordini
Destinatari dei dati	• Fornitore di servizi di pagamento esterno • Fornitore di servizi di consegna esterna • Sistema CRM (Internal Customer Relation Management) interno • Sistema ERP (Enterprise Resource Planning) interno
Responsabile del trattamento	Interno ed esterno

4.1.2 Valutazione dell'impatto

Perdita della riservatezza e dell'integrità

Nell'ambito del trattamento descritto in precedenza, l'impatto derivante dalla perdita della riservatezza e/o dell'integrità del dato è considerato come **MEDIO** (la divulgazione e/o alterazione non autorizzata di dati personali trattati, compresi i dati finanziari, potrebbe comportare notevoli inconvenienti per il soggetto al quale i dati si riferiscono).

Perdita di disponibilità

Il livello di impatto derivante dalla perdita di disponibilità del dato è considerato **BASSO** : l'indisponibilità dei dati personali dovrebbe comportare solo lievi disagi per l'interessato, facilmente superabili (ad es. un ritardo nella consegna della merce).

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Medium**	**Low**
	Overall Impact Evaluation	**MEDIUM**

Il risultato complessivo della valutazione dell'impatto è quindi **MEDIO**.

Oltre alle ipotesi appena formulate, potrebbero verificarsi casi in cui l'impatto complessivo è diverso (ad esempio superiore) da quello appena calcolato. È il caso in cui i prodotti messi a disposizione per l'acquisto dell'utente sono in grado di rivelare dati sensibili sull'individuo, ad es. dati relativi alla sua salute, alle sue preferenze sessuali, politiche e religiose.

4.1.3 Probabilità di occorrenza di una minaccia

In base a quanto evidenziato nella sezione 2.1.3, è possibile effettuare la seguente valutazione per ciascuna dimensione del trattamento che stiamo qui analizzando.

- **Risorse di rete e tecniche**: la probabilità che si verifichi una minaccia è di valore MEDIO , poiché parte del trattamento dei dati personali viene eseguita tramite Internet e il sistema di elaborazione è interconnesso con altri sistemi IT interni ed esterni. Si presuppone che l'accesso non autorizzato ai dati personali sia impedito in base alle migliori best practice esistenti.
- **Processi/Procedure relativi al trattamento dei dati personali:** la probabilità che si verifichi una minaccia è **BASSA** , poiché si presuppone che i ruoli e le responsabilità dei dipendenti siano chiaramente definiti all'interno di una policy condivisa, che il trattamento dei dati personali sia limitato a quanto previsto dall'azienda e che per qualsiasi attività di elaborazione eseguita vengano creati dei log files.
- **Team/Persone coinvolte nel trattamento dei dati personali:** la probabilità che si verifichi una minaccia è di valore MEDIO , poiché non tutti i dipendenti hanno ricevuto formazione sulla sicurezza delle informazioni e non è garantito che i dati personali siano sempre trattati e / o distrutti in modo sicuro.
- **Settore di operatività e scala/dimensione del trattamento :** la probabilità che si verifichi una minaccia è di valore MEDIO poiché il settore di operatività commerciale della PMI (vendita attraverso un e-shop) può essere considerato, in generale, soggetto a cyber attacchi e il

trattamento riguarda un numero elevato di individui. Inoltre, nello scenario pratico considerato, si presuppone che una violazione dei dati personali si sia verificata spesso in passato.

ASSESSMENT AREA	LIVELLO (probabilità)	PUNTEGGIO (probabilità)
Risorse di rete e tecniche:	MEDIO	2
Processi e procedure relativi al trattamento dei dati personali	BASSO	1
Team o persone coinvolte nel processo di trattamento dei dati personali	MEDIO	2
Settore di operatività e scala/dimensione del trattamento	MEDIO	2
Probabilità complessiva che si verifichi la minaccia: MEDIO (7)		

Seguendo la valutazione di cui sopra, la probabilità la probabilità che si verifichi una minaccia è di valore **MEDIO** .

4.1.4 Valutazione del rischio

Utilizzando i risultati della valutazione dell'impatto e della probabilità del verificarsi di minacce, il rischio viene calcolato in base al metodo ed ai parametri indicati nella Sezione 2.1.4

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low			
	Medium		X	
	High			

Il rischio, come si evince dalla tabella, è considerato come **MEDIO** .

L'allegato A (A.1 e A.2) può essere utilizzato per l'adozione di misure adeguate al rischio presentato. È necessario prendere nota del fatto che il rischio potrebbe essere diverso (ad esempio superiore) in condizioni direttamente correlate all'operazione di trattamento dei dati e che ciò influisce sull'impatto o sulla probabilità che si verifichi la minaccia (si vedano anche le considerazioni effettuate nella sezione 4.1.2).

4.2 Marketing / pubblicità

Consideriamo la PMI al dettaglio descritta nella sezione 4.1, che tratta i dati personali dei potenziali clienti al fine di promuovere i diversi tipi di beni disponibili sul proprio catalogo. Affinché tale trattamento avvenga, si presume che gli interessati abbiano già fornito il loro consenso in modalità cartacea o

elettronica (si dà per presupposto il rispetto del quadro legale di riferimento, non preso in considerazione nella presente analisi di sicurezza).
Per questa operazione di trattamento la PMI si avvale di uno strumento web dedicato, offerto da un fornitore terzo specializzato in tali attività. Il fornitore terzo è stabilito nell'UE e aderisce alle best practice di sicurezza.
Ogni mese un componente del reparto marketing inserisce su un'apposita interfaccia web le informazioni di contatto (nome e cognome, indirizzo email) dei potenziali clienti e aggiorna l'elenco con eventuali potenziali clienti che hanno richiesto di non essere inclusi nella lista.
Ogni settimana attiva una nuova campagna di web marketing, inviando e-mail personalizzate all'elenco aggiornato dei destinatari. Per ogni campagna di web marketing la piattaforma gli fornisce un report con statistiche sulla percentuale di e-mail lette, non lette, di richieste di opt-out, senza tuttavia fornire informazioni su individui specifici.

4.2.1 Definizione del trattamento e del relativo contesto

La specifica operazione di trattamento dei dati personali considerata nello scenario pratico può essere dettagliata come segue:

TIPO DI TRATTAMENTO	MARKETING/ADVERTISING
Dati personali oggetto di trattamento	Informazioni di contatto (cognome e nome, indirizzo, numero di telefono, email)
Finalità del trattamento	Promozione di beni e di offerte speciali a potenziali clienti
Soggetti interessati	Clienti e potenziali clienti
Mezzi impiegati per il trattamento	Servizi di campagne di web marketing di terze parti
Destinatari dei dati	• Esterni: Provider di servizi di campagne di web marketing • Interno: Dipartimento di marketing • Interno: Sistema CRM
Responsabile del trattamento	Provider di servizi di campagne di web marketing

4.2.2 Valutazione dell'impatto

Perdita di riservatezza, integrità e disponibilità

Nell'ambito di questo specifico trattamento, l'impatto derivante dalla perdita di riservatezza e/o integrità e/o disponibilità è considerato **BASSO** , in quanto i singoli individui possono incontrare alcuni piccoli inconvenienti (ad es. mediante divulgazione non autorizzata delle loro informazioni di contatto - che potrebbero portare a spam - o modifica non autorizzata dei loro dati), ma in tutti i casi il problema potrà essere facilmente risolto con un piccolo sforzo.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Low	**Low**	**Low**
	Overall Impact Evaluation	**LOW**

Il risultato complessivo della valutazione dell'impatto è quindi **BASSO** .

Oltre alle ipotesi appena formulate, potrebbero verificarsi casi in cui l'impatto complessivo è diverso (ad esempio superiore) da quello calcolato appena calcolato È il caso in cui l'inclusione di un individuo in una campagna di marketing possa rivelare informazioni sensibili, perché legata alla sua origine razziale o etnica, alle sue opinioni politiche o al suo stato di salute. Un altro esempio potrebbe essere quello in cui il trattamento di dati personali avviene al fine di comprendere sempre meglio i gusti, le abitudini e le caratteristiche del cliente e orientarlo nelle sue scelte secondo precise strategie di marketing. Questo tipo di elaborazione sarebbe quindi una "profilazione" e i dati trattati sarebbero relativi alle possibili preferenze e interessi degli interessati (acquisiti attraverso il processo di profilazione).

Nell'ambito di questo trattamento, l'impatto derivante dalla perdita di riservatezza sarebbe quindi considerato come **MEDIO**, in quanto i singoli individui potrebbero incontrare in determinati casi problemi significativi essendo le loro preferenze, le loro abitudini di acquisto e i loro interessi accessibili a terzi in un modo sconosciuto. Potrebbe essere considerato, invece, **ALTO** nel caso in cui la menzionata profilazione sia basata su dati sensibili.

4.2.3 Probabilità di occorrenza di una minaccia

In base alle domande e all'approccio presentati nella sezione 2.1.3, è possibile effettuare la seguente valutazione di impatto:

- **Risorse di rete e tecniche:** la probabilità che si verifichi una minaccia è di valore **MEDIO**, poiché il trattamento dei dati personali avviene tramite Internet e il sistema di elaborazione è interconnesso con altri sistemi IT interni ed esterni.
- **Processi/Procedure relative al trattamento dei dati personali:** la probabilità che si verifichi una minaccia è **BASSA** , poiché si presuppone che i processi siano ben definiti e che la parte terza specializzata aderisca alle best practice di sicurezza.
- **Parti/Persone coinvolte nel trattamento dei dati personali:** la probabilità che si verifichi una minaccia è di valore **MEDIO**, in quanto parte dell'elaborazione dei dati è eseguita da un responsabile del trattamento (terza parte) e, pertanto, la PMI non ha il pieno controllo dei dati. Si presume, tuttavia, che il terzo specializzato aderisca alle best practice di sicurezza esistenti nel business di riferimento.
- **Settore di operatività e scala/dimensione del trattamento :** la probabilità che si verifichi una minaccia è di valore **MEDIO**, poiché il settore di operatività commerciale della PMI (vendita attraverso un e-shop) può essere considerato, in generale, soggetto a cyber attacchi e il trattamento riguarda un numero elevato di individui. In ogni caso, nello scenario pratico considerato, si presuppone che non si sia mai verificata in passato una violazione dei dati personali.

ASSESSMENT AREA	LIVELLO (probabilità)	PUNTEGGIO (probabilità)
Risorse di rete e tecniche	MEDIO	2
Processi e procedure relativi al trattamento dei dati personali	BASSO	1
Team o persone coinvolte nel processo di trattamento dei dati personali	MEDIO	2
Settore di operatività e scala/dimensione del trattamento	MEDIO	2
Probabilità complessiva che si verifichi la minaccia: MEDIO (7)		

Seguendo la valutazione di cui sopra, la probabilità che si verifichi una minaccia è calcolata come di valore **MEDIO**.

4.2.4 Valutazione del rischio

Utilizzando i risultati della valutazione dell'impatto e della probabilità che si verifichi la minaccia, il rischio viene calcolato in base alla Sezione 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low			
	Medium	X		
	High			

In particolare, il rischio complessivo per questo caso particolare è considerato **BASSO.** L'allegato A (A.1) può essere utilizzato per l'adozione di misure adeguate al rischio presentato. Si dovrebbe prendere atto che il rischio potrebbe essere diverso (Medio anche Alto) in condizioni direttamente correlate a trattamenti di dati specifici e che influiscono sull'impatto o sulla probabilità di accadimento della minaccia (si vedano anche le relative considerazioni esposte nella sezione 4.2.2).

4.3 Fornitori di beni e servizi

Si consideri ora la PMI come descritta al paragrafo 4.1, nella sua qualità di soggetto che acquisisce in via ordinaria servizi e beni necessari sia per lo svolgimento delle attività quotidiane che per la vendita di beni. Queste procedure possono includere, in determinati casi di trattamento di dati personali, dati di contatto di dipendenti che lavorano per i fornitori o contatti e dati finanziari di persone che sono in contratto diretto con la PMI (che agiscono cioè direttamente come fornitori di beni o servizi).

L'operazione di trattamento dei dati è supportata da un sistema IT connesso al sistema ERP (Enterprise Resource Planning) e al sistema di contabilità. I dati personali trattati comprendono il nome della società fornitrice e i dettagli di contatto, dati finanziari (codice fiscale, conto bancario), immagini dei dipendenti e credenziali di accesso (per il personale che lavora all'interno dei locali). Tutte le relazioni commerciali tra la PMI e i fornitori avvengono tramite CRM extranet, direttamente connesse alle piattaforme dei fornitori. I pagamenti vengono effettuati utilizzando servizi bancari da remoto. Esiste anche una piattaforma off-line

all’interno della quale le bolle di consegna e le fatture vengono caricate durante la notte in serie. Le comunicazioni amministrative con i fornitori avvengono tramite un normale servizio di posta elettronica.

4.3.1 Definizione dell'operazione di elaborazione dei dati e del suo contesto

TIPO DI TRATTAMENTO	ACQUISIZIONE (fornitura di materie prime, beni e servizi)
Dati personali oggetto di trattamento	Nome e cognome, informazioni di contatto, informazioni bancarie e fiscali (per i fornitori), identificazione e credenziali di accesso (per il personale che lavora nei locali)
Finalità del trattamento	Gestione dell'offerta
Soggetti interessati	Impiegati che lavorano per fornitori di beni e servizi
Mezzi impiegati per il trattamento	Sistema IT
Destinatari dei dati	• Interno: Sistema ERP • Interno: sistema di contabilità • Esterno: CRM fornitori • Esterno: Provider di pagamento
Responsabile del trattamento	Interno (nessun Responsabile del trattamento)

4.3.2 Valutazione dell'impatto

Perdita di riservatezza

Nell'ambito dell'operazione di trattamento specifica, l'impatto della perdita di riservatezza è considerato **BASSO** poiché potrebbero derivare limitati e minori disagi per gli interessati dal trattamento dei loro dati personali rappresentato dall'accesso di terze parti alle informazioni in modalità non conosciute.

Perdita di integrità e disponibilità

L'impatto da perdita di integrità e/o disponibilità è considerato BASSO in quanto gli interessati possono imbattersi nell'inconveniente di veder ritardato l'adempimento commerciale con la società, o la merce ordinata potrebbe essere consegnata ad un indirizzo errato o non essere consegnata affatto. Tali inconvenienti, tuttavia, possono essere superati con uno sforzo limitato.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Low	Low	Low

Il risultato complessivo della valutazione dell'impatto è **BASSO** . Oltre alle ipotesi appena formulate, potrebbero verificarsi casi in cui l'impatto complessivo è diverso (ad esempio superiore) da quello appena calcolato. Un esempio potrebbe essere quello in cui la società opera in un ambiente "sensibile" e, pertanto, la divulgazione dei nomi dei dipendenti potrebbe metterli a rischio (ad esempio in un ambiente militare).

4.3.3 Probabilità di occorrenza di una minaccia

In base ai quesiti e all'approccio presentati nella sezione 2.1.3, è possibile effettuare la seguente valutazione per ciascuna dimensione dell'ambiente specifico di trattamento dei dati riferito al presente scenario pratico :

- **Risorse di rete e tecniche:** la probabilità che si verifichi una minaccia è di valore **MEDIO**, poiché il sistema è connesso a Internet ed è possibile fornire l'accesso al sistema di elaborazione dei dati personali interno tramite Internet. Tuttavia, vengono utilizzate le *best practice* per impedire l'accesso non autorizzato.
- **Processi/Procedure relative al trattamento dei dati personali:** la probabilità che si verifichi una minaccia è **BASSA** , poiché si presuppone che i ruoli e le responsabilità del personale siano chiaramente definiti all'interno di una policy condivisa, che ai dipendenti non sia consentito portare con sé i propri dispositivi nonché conservare, trasferire o elaborare i dati personali al di fuori dei locali dell'organizzazione e creare log file per qualsiasi attività di elaborazione dei dati sia eseguita.
- **Parti/Persone coinvolte nel trattamento dei dati personali:** la probabilità che si verifichi una minaccia è **BASSA** , in quanto i dipendenti non sono in grado di trasferire, archiviare o elaborare in altro modo i dati personali al di fuori dei locali dell'organizzazione; inoltre l'uso della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è chiaramente definito e i dipendenti coinvolti nell'operazione di trattamento dei dati archiviano e distruggono in modo sicuro i dati personali.
- **Settore di operatività e scala/dimensione del trattamento :** la probabilità che si verifichi una minaccia è **BASSA** poiché il settore in cui opera la PMI non è generalmente considerato soggetto ad attacchi informatici, o ad incidenti o violazione della sicurezza. Nessun reclamo è stato ricevuto negli ultimi due anni e il trattamento non riguarda un elevato numero di individui.

ASSESSMENT AREA	LIVELLO (probabilità)	PUNTEGGIO (probabilità)
Risorse di rete e tecniche	MEDIO	2
Processi e procedure relativi al trattamento dei dati personali	BASSO	1
Team o persone coinvolte nel processo di trattamento dei	BASSO	1

dati personali		
Settore di operatività e scala/dimensione del trattamento	BASSO	1
Probabilità complessiva che si verifichi la minaccia: BASSO (5)		

4.3.4 Valutazione del rischio

Utilizzando i risultati della valutazione dell'impatto e della probabilità che si verifichi una minaccia, il rischio viene calcolato in base alla Sezione 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	X		
	Medium			
	High			

In particolare, il rischio complessivo è generalmente considerato BASSO . L'allegato A (A.1) può essere utilizzato per l'adozione di misure adeguate al rischio presentato.

È necessario tenere presente che il rischio potrebbe essere diverso (Medio o Alto) in condizioni direttamente correlate ad uno specifico trattamento dei dati (si vedano anche le relative considerazioni riportate nella sezione 4.3.2).

5. Sicurezza

5.1 Controllo degli accessi

Si consideri ora il caso il caso di un'azienda di consulenza (PMI) che, al fine di garantire l'accesso all'interno e all'esterno di specifiche aree autorizzate, mantenga un database contenente i dati personali relativi a dipendenti e visitatori. Il sistema di controllo degli accessi implementato è comprensivo dei lettori di schede RFID installati in punti predefiniti, delle relative RFID card da consegnare al personale e della relativa piattaforma di gestione e di controllo. Ogni dipendente, al fine di permettergli di svolgere le proprie funzioni, viene registrato nella piattaforma e gli viene assegnato un codice alfanumerico univoco che viene memorizzato nella RFID card che gli viene consegnata.

I dati personali utilizzati durante la registrazione sulla piattaforma comprendono il nome, il cognome, la data di assunzione, la posizione all'interno dell'organizzazione, la data di scadenza del contratto in essere (in caso questa sia specificata) ed una foto del profilo. La RFID card di ciascun dipendente viene quindi personalizzata stampando su di essa il nome , il cognome ed una fotografia dell'interessato. Per ogni tipo di posizione all'interno dell'organizzazione (amministrazione, manager, supporto, segreteria, ecc..) sono stati definiti i relativi diritti di accesso specifici.

Ogni volta che un dipendente scorre la propria carta sul lettore, la piattaforma controlla i diritti in base ai quali garantisce l'accesso alle aree permesse. Ogni tentativo viene registrato all'interno della piattaforma e, in caso di un tentativo di accesso non autorizzato, viene inviato un avviso al responsabile della sicurezza.

Per i visitatori esistono delle RFID card configurate per dare l'accesso alla sola sala riunioni dell'azienda. All'arrivo di un visitatore, l'agente preposto registra all'interno della piattaforma i dati anagrafici (nome e cognome) dell'ospite e del dipendente accompagnatore, la durata prevista della visita e assegna al visitatore una RFID card temporanea. Al termine della visita o allo scadere della durata della visita impostata, la carta viene automaticamente invalidata dal sistema e deve essere restituita al gruppo operativo di sicurezza che l'ha emessa. Gli operatori della sicurezza che gestiscono la piattaforma hanno ricevuto una formazione specifica sulle funzioni della piattaforma stessa e degli obblighi derivanti dal suo utilizzo, assumendo che vengano seguite le migliori prassi di utilizzo.

OPERAZIONE DI TRATTAMENTO	CONTROLLO DEGLI ACCESSI	
Dati Personali oggetto del trattamento	**Per I dipendenti: nome e cognome, data di assunzione, posizione aziendale, scadenza del contratto, foto del profilo.** **Per I visitatori: nome e cognome, data della visita, data di partenza prevista.**	
Finalità del trattamento	**Controllo della sicurezza degli accessi logico-fisica**	
Interessati	**Dipendenti, Ospiti**	
Strumenti per il trattamento dei dati	**Piattaforma di gestione e controllo degli accessi**	
Destinatari dei dati	**Interni**	**Responsabile della sicurezza**
Utilizzo	**Uso esclusivamente interno**	

5.1.1 Valutazione di impatto

Perdita di confidenzialità, integrità e disponibilità del dato

Nell'ambito dell'operazione di trattamento del paragrafo precedente, è evidente che l'impatto derivante dalla perdita di riservatezza e/o integrità e/o disponibilità viene considerato **BASSO** poiché ci si aspetta che ciascun individuo incontri lievi disagi che potranno essere superati con uno sforzo limitato. Ad esempio, i dipendenti potrebbero non essere in grado di accedere a specifici locali della dell'azienda e svolgere il loro compito (integrità o perdita di disponibilità) o la presenza di un visitatore nei locali della PMI potrebbe essere divulgata (perdita di riservatezza).

VALUTAZIONE DI IMPATTO		
Confidenzialità	Integrità	Disponibilità
Bassa	**Bassa**	**Bassa**
	Valutazione di Impatto Totale	**Bassa**

Il risultato complessivo della valutazione dell'impatto è quindi **BASSO**.

Oltre alle ipotesi formulate in questo esempio, potrebbero esserci casi in cui l'impatto complessivo potrebbe essere diverso (superiore) da quello calcolato sopra. Ad esempio nel caso in cui la visita ai locali delle PMI possa rivelare informazioni sensibili specifiche, ad es. per quanto riguarda la salute, le credenze religiose, le preferenze politiche o sessuali.

5.1.2 Probabilità di occorrenza di una minaccia

In base alle domande e all'approccio presentati nella sezione 2.1.3, per ogni valore specifico inerente al trattamento dei dati considerato in questo specifico scenario pratico è possibile formulare le seguenti valutazioni:

- **Risorse tecniche e di rete:** La probabilità di occorrenza della minaccia, a patto che vengano utilizzate le *best practices* per impedire l'accesso non autorizzato al sistema, è **BASSA**, poiché il sistema non è connesso a Internet, non consente l'accesso da Internet a risorse interne nè la connessione ad altri sistemi IT.
- **Processi / Procedure relative al trattamento dei dati personali:** La probabilità di occorrenza della minaccia è **BASSA**, poiché si presuppone che siano chiaramente definiti i ruoli e le responsabilità del responsabile della sicurezza uniti ad una politica di utilizzo coerente e che qualsiasi attività di elaborazione eseguita venga tracciata su appositi file di log.
- **Parti / Persone coinvolte nel trattamento dei dati personali:** La probabilità di occorrenza della minaccia è **BASSA** in quanto non è possibile trasferire, archiviare o elaborare i dati personali in altro modo al di fuori delle sedi dell'organizzazione, mentre risulta chiaramente accettabile l'utilizzo della rete, del sistema e delle risorse fisiche all'interno della PMI.
- **Settore di operatività e scala/dimensione del trattamento S:** la probabilità di occorrenza della minaccia è **BASSA** sia perché il settore di mercato della PMI considerata non è generalmente soggetto ad attacchi ti tipo informatico, sia perché in passato non è stata registrata alcuna una violazione di dati personali (data breach) e sia perchè il trattamento non riguarda un numero elevato di individui.

AREA DI VALUTAZIONE	PROBABILITA	
	LIVELLO	PUNTEGGIO
Risorse tecniche e di rete	Basso	1
Processi / Procedure relative al trattamento dei dati personali	Basso	1
Parti / Persone coinvolte nel trattamento dei dati personali	Basso	1
Settore di operatività e scala/dimensione del trattamento	Basso	1
Probabilità totale di occorrenza di una minaccia	**Basso (4)**	

5.1.3 Valutazione dei rischi

Tenuto conto dei risultati della valutazione dell'impatto e della probabilità di occorrenza delle minacce, il rischio viene calcolato sulla base alla Sezione 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	X		
	Medium			
	High			

Tenuto conto dei risultati della valutazione dell'impatto e della probabilità di occorrenza delle minacce, il rischio viene calcolato sulla base alla Sezione 2.1.4. In particolare, il rischio complessivo per questo caso particolare è generalmente considerato **BASSO**.

L'allegato A (A.1) può essere utilizzato adottare le misure adeguate al rischio presentato.

È necessario notare che il rischio potrebbe essere diverso (Medio o Alto) in condizioni direttamente correlate ad uno specifico e diverso trattamento di dati e influire sull'impatto o sulla probabilità di occorrenza della minaccia (si vedano anche le relative considerazioni nella sezione 5.1.2). Ad esempio, la probabilità di occorrenza delle minacce potrebbe essere maggiore nel caso in cui la PMI operi in un ambiente "sensibile", ad es. un laboratorio di dati sanitari (aumentando così le possibilità di tentativi malevoli di ottenere accesso non autorizzato ai locali). Inoltre, si dovrebbe tenere conto che in generale il controllo degli accessi sia una misura integrale per impedire l'accesso non autorizzato ai propri locali e, quindi, direttamente collegato alla sicurezza di persone e merci. Pertanto, a seconda della natura dell'organizzazione, la PMI potrebbe considerare l'aumento del rischio complessivo a MEDIO o ALTO.

5.2 Sistema di Videosorveglianza a circuito chiuso (Closed Circuit Television System - CCTV)

Sempre rimanendo nell'ambito del presente scenario pratico si consideri la PMI descritta nella sezione 5.1 che, al fine di migliorare la sicurezza delle persone e delle merci all'interno dei propri locali, tratta dati personali anche per mezzo del proprio Sistema di videosorveglianza a circuito chiuso, di seguito CCTV

(Closed Circuit Television System), costituito da immagini e video senza audio. Si evidenzia che il presente scenario pratico analizza solo gli aspetti di sicurezza e prescinde dalla analisi della conformità legale del trattamento. In altri termini, si presuppone che il trattamento tramite videosorveglianza sia conforme al GDPR e che siano state prese in considerazione le Linee Guide pertinenti dell'Autorità per la protezione dei dati (DPA). Ovviamente, si ricordi che in tutti i casi dovrebbe essere prestata particolare attenzione all'aspetto legale delle operazioni di un Sistema di videosorveglianza a circuito chiuso - CCTV, che dovrebbe essere conforme ai requisiti e agli obblighi legali e normativi sia in materia di lavoro che di protezione dei dati.

Il sistema CCTV nel nostro esempio comprende la telecamera e il sistema di gestione che registra le immagini, le mostra ai responsabili della sicurezza e traccia qualsiasi attività di elaborazione non-real time. Il dato rimane salvato per il tempo indicato dalle Linee Guida della Autorità per la protezione dei dati personali per poi essere successivamente eliminato in modo sicuro automaticamente al termine del periodo impostato, a meno che l'operatore non lo estragga manualmente per i casi che richiedono un esame approfondito (ad esempio un allarme di sicurezza durante le ore non lavorative, ecc.). Avendo il personale della sicurezza che opera sulla piattaforma ricevuto una formazione specifica sulle funzioni della stessa e sugli obblighi derivanti dalla loro posizione, si presume che vengano utilizzate le migliori precauzioni al fine di evitare l'accesso non autorizzato ai dati in essa contenuti.

È necessario prestare particolare attenzione alla giurisprudenza riguardante l'installazione e il funzionamento del sistema CCTV, che deve essere conforme sia alla protezione dei dati che ai requisiti e agli obblighi legali e normativi in materia di lavoro.

5.2.1 Definizione di elaborazione e del suo contesto

DESCRIZIONE DEL TRATTAMENTO	CCTV
Dati personali oggetto di trattamento	**Immagini e video di persone fisiche (dipendenti, visitatori) .**
Finalità del trattamento	**Sicurezza fisica del personale, di visitatori e del patrimonio Aziendale**
Soggetti interessati	**Dipendenti, visitatori**
Mezzi impiegati per il trattamento	**Sistema di Videosorveglianza e Sistemi IT**
Destinatari dei dati	**Interni**
ed Responsabile del trattamento	**Interno (nessun Responsabile del trattamento)**

5.2.2 Valutazione di impatto

Perdita di Riservatezza

Nell'ambito dell'operazione di trattamento specifica, l'impatto della perdita di riservatezza è considerato **BASSO**, in quanto in alcuni casi, come ad esempio l'indesiderato rilevamento della presenza di un particolare visitatore, può comportare solo limitati disagi.

Perdita di integrità e disponibilità

La perdita di integrità è piuttosto difficile possa verificarsi (da un punto di vista tecnico) in questo caso particolare, poiché richiederebbe la manipolazione delle immagini video. La perdita di disponibilità si riferisce alla indisponibilità (totale o temporale) delle riprese video. In entrambi i casi, l'impatto è considerato **BASSO** e si potrebbe anche affermare che non vi è alcun impatto per le persone (poiché la perdita di filmati CCTV è un problema per le PMI, ma non per le persone che vengono registrate).

VALUTAZIONE DI IMPATTO		
Riservatezza	Integrità	Disponibilità
Basso	**Basso**	**Basso**
Valutazione Complessiva dell'impatto		**LOW**

Il risultato complessivo della valutazione dell'impatto è quindi **BASSO**.

Oltre alle ipotesi formulate in questo esempio, potrebbero esserci casi in cui l'impatto complessivo potrebbe essere diverso (superiore) da quello calcolato sopra. Un esempio di tale caso è quando la visita nei locali delle PMI potrebbe rivelare o dedurre informazioni sensibili, ad es. in relazione allo stato di salute, alle credenze religiose, alle preferenze politiche o sessuali.

5.2.3 Probabilità di occorrenza di una minaccia

In base alle domande e all'approccio presentati nella sezione 2.1.3, per ogni valore specifico inerente al trattamento dei dati considerato in questo specifico scenario pratico è possibile formulare le seguenti valutazioni:

- **Risorse tecniche e di rete:** La probabilità di occorrenza della minaccia è BASSA, poiché si presume che il sistema non sia connesso ad Internet e che vengano utilizzate le migliori precauzioni per impedire l'accesso non autorizzato.
- **Processi / Procedure relative al trattamento dei dati personali:** La probabilità di occorrenza della minaccia è **BASSA**, poiché si presuppone che siano chiaramente definiti i ruoli e le responsabilità del responsabile della sicurezza uniti ad a una politica di utilizzo accettabile e che qualsiasi attività di elaborazione eseguita venga tracciata su appositi file di log.
- **Parti / Persone coinvolte nel trattamento dei dati personali:** La probabilità di occorrenza delle minacce è **BASSA** poiché i dipendenti non possono trasferire, archiviare o elaborare i dati proveniente da sorgenti CCTV all'esterno delle sedi dell'organizzazione, mentre risulta chiaramente accettabile l'utilizzo della rete, del sistema e delle risorse fisiche all'interno della PMI.
- **Settore di operatività e scala/dimensione del trattamento :** la probabilità di occorrenza della minaccia è **BASSA** sia perché il settore di mercato della PMI considerata non è generalmente soggetto ad attacchi ti tipo informatico, sia perché in passato non è stata registrata alcuna una violazione di dati personali (data breach) e sia perchè il trattamento non riguarda un numero elevato di individui.

AREA DI	PROBABILITA'	
	LIVELLO	PUNTEGGIO

Risorse di rete e tecniche	**Basso**	**1**
Processi/Procedure relative alla operazioni di trattamento dei dati personali	**Basso**	**1**
Parti/Persone coinvolte dalla operazioni di trattamento	**Basso**	**1**
Settore di operatività e scala/dimensione del trattamento	**Basso**	**1**
Probabilità complessiva	**Basso**	

5.2.4 Valutazione del rischio

Tenuto conto dei risultati della valutazione dell'impatto e della probabilità di occorrenza delle minacce, il rischio viene calcolato sulla base alla Sezione 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	X		
	Medium			
	High			

In particolare, il rischio complessivo per questo caso particolare è generalmente considerato **BASSO**. L'allegato A (A.1) può essere utilizzato adottare le misure adeguate al rischio presentato.

È necessario notare che il rischio potrebbe essere diverso (medio o alto) in condizioni direttamente correlate ad uno specifico trattamento di dati e influire sull'impatto o sulla probabilità di occorrenza della minaccia (si vedano anche le relative considerazioni nella sezione 5.2.2). Ad esempio, la probabilità di occorrenza delle minacce potrebbe essere maggiore nel caso in cui la PMI utilizzi sistemi CCTV avanzati, che consentono zoom e registrazione video (notare che in tali casi la legalità complessiva dell'operazione di elaborazione dei dati deve essere analizzata attentamente).

6. Scenario pratico: il settore sanitario

6.1 Prestazione di servizi sanitari

Nell'ambito di questo Scenario pratico, si consideri una PMI operante nel settore sanitario (es: una piccola clinica) che tratta i dati personali al fine di fornire servizi sanitari. Per ogni paziente che frequenta la clinica per effettuare un esame o una visita di consultazione, viene creato (o aggiornato) un registro elettronico che include i dettagli di contatto dei pazienti, numero di assicurazione medica, risultati degli esami medici, patologie, allergie, diagnosi e schemi di cura (informazioni mediche). Attraverso questo registro, i medici e gli infermieri hanno una panoramica della storia e dello stato di salute dei pazienti e possono accedervi se necessario da terminali predefiniti all'interno dei locali della clinica. Prima dell'esame medico o della visita di consultazione, l'idoneità del paziente a ricevere tale esame o trattamento gratuitamente è validata consultando il registro del sistema sanitario pubblico. Se il paziente o l'esame non sono idonei alla gratuità, il costo viene comunicato al sistema informatico contabile che emette la relativa fattura. Dopo ogni visita i dati dei pazienti vengono aggiornati con dati più recenti dal medico curante o dall'infermiere, mediante la scansione di documenti cartacei o l'inserimento manuale di schemi di diagnosi e cura.

La piattaforma IT a supporto di questa operazione di trattamento è ospitata nei locali della PMI e non è accessibile tramite Internet. Ai fini del presente scenario pratico , si dà per presupposto che vengano utilizzate le *best practices* per impedire l'accesso non autorizzato alla piattaforma e che vengano organizzati corsi periodici di sensibilizzazione sulla sicurezza. Tuttavia, i diritti di accesso alle cartelle cliniche dei pazienti non sono esplicitamente definiti ad un necessario livello di dettaglio, dal momento che infermieri e medici devono essere in grado di accedere ai file in qualsiasi momento e il sistema non supporta un tale livello di dettaglio. La clinica prevede di avere un sistema di registrazione dei pazienti più dedicato entro i prossimi anni.

6.1.1 Definizione del trattamento dei dati e del relativo contesto

DESCRIZIONE DEL TRATTAMENTO	SERVIZI SANITARI EROGATI
Trattamento dati personali	Informazioni di contatto (cognome e cognome, indirizzo, numero di telefono,) numero della tessera sanitaria, risultati di esami medici, patologie, allergie, schemi di diagnosi e cura (informazioni mediche), informazioni amministrative e finanziarie (fatture, documenti di ospedalizzazione, ecc.).
Finalità del trattamento	Fornitura di servizi sanitari (diagnosi, trattamento e ospedalizzazione)
Interessati	Pazienti
Mezzi impiegati per il trattamento	Sistema IT medico
Destinatari dei dati	Interni: trattamento dottori ed infermieri Interni: Amministrazione e Sistema IT Esterni: Servizio Sanitario Nazionale

Responsabili del trattamento	In-house (nessun responsabile del trattamento)

6.1.2 Valutazione di impatto

Perdita di riservatezza, integrità e disponibilità

Nell'ambito dell'operazione di trattamento specificata, l'impatto derivante dalla perdita di riservatezza è considerato **ALTO** poiché si prevede che gli individui sperimentino rilevanti conseguenze negative da accessi non autorizzati ai propri dati sanitari . Altrettanto importante (ALTO) può essere l'impatto derivante dalla perdita di integrità, in quanto informazioni mediche errate potrebbero addirittura mettere a rischio la vita di un individuo. Lo stesso valore (ALTO) potrebbe essere attribuito anche all'impatto derivante dalla perdita di disponibilità, in quanto anche una temporanea indisponibilità del sistema informatico della clinica potrebbe ostacolarne le operazioni, mettendo così i pazienti a serio rischio.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
High	**High**	**High**
	Overall Impact Evaluation	**HIGH**

Il risultato complessivo della valutazione dell'impatto è quindi **ALTO**.

Oltre alle ipotesi formulate nell'ambito del presente scenario pratico , potrebbero verificarsi casi in cui l'impatto complessivo potrebbe anche essere considerato MOLTO ALTO, ad esempio in caso di categorie di soggetti vulnerabili o di trattamento di dati riferiti a minori.

6.1.3 Probabilità di occorrenza di una minaccia

In base alle domande e all'approccio presentati nella sezione 2.1.3, per ogni valore specifico inerente al trattamento dei dati considerato in questo specifico scenario pratico è possibile formulare le seguenti valutazioni:

- **Risorse di rete e tecniche:** la probabilità di minacce è di valore **MEDIO**, poiché il sistema è interconnesso con altri sistemi interni ed esterni. Tuttavia, non è possibile accedere ai dati tramite Internet e, in base Ai descritti presupposti dello scenari pratico in considerazione , sono state applicate le migliori *best practices* sulla sicurezza per impedire l'accesso non autorizzato al sistema.
- **Processi / Procedure relative al trattamento dei dati personali:** la probabilità di minaccia è **BASSA**, poiché i ruoli e le responsabilità del personale sono chiaramente definiti nella policy di utilizzo interna , il trattamento dei dati è limitato nelle sedi della clinica vengono generati file di log per tracciare qualsiasi attività di trattamento svolta .
- **Parti / Persone coinvolte nel trattamento dei dati personali:** la probabilità di occorrenza delle minacce è **ALTA** in quanto il trattamento dei dati personali viene eseguito da un numero indefinito di dipendenti e non esiste una politica chiara in merito all'accesso dettagliato alle cartelle cliniche. Tuttavia, gli obblighi di tutte le parti coinvolte nel trattamento sono chiaramente definiti e sono organizzati periodicamente seminari di sensibilizzazione.
- **Settore di operatività e scala/dimensione del trattamento :** la probabilità di occorrenza delle minacce è **ALTA** poiché il settore (sanità) è generalmente considerato soggetto ad attacchi informatici e l'operazione di trattamento riguarda un numero elevato di individui. Tuttavia, si

presume nello scenario pratico considerato che nessuna violazione dei dati personali si sia verificata in passato.

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
Risorse di rete e tecniche	Medio	2
Processi / Procedure relative al trattamento dei dati personali	Basso	1
Parti / Persone coinvolte nel trattamento dei dati personali	Alto	3
Settore di attività e livello di elaborazione	Alto	3
Probabilità complessiva di occorrenza di una minaccia	ALTO (9)	

6.1.4 Valutazione del rischio

Utilizzando i risultati della valutazione d'impatto e della probabilità della minaccia dell'evento, il rischio viene calcolato basandosi sui parametri indicati nella Sezione 2.1.4.

PROBABILITA' DI OCCORRENZA DELLA MINACCIA	Low	Medium	High / Very High
Low			
Medium			
High			X

In particolare, il rischio complessivo per questo caso particolare è generalmente considerato **ALTO**. L'allegato A (A.1 e A.2 e A.3) può essere utilizzato per l'adozione di misure adeguate al rischio considerato.

6.2 Procreazione medicalmente assistita

Nell'ambito di questo scenario pratico si consideri una PMI nel settore dell'assistenza sanitaria specializzata in Procreazione medicalmente assistita (PMA) che tratta i dati personali per la gestione e il tracciamento dei campioni biologici conservati nei suoi locali. La PMA include diversi metodi o tecniche basate sulla manipolazione di cellule riproduttive che consentiranno alle coppie infertili di concepire un bambino. Le procedure PMA includono anche tecniche di crioconservazione per gameti (ovociti e spermatozoi) ed embrioni.

Il sistema IT implementato internamente per supportare la conservazione di schede/ record PMA per ogni campione include: informazioni sul donatore (nome e cognome, indirizzo, numero di telefono, data di nascita), numero di tessera sanitaria, dati sanitari, dati del campione genetico e identificatore del campione genetico. Attraverso la piattaforma l'operatore può svolgere le seguenti funzioni: a) gestione del campione, tracciabilità di tutte le manifestazioni del campione, gestione della posizione del campione all'interno di contenitori criogenici e b) gestione degli accessi e registrazione dei campioni crioconservati.

Per quanto riguarda l'uso del sistema informatico, è in atto una politica di utilizzo specifica insieme a politiche specifiche riguardanti la conservazione e la distruzione dei dati. Il trattamento dei dati personali è limitato ai locali della PMI. L'accesso alla piattaforma è consentito solo a specifici dipendenti della PMI, in qualità di operatori, al personale medico e biologo responsabile dell'esecuzione di PMA. Tutti gli utenti della piattaforma sono stati chiaramente informati dei loro obblighi in materia di elaborazione dei dati personali e la formazione di sensibilizzazione è organizzata periodicamente. La piattaforma non è collegata a Internet e si presume che vengano utilizzate le migliori pratiche per impedire l'accesso non autorizzato.

6.2.1 Definizione del trattamento e del relativo contesto

Lo specifico trattamento può essere riassunto come segue:

DESCRIZIONE DEL TRATTAMENTO	GESTIONE DEI CAMPIONI BIOLOGICI PER PROCREAZIONE ASSISTITA
Tipologia di dati personali	**Informazioni sul donatore (nome e cognome, indirizzo, numero di telefono, data di nascita), numero di tessera sanitaria, dati sanitari, dati del campione genetico e identificatore del campione genetico**
Finalità del trattamento	**Gestione del campione genetico per la procreazione assistita (PMA)**
Interessati	**Donatori**

DESCRIZIONE OPERAZIONE DI ELABORAZIONE	GESTIONE DEI CAMPIONI BIOLOGICI PER PROCREAZIONE ASSISTITA
Mezzi impiegati per il trattamento	**Sistema IT procreazione medicalmente assistita PMA**
Destinatari dei dati	**Personale Interno**
Responsabile dati personali	**In-house (nessun Responsabile)**

6.2.2 Valutazione di impatto

Seguendo l'approccio presentato nella sezione 2.1.2, può essere fatta la seguente analisi:

Perdita di riservatezza, integrità e disponibilità

Nell'ambito dell'operazione di trattamento specifica, l'impatto derivante dalla perdita di riservatezza è considerato **ALTO**, poiché gli interessati potrebbero sperimentare significativi effetti negativi dalla divulgazione non autorizzata di dati sanitari e genetici. L'impatto da perdita di integrità o disponibilità è ugualmente importante (**ALTO**), poiché i soggetti interessati potrebbero sperimentare significativi effetti negativi o addirittura irreversibili derivanti da alterazioni non autorizzate o perdita di dati genetici o relativi alla salute, che potrebbero persino impedire loro di sottoporsi a una procedura PMA.

VALUTAZIONE D'IMPATTO		
Riservatezza	Integrità	Disponibilità
Alto	**Alto**	**Alto**
	Totale valutazione d'impatto	**Alto**

Il risultato complessivo della valutazione dell'impatto è il più alto identificato e pertanto l'impatto complessivo valutato è **ALTO**.

Oltre alle ipotesi formulate nel presente scenario pratico , potrebbero verificarsi casi in cui l'impatto complessivo potrebbe essere addirittura considerato **MOLTO ALTO**, ad esempio, in caso di categorie vulnerabili di interessati (ad esempio soggetti con malattie o handicap specifici).

6.2.3 Probabilità di occorrenza di una minaccia

- **Risorse di rete e tecniche**: la probabilità di occorrenza delle minacce è **BASSA**, poiché il sistema non è connesso a Internet, non è possibile fornire accesso al sistema di elaborazione dei dati personali interno attraverso Internet e vengono utilizzate *best practices* per impedire l'accesso non autorizzato.
- **Processi / Procedure relative al trattamento dei dati personali:** la probabilità di occorrenza della minaccia è **BASSA**, poiché i ruoli e le responsabilità del personale sono chiaramente definiti insieme a una adeguata policy di utilizzo interna , il trattamento è limitato ai locali della PMI e vengono generati file di log per tracciare qualsiasi attività di trattamento effettuata .

- **Parti / Persone coinvolte nel trattamento dei dati personali:** La probabilità di occorrenza della minaccia è **BASSA** in quanto l'elaborazione dei dati personali viene eseguita da un numero definito di dipendenti con obblighi chiaramente definiti e si dà per presupposto che i dipendenti coinvolti nell'operazione di trattamento dei dati archivino e distruggano in modo sicuro i dati personali trattati.
- **Settore di operatività e scala/dimensione del trattamento :** La probabilità di occorrenza della minaccia è di valore **ALTO**A in quanto il settore di operatività della PMI potrebbe essere considerato soggetto ad attacchi informatici e potenzialmente potrebbe riguardare un numero elevato di individui. Tuttavia, si dà per presupposto che non si sia verificata in passato alcuna violazione dei dati personali.

AREA DI	PROBABILITA'	
	LIVELLO	PUNTEGGI
Risorse di rete e tecniche	BASSO	1
Processi / Procedure relative al trattamento dei dati personali	BASSO	1
Parti/Persone coinvolte nel trattamento dei dati personali	BASSO	1
Settore di operatività e scala/dimensione del trattamento	ALTO	3
TOTALE	MEDIO (6)	

6.2.4 Valutazione del rischio

Utilizzando i risultati della valutazione di impatto e della probabilità di occorrenza delle minacce, il rischio viene calcolato sulla base dei parametri indicati nella Sezione 2.1.4.

LIVELLO D'IMPATTO

PROBABILITA' DI OCCORRENZA DI UNA MINACCIA	BASSO	MEDIO	ALTO/MOLTO ALTO
BASSO			
MEDIO			X
ALTO			

In particolare, il rischio complessivo per questo caso particolare è generalmente considerato **ALTO**. L'allegato A (A.1 e A.2 e A.3) può essere utilizzato per l'adozione di misure adeguate al rischio presentato.

6.3 Monitoraggio remoto di pazienti con malattie croniche

Nell'ambito di questo Scenario pratico, si consideri una PMI nel settore sanitario specializzata nella fornitura di servizi di monitoraggio domiciliare da remoto per pazienti a cui è stata diagnosticata una patologia cronica. Ogni paziente è dotato di un dispositivo di monitoraggio, che consente di tracciare in tempo reale i segni vitali e la trasmissione di informazioni come la pressione sanguigna, il livello di glucosio, il battito cardiaco e il ritmo ECG in intervalli regolari di diagnosi al centro sanitario affiliato. Il dispositivo di monitoraggio funge anche da dispositivo di comunicazione, consentendo ai pazienti di rispondere a indagini personalizzate dirette dai medici relative al livello di conformità della terapia.

Il dispositivo di monitoraggio da remoto è supportato da una piattaforma Web, ospitata da un provider di servizi cloud all'interno dell'UE, che raccoglie e mette in correlazione tutti i dati trasmessi al fine di rilevare eventuali deviazioni dal protocollo clinico e determinare lo stato generale di salute del paziente. Se viene

rilevata una deviazione dai valori e procedure accettabili, il medico comunica tramite telefono con il paziente per determinare se è necessaria una visita.

I dati personali coinvolti nell'operazione di trattamento includono le informazioni personali dei pazienti, come ad esempio il nome e cognome, indirizzo, numeri di telefono, data di nascita, numero di tessera sanitaria, dati sullo stato di salute, risultati della diagnosi, schemi di terapia, letture dei segni vitali e statistiche pertinenti. La piattaforma web è gestita da medici autorizzati con ruoli, responsabilità e obblighi chiaramente definiti relativi all'elaborazione dei dati personali.

6.3.1 Descrizione del trattamento e del relativo contesto

DESCRIZIONE DEL TRATTAMENTO	REMOTE MONITORING OF PATIENTS WITH CHRONIC DISEASES	
Dati Personali oggetto di trattamento	**Nome e cognome, indirizzo, numeri di telefono, data di nascita, numero di tessera sanitaria, dati sullo stato di salute, risultati della diagnosi, schemi di terapia, risultati dei test di laboratorio e statistiche pertinenti.**	
Finalità del trattamento	**Fornitura di servizi sanitari (monitoraggio a distanza di pazienti con malattie croniche**	
Interessati	**Pazienti**	
Mezzi impiegati per il trattamento	Dispositivi di monitoraggio remoto, monitoraggio della piattaforma web	
Destinatari dei dati	**Esterni**	
	Interni	
Responsabili del trattamento	**Hosting cloud provider**	

6.3.2 Valutazione di impatto

Perdita di riservatezza, integrità e disponibilità

Nell'ambito dell'operazione di trattamento specifica, l'impatto derivante dalla perdita di riservatezza è considerato **ALTO** in quanto si prevede che gli interessati sperimenterebbero significativi effetti negativi dalla divulgazione non autorizzata dei propri dati sanitari. La perdita di integrità è ugualmente importante (**ALTO**), poiché gli interessati sperimenterebbero significativi effetti negativi o addirittura irreversibili derivanti da alterazioni non autorizzate di dati sanitari (segnali e statistiche), che potrebbero persino rendere difficile per il paziente ricevere una terapia adeguata. La perdita di disponibilità è anche considerata una minaccia di valore **ALTO**, in quanto potrebbe nuovamente ostacolare il trattamento tempestivo e accurato delle persone interessate, che potrebbero anche vedere messa a rischio la loro vita.

VALUTAZIONE D'IMPATTO		
Riservatezza	Integrità	Disponibilità
Alto	**Alto**	**Alto**
	Totale valutazione d'impatto	**ALTO**

Il risultato complessivo della valutazione dell'impatto è il più alto identificato e pertanto l'impatto complessivo valutato è **ALTO**.

Oltre alle ipotesi formulate in questo esempio, potrebbero verificarsi casi in cui l'impatto complessivo potrebbe persino essere considerato **MOLTO ALTO**, ad esempio quando il trattamento si riferisce a pazienti minori di età.

6.3.3 Probabilità di occorrenza di una minaccia

In base alle domande e all'approccio presentati nella sezione 2.1.3, per ogni valore specifico inerente al trattamento dei dati considerato in questo specifico scenario pratico è possibile formulare le seguenti valutazioni:

- **Risorse di rete e tecniche:** la probabilità di occorrenza di una minaccia è considerata di valore **ALTO**, poiché il sistema è connesso a Internet ed è possibile fornire l'accesso al sistema di trattamento dei dati personali interno attraverso Internet. Inoltre, diversi strumenti e sistemi sono interconnessi e un elevato numero di dispositivi in rete va parimenti protetto.
- **Processi / Procedure relative al trattamento dei dati personali:** la probabilità di occorrenza di una minaccia è di valore **MEDIO**, in quanto i ruoli e le responsabilità sono complessi nello scenario pratico considerato, a causa di molti attori e sistemi coinvolti.
- **Parti / Persone coinvolte nel trattamento dei dati personali:** la probabilità di occorrenza di una minaccia è di valore **ALTO** quando viene utilizzato un responsabile del trattamento che fornisce servizi di tipo cloud. Ad ogni modo, tale è il valore anche se il trattamento viene eseguito da un numero predefinito di dipendenti e si presume che essi siano periodicamente destinatari di iniziative di sensibilizzazione.
- **Settore di operatività e scala/dimensione del trattamento :** la probabilità di occorrenza di una minaccia è di valore **ALTO** in quanto il settore di operatività potrebbe essere considerato soggetto ad attacchi informatici e potenzialmente potrebbe essere coinvolto un numero elevato di interessati. Tuttavia, si dà per presupposto che non si sia verificata alcuna violazione dei dati personali in passato.

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
Risorse di rete e tecniche	ALTO	3
Processi / Procedure relative al trattamento dei dati personali	ALTO	2
Parti / Persone coinvolte nel trattamento dei dati personali	ALTO	3
Settore di attività e scala di trattamento	ALTO	3
Probabilità complessiva di occorrenza di una minaccia	**ALTO (11)**	

6.3.4 Valutazione del rischio

Utilizzando i risultati della valutazione dell'impatto e della probabilità di minacce, il rischio viene calcolato sulla base di (vedi Sezione 2.1.4.).

		LIVELLO D'IMPATTO		
		Bas	Me	Alto/ Molto
PROBABILITA' MINACCIA	B			
	M			
	A			X

In particolare, il rischio complessivo per questo caso particolare è generalmente considerato **ALTO**. L'allegato A (A.1 e A.2 e A.3) può essere utilizzato per l'adozione di misure adeguate al rischio presentato.

7. Scenario pratico specifico: il settore dell'istruzione

7.1 Prima infanzia - l'asilo nido

Si consideri il caso di una scuola per la prima infanzia che utilizza una piattaforma web per la comunicazione quotidiana delle attività fisiche, intellettuali, linguistiche, emotive e sociali dei propri alunni, tra la scuola e i genitori. Inoltre la piattaforma può anche includere informazioni sulla salute, l'appetito e l'indole dei bambini (fornite dai genitori). I genitori sono anche in grado di comunicare con l'insegnante e cercare consigli e supporto su come nutrire e supportare meglio lo sviluppo cognitivo e socio-emotivo del loro bambino. La piattaforma viene ospitata presso un provider di hosting riconosciuto dall'UE e gestita dagli insegnanti. Ogni insegnante gestisce e aggiorna le informazioni sui bambini assegnati alla propria classe, mentre l'amministrazione generale della piattaforma viene eseguita dalla segreteria della scuola. I genitori vengono registrati sulla piattaforma dalla segreteria e possono solo accedere ed aggiornare i dati del loro bambino. Si suppone che vengano utilizzate *best practices* per impedire l'accesso non autorizzato, che siano definiti chiaramente e comunicati i ruoli e le responsabilità dei dipendenti coinvolti e che vengano creati i file di registro per tutte le attività di elaborazione dei dati. La piattaforma elabora i seguenti dati: nome, cognome, data di nascita, indirizzo di casa, informazioni giornaliere sulle prestazioni (inclusi alimenti, attività, ecc.), dati sanitari, allergie, intolleranze alimentari del bambino e il nome, il cognome il numero di telefono, il numero di contatto di emergenza dei rispettivi genitori.

7.1.1 Descrizione del trattamento e del relativo contesto

PROCESSING OPERATION DESCRIPTION	EARLY CHILDHOOD SCHOOL COMMUNICATION PLATFORM	
Dati personali oggetto di trattamento	**Nome e cognome, data di nascita; Indirizzo, informazioni sulle attività giornaliere dei bambini (mensa, attività, etc), dati sanitari, allergie, intolleranze alimentari, nome e cognome dei genitori, recapiti telefonici di contatto, contatti per emergenze. contact number**	
Finalità del trattamento	**Prestazione di servizi relativi all'istruzione (comunicazione giornaliera dello sviluppo dei bambini)**	
Interessati	**Bambini e Genitori**	
Mezzi impiegati per il trattamento	**Web based**	
Destinatari dei dati	**Esterni**	**Genitori**
	Interni	**Segreteria, Insegnanti**
Responsabile del trattamento	**Web hosting provider**	

7.1.2 Valutazione di impatto

Perdita di riservatezza

Nell'ambito dell'operazione di trattamento specifica, l'impatto della perdita di riservatezza è considerato come **MEDIO**, in quanto in alcuni casi gli individui (bambini e genitori) potrebbero sperimentare notevoli effetti negativi derivanti dalla divulgazione di determinati dati (ad esempio riguardo al comportamento del bambino o alla comunicazione o ai modelli di alimentazione).

Perdita dell'integrità

L'impatto derivante dalla perdita di integrità può parimenti essere considerato come di valore MEDIO, in quanto la modifica non autorizzata di questi dati potrebbe ostacolare la fornitura di un servizio adeguato da parte dell'asilo nido (in particolare per quanto riguarda le allergie, i modelli alimentari e altri dati correlati).

Perdita della disponibilità

L'impatto derivante dalla perdita di disponibilità può essere considerato **BASSO**, dal momento che l'indisponibilità dei dati può determinare limitati inconvenienti che possono essere facilmente superati (ad esempio inserendo nuovamente i dati nella piattaforma o comunicando con i genitori attraverso altri mezzi).

VALUTAZIONE DELL'IMPATTO		
Riservatezza	Integrità	Disponibilità
Medio	**Medio**	**Basso**
	Valutazione complessiva dell'impatto	**MEDIO**

Essendo il risultato complessivo della valutazione dell'impatto il più alto identificato, l'impatto complessivo valutato risulta essere **MEDIO**.

Oltre alle ipotesi formulate nell'ambito del presente scenario pratico potrebbero verificarsi casi in cui l'impatto complessivo potrebbe essere superiore a quello appena sopra calcolato . Un esempio di tali ipotesi è quando vi sono particolari piani dietetici seguiti da bambini specifici (ad esempio a causa di credenze religiose). Un altro esempio è il caso di una scuola specificamente dedicata ai bambini con condizioni speciali o di disabilità.

7.1.3 Probabilità di occorrenza di una minaccia

In base alle domande e all'approccio presentati nella sezione 2.1.3, per ogni valore specifico inerente al trattamento dei dati considerato in questo specifico scenario pratico è possibile formulare le seguenti valutazioni:

- **Risorse tecniche e di rete:** La probabilità di occorrenza di una minaccia è di valore **MEDIO**, poiché il sistema è connesso ad Internet ed è possibile fornire l'accesso al sistema di elaborazione dei dati personali tramite Internet. Tuttavia, vengono utilizzate *best practices* per impedire l'accesso non autorizzato e si dà per presupposto il loro aggiornamento.
- **Processi / Procedure relative al trattamento dei dati personali:** La probabilità di occorrenza di una minaccia è di valore **MEDIO**, in quanto vi sono diversi soggetti che accedono alla stessa piattaforma e non è chiaro se i ruoli e le responsabilità siano stati chiaramente definiti. Tuttavia, esiste una politica interna di utilizzo e vengono creati file di registro per tracciare qualsiasi attività di trattamento svolta.

- **Parti / Persone coinvolte nel trattamento dei dati personali:** La probabilità di occorrenza di una minaccia è di valore **MEDIO** poiché è presente un Responsabile esterno dei dati personali e i dipendenti sono in grado di trasferire, archiviare o elaborare dati personali al di fuori dei locali della scuola. Tuttavia, si presume sia chiaramente definito che l'uso della rete, del sistema e delle risorse fisiche.
- **Settore di operatività e scala/dimensione del trattamento :** la probabilità di occorrenza di una minaccia è di valore **BASSO** poiché il settore di operatività (istruzione) non è generalmente considerato soggetto ad attacchi informatici e l'operazione di trattamento non riguarda un numero elevato di interessati. Si presume che nessuna violazione dei dati personali sia mai avvenuta in passato.

ASSESSMENT AREA	PROBABILITA'	
	LIVELLO	PUNTEGGIO
Risorse di rete e Tecniche	**Medio**	**2**
Processi / Procedure relative al trattamento dei dati personali	**Medio**	**2**
Parti / Persone coinvolte nel trattamento dei dati personali	**Medio**	**2**
• Settore di operatività e scala/dimensione del trattamento	**Basso**	**1**
Probabilità complessiva di occorrenza di una minaccia	**Medio (7)**	

7.1.4 Valutazione del rischio

Tenuto conto dei risultati della valutazione dell'impatto e della probabilità di occorrenza delle minacce, il rischio viene calcolato sulla base alla Sezione 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low			
	Medium		X	
	High			

In particolare, il rischio complessivo per lo scenario pratico qui preso in considerazione è in via generale considerato **MEDIO**. È possibile utilizzare l'allegato A (A.1) per adottare misure adeguate al rischio presentato.

È necessario notare che il rischio potrebbe essere diverso (ALTO) in condizioni direttamente correlate ad uno specifico trattamento di dati e influire sull'impatto o sulla probabilità di occorrenza della minaccia (si vedano anche le relative considerazioni nella sezione 7.1.2).

7.2 Piattaforme di e-learning universitario

Si prenda in considerazione il seguente, ulteriore scenario pratico: quello di una università che offre un corso di management attraverso una piattaforma di e-learning ospitata presso un server web interno all'Università. Attraverso la piattaforma, i professori e l'amministrazione possono inviare annunci agli studenti e gli studenti possono recuperare i materiali del loro corso, le dispense e le diapositive, inviare compiti, effettuare valutazioni e test e ottenere risultati e voti. All'inizio di ogni semestre il dipartimento amministrativo dell'università iscrive gli studenti ai moduli didattici e assegna, sia agli studenti che al personale accademico, i rispettivi diritti di accesso e privilegi. Si presuppone poi che vengano utilizzate *best practices* per impedire l'accesso non autorizzato, che siano chiaramente definiti e comunicati i ruoli e le responsabilità dei dipendenti coinvolti e che vengono creati i relativi file di log per tutte le attività di trattamento dei dati. Per i risultati della valutazione, i professori consegnano i punteggi finali in formato cartaceo all'amministrazione la quale li inserisce nella piattaforma. La piattaforma elabora i seguenti dati: a) Studenti: nome e cognome, data di nascita, data di ammissione, corso (i) selezionato(i), risultati della valutazione, voti; b) Personale accademico: nome e cognome, data di nascita, corso (i) assegnato (i).

7.2.1 Descrizione del trattamento e del relativo contesto

DESCRIZIONE DEL TRATTAMENTO	PIATTAFORMA UNIVERSITARIA DI E-LEARNING	
Dati Personali oggetto di trattamento	Studenti: nome e cognome, data di nascita, data di ammissione, corsi prescelti, risultati degli esami e delle valutazioni, voti. Personale docente e staff accademico : nome e cognome, data di nascita, corsi accademici assegnati.	
Finalità del trattamento	Gestione della piattaforma e-Learning e del corso di management, inclusi l'inserimento di valutazioni e test	
Interessati	Studenti, Professori	
Mezzi impiegati per il trattamento	Piattaforma e-Learning per il corso di management	
Destinatari dei dati	Interni	Uffici Amministrazione dell'Università
	Interni	Capi Dipartimento
Responsabile del trattamento	In-house (Nessun Responsabile del trattamento)	

7.2.2 Valutazione di impatto

Perdita di riservatezza

Nell'ambito del trattamento descritto dal presente scenario pratico l'impatto derivante dalla perdita di riservatezza è considerato di valore **MEDIO**, in quanto gli interessati potrebbero sperimentare notevoli effetti negativi derivanti dalla divulgazione non autorizzata di dati personali relativi alle loro prestazioni, voti e risultati accademici.

Perdita di integrità

L'impatto della perdita di riservatezza è considerato di valore **MEDIO** , poiché gli interessati potrebbero sperimentare notevoli effetti negativi derivanti dalla modifica non autorizzata di dati personali che influenzano direttamente le loro prestazioni e i loro voti.

Perdita di disponibilità

L'impatto della perdita di riservatezza è considerato **BASSO**, poiché gli interessati sperimenterebbero limitati inconvenienti derivanti dalla indisponibilità dei dati personali, che possono essere facilmente

superati (presupponendo che siano disponibili back-up e informazioni sui risultati di valutazione e sui voti anche offline).

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Medium**	**Low**
	Overall Impact Evaluation	**MEDIUM**

Il risultato complessivo della valutazione dell'impatto è il più alto identificato e pertanto è valutato come **MEDIO**.

Oltre alle ipotesi formulate in questo esempio, potrebbero verificarsi casi in cui l'impatto complessivo potrebbe essere diverso (superiore) rispetto a quello calcolato sopra. Un esempio di tali ipotesi potrebbe essere la possibile integrazione della piattaforma con i profili dei social network, dove vengono anche raccolti altri dati sugli studenti (ad esempio stile di vita, abitudini, ecc.). Un altro esempio potrebbe essere il possibile utilizzo della piattaforma per svolgere statistiche.

7.2.3 Probabilità di occorrenza di una minaccia

In base alle domande e all'approccio presentati nella sezione 2.1.3, per ogni valore specifico inerente al trattamento dei dati considerato in questo specifico scenario pratico è possibile formulare le seguenti valutazioni:

- **Risorse di rete e tecniche:** la probabilità di occorrenza delle minacce è di valore **MEDIO**, poiché il sistema è connesso alla rete esterna ed è possibile fornire l'accesso al sistema di trattamento dei dati personali interno tramite Internet. Tuttavia, si presume che vengano utilizzate *best practices* aggiornate per impedire l'accesso non autorizzato.
- **Processi / Procedure relative al trattamento di dati personali:** la probabilità di occorrenza di una minaccia è di valore **MEDIO**, a causa delle diverse parti che accedono al sistema e del fatto che i ruoli e le responsabilità devono essere chiaramente definiti. Tuttavia, si dà per presupposto che vi sia una policy di utilizzo interna e che vengano creati appositi file di log per tracciare qualsiasi attività di trattamento svolta .
- **Parti / Persone coinvolte nel trattamento dei dati personali:** la probabilità di occorrenza di una minaccia è **BASSA** poiché c'è un responsabile del trattamento terzo. Tuttavia, si dà per presupposto che siano definite le policy per l'uso della rete, del sistema e delle risorse fisiche e che i dipendenti siano in grado di trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'Università .
- **Settore di operatività e scala/dimensione del trattamento:** la probabilità di occorrenza di una minaccia è di valore **MEDIO** poiché il trattamento riguarda un numero elevato di interessati e il settore di operatività (istruzione superiore - università) potrebbe potenzialmente essere soggetto a attacchi informatici. Si dà per presupposto che non si sia mai verificata in passato alcuna violazione dei dati personali.

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
Risorse di rete e tecniche	Medio	2
Processi / Procedure relative al trattamento di dati personali	Medio	2

Parti / Persone coinvolte nel trattamento dei dati personali	Basso	1
Settore di operatività e scala/dimensione del trattamento	Medio	1
Probabilità complessiva di occorrenza di una minaccia	Medio (7)	

7.2.4 Valutazione del rischio

Utilizzando i risultati della valutazione dell'impatto e della probabilità di occorrenza delle minacce, il rischio viene calcolato sulla base di Sezione 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low			
	Medium		X	
	High			

In particolare, il rischio generale per questo caso particolare è generalmente considerato come **MEDIO**. L'allegato A (A.1 e A.2) può essere utilizzato per l'adozione di misure adeguate al rischio presentato.

È necessario notare che il rischio potrebbe essere diverso (ALTO) in condizioni direttamente correlate ad uno specifico trattamento di dati e influire sull'impatto o sulla probabilità di occorrenza della minaccia (vedere anche le considerazioni rilevanti nella sezione 7.2.2).

8. Conclusioni

La sicurezza del trattamento dei dati personali è già un obbligo di legge per i titolari del trattamento, tuttavia il Regolamento Generale UE sulla protezione dei dati personali rafforza le relative previsioni (sia nella sostanza che nel contesto) ed estende la responsabilità di corretta adozione delle adeguate misure di sicurezza nel trattamento anche direttamente ai responsabili del trattamento dei dati. Considerate le caratteristiche specifiche delle PMI, come per esempio le risorse limitate e l'indisponibilità di personale qualificato, il presente Manuale richiama i suggerimenti metodologici delle linee guida 2016 dell'ENISA per le PMI sulla sicurezza del trattamento dei dati personali e fornisce scenari di applicazione pratica specifici. Ogni scenario pratico corrisponde a una specifica operazione di trattamento dei dati personali e formula ipotesi specifiche sull'ambiente di trattamento dei dati e sul contesto generale del trattamento. Gli esempi forniti si concentrano solo sulle misure di sicurezza e non mirano a fornire alcuna analisi legale o valutazione della conformità al GDPR per le specifiche operazioni di trattamento dei dati considerate negli esempi.

Alcune conclusioni e raccomandazioni pertinenti possono essere conclusivamente formulate come segue.

Approccio guidato e di dettaglio alle misure di sicurezza per ciascun singolo trattamento.

Operazioni di trattamento dei dati personali simili tra loro in astratto possono tuttavia diversificarsi in concreto a seconda dei titolari del trattamento, o tenendo conto delle loro specificità, degli strumenti utilizzati per il trattamento dei dati personali, delle categorie dei soggetti interessati, dei responsabili esterni del trattamento e dei destinatari dei dati, etc. Pertanto, un approccio standardizzato alle misure di sicurezza idonee da adottare che prescinda dalla valutazione preventiva delle peculiarità di ciascun singolo trattamento in concreto, non può essere considerato fattibile e pragmatico. Ogni operazione di trattamento dovrebbe essere esaminata separatamente tenendo anche conto del contesto e dell'ambiente del trattamento. Pertanto, anziché classificare a priori le operazioni di elaborazione in livelli di rischio, l'attenzione dovrebbe essere spostata sulla responsabilizzazione e guida dei titolari del trattamento dei dati per comprendere innanzitutto le loro operazioni di trattamento e quindi valutare il livello di rischio e implementare le misure di sicurezza appropriate.

Gli organismi competenti dell'UE, i responsabili delle politiche e le Autorità di controllo dell'UE (ad esempio le Autorità per la protezione dei dati) dovrebbero elaborare linee guida pratiche e modulari che siano in grado di supportare e assistere diverse tipologie di titolari del trattamento e rivolgersi a comunità di soggetti interessati specifici.

DPO esperti

La responsabilizzazione dei titolari del trattamento può anche essere percepita come una questione di sensibilizzazione alle loro operazioni di trattamento e alle disposizioni generali del GDPR. Tuttavia, per essere in grado di gestire la conformità in maniera più strutturata, piuttosto che un'azione correttiva sporadica, si prevede che cerchino supporto e guida. In quest'ottica è centrale il ruolo di un responsabile della protezione dei dati adeguatamente qualificato (DPO), anche nel caso in cui la designazione di un DPO non sia obbligatoria ai sensi dell'articolo 37 del GDPR. Detto questo, è importante notare che l'adempimento di questo ruolo richiede sia una buona comprensione del quadro giuridico sulla protezione

dei dati, sia delle moderne tecnologie IT (e delle relative best practice sulla sicurezza), che oggi costituiscono la base per la maggior parte dei più comuni strumenti di elaborazione dei dati[9].

Gli organismi competenti dell'UE, i responsabili delle politiche e le Autorità di controllo dell'UE (ad esempio le Autorità per la protezione dei dati) dovrebbero definire una serie di competenze professionali e requisiti di base che i responsabili della protezione dei dati dovrebbero soddisfare.

Dimostrare la conformità

Come discusso in precedenza, la sicurezza del trattamento dei dati personali non dovrebbe essere considerata dai titolari del trattamento come un obbligo isolato nell'ambito del GDPR, ma come parte del quadro generale di conformità che dovrebbero sviluppare, attuare e mantenere. La metodologia ENISA può essere utile a tale riguardo in tutti i casi in cui è prevista la valutazione del rischio ai sensi del regolamento (ad esempio notifica delle violazioni dei dati personali). Durante lo sviluppo del suddetto piano di conformità, i titolari del trattamento dei dati dovrebbero cercare di estendere la documentazione del loro adeguamento, oltre il livello imposto dalle disposizioni del GDPR. Ciò non solo garantisce che essi prendano attivamente e positivamente in considerazione i rischi di qualsiasi trattamento di dati che intraprendono, ma anche che intensificheranno i loro sforzi per rispettare il principio di responsabilizzazione e dimostrare la loro conformità. Inoltre, poiché l'approccio basato sul rischio è parte integrante della valutazione dell'impatto sulla protezione dei dati (DPIA), si prevede anche che la disponibilità di documentazione faciliterà l'impegno, anche su base volontaria, della DPIA.

Le associazioni di categoria delle PMI e i titolari del trattamento dati dovrebbero dedicarsi all'elaborazione della teoria della valutazione del rischio e di una documentazione strutturata come parte integrante dei sistemi di gestione delle informazioni per i dati personali.

La Autorità di controllo (ad esempio le Autorità per la protezione dei dati) dovrebbero fornire assistenza e supporto alla formazione in questo contesto per i titolari del trattamento dei dati.

Schemi di certificazione modulari

I meccanismi di certificazione della protezione dei dati del GDPR (articoli 42 e 43) possono svolgere un ruolo significativo nel consentire ai titolari del trattamento di conseguire e dimostrare l'esistenza di garanzie adeguate, comprese le misure di sicurezza, e quindi la conformità delle loro operazioni di trattamento alle disposizioni del GDPR. Poiché i titolari del trattamento dei dati, e in particolare le PMI, si affidano sempre di più a tecnologie, prodotti e servizi di terzi, è importante essere incoraggiati e motivati a valutare il livello di conformità di tali parti e, se possibile, acquisire tali certificazioni. Data la natura volontaria dei meccanismi di certificazione ai sensi del GDPR, è fondamentale che i titolari del trattamento dati siano motivati e incoraggiati ad aderire agli schemi di certificazione, nonché ad optare per responsabili esterni del trattamento che seguono pratiche simili.

I responsabili delle politiche e le Autorità di controllo dell'UE (ad esempio le Autorità per la protezione dei dati) dovrebbero definire e promuovere schemi di certificazione di protezione dei dati modulari, che soddisfino le esigenze delle PMI e consentano loro di raggiungere e dimostrare la conformità.

[9] Si vedano le pertinenti Linee Guida sul Responsabile della protezione dei dati personali adottate dall' Article 29 Data Protection Working Party,
http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

Le associazioni di categoria delle PMI e i titolari del trattamento dati dovrebbero optare per responsabili esterni del trattamento dati che aderiscono alle migliori pratiche di sicurezza e agli attinenti meccanismi di certificazione.

Nuove metodologie di gestione del rischio

La gestione dei rischi di sicurezza delle informazioni e la gestione dei rischi di sicurezza dei dati personali riguardano il calcolo dei livelli di rischio da due punti di vista diversi: il primo si concentra sull'impatto per il titolare del trattamento e il secondo sull'impatto per gli interessati. Tuttavia, entrambi gli approcci confluiscono in una serie di misure organizzative e tecniche che devono essere implementate, mantenute e riviste dal titolare del trattamento. Indipendentemente dalle specificità descritte in precedenza, una metodologia comune, che abbraccia entrambi gli aspetti, potrebbe consentire ai titolari del trattamento dei dati, in particolare alle PMI, di seguire un approccio sistematico per conseguire la conformità.

La comunità di ricerca e gli organismi competenti dell'UE, in stretta collaborazione con le Autorità di controllo (ad esempio le Autorità per la protezione dei dati), dovrebbero proporre metodologie che combinano la gestione dei rischi di sicurezza e la gestione dei rischi derivanti dal trattamento di dati personali.

Comunicazione e sensibilizzazione

Le PMI europee stanno iniziando soltanto a considerare i cambiamenti che devono intraprendere e ad ampliare la visione della loro sicurezza delle informazioni e delle strategie aziendali esistenti al fine di soddisfare i requisiti legali. Tuttavia, l'entità delle modifiche necessarie da integrare nei processi aziendali esistenti, non può essere prevista. I titolari del trattamento dati sono spesso riluttanti e percepiscono tali cambiamenti come un ostacolo piuttosto che un'opportunità per posizionarsi in un mercato di nuova creazione, che rafforza anche la sicurezza e la fiducia dei loro clienti.

Le associazioni di categoria delle PMI, in stretta collaborazione con gli organismi e le Autorità di controllo competenti dell'UE (ad esempio le Autorità per la protezione dei dati), dovrebbero comunicare e incoraggiare i titolari del trattamento a intraprendere azioni verso la sicurezza e la conformità della privacy come vantaggio competitivo accanto agli obblighi legali sottostanti.

Le associazioni di categoria delle PMI, in stretta collaborazione con gli organismi e le Autorità di controllo competenti dell'UE (ad esempio le Autorità per la protezione dei dati), dovrebbero comunicare e incoraggiare i titolari del trattamento a intraprendere azioni verso la sicurezza e la conformità della privacy come vantaggio competitivo accanto agli obblighi legali sottostanti.

Allegato A: misure tecniche e organizzative

In ogni sezione (A.1, A.2 e A.3) le misure di sicurezza sono presentate per livello di rischio (basso: verde, medio: giallo, alto: rosso). Per conseguire la scalabilità, si presume che tutte le misure descritte nel livello basso (verde) siano applicabili a tutti i livelli. Allo stesso modo, le misure presentate nel livello medio

(giallo) sono applicabili anche ad alto livello di rischio. Le misure presentate nel livello alto (rosso) non sono applicabili a nessun 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	IDENTIFICATORE DELLA MISURA	DESCRIZIONE DELLA MISURA DI SICUREZZA	PERTINENTE ALLA CERTIFICAZIONE ISO / IEC 27001: 2013 CONTROLLO
Politica di sicurezza e procedure per la protezione dei dati personali	**A.1**	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	**A.5 Politica di sicurezza**
Politica di sicurezza e procedure per la protezione dei dati personali	**A.2**	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.	**A.5 Politica di sicurezza**
Ruoli e responsabilità	**B.1**	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	**A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni**
Ruoli e responsabilità	**B.2**	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.	**A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni**
Politica di controllo degli accessi	**C.1**	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati .	**A.9.1.1 Politica di controllo degli accessi**
Gestione risorse/asset	**D.1**	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	**A.8 Asset management**
Gestione risorse/asset	**D.2**	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	**A.8 Asset management**
Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT	**E.1**	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	**A. 12.1 Procedure operative e responsabilità**

Gestione delle operazioni di sviluppo software e dei test di sviluppo	**E.2**	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	**A. 12.1 Procedure operative e responsabilità**
Responsabili del trattamento	**F.1**	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.	**A.15 Rapporti con i fornitori**
Responsabili del trattamento	**F.2**	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	**A.15 Rapporti con i fornitori**
Responsabili del trattamento	**F.3**	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.	**A.15 Rapporti con i fornitori**
Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)	**G.1**	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	**A.16 Gestione degli incidenti sulla sicurezza delle informazioni**
Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)	**G.2**	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.	**A.16 Gestione degli incidenti sulla sicurezza delle informazioni**
Business continuity	**H.1**	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).	**A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa**
Obblighi di confidenzialità imposti al personale	**I.1**	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione .	**A.7 Sicurezza delle risorse umane**

Formazione	**J.1**	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.	**A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione**
Controllo degli accessi e autenticazione	**K.1**	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.	**A.9 Controllo degli accessi**
Controllo degli accessi e autenticazione	**K.2**	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.	**A.9 Controllo degli accessi**
Controllo degli accessi e autenticazione	**K.3**	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.	**A.9 Controllo degli accessi**
Controllo degli accessi e autenticazione	**K.4**	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).	**A.9 Controllo degli accessi**
Generazione di file di log e monitoraggio	**L.1**	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	**A.12.4 Registrazione e monitoraggio**
Generazione di file di log e monitoraggio	**L.2**	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento	**A.12.4 Registrazione e monitoraggio**
Sicurezza di Server e Database	**M.1**	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	**A. 12 Operations security**
Sicurezza di Server e Database	**M.2**	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR) .	**A. 12 Operations security**
Sicurezza delle Postazioni di lavoro	**N.1**	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza delle Postazioni di lavoro	**N.2**	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza delle Postazioni di lavoro	**N.3**	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza delle Postazioni di lavoro	**N.4**	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**

Sicurezza delle Postazioni di lavoro	**N.5**	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica	**O.1**	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	**A.13 Communications Security**
Back-ups	**P.1**	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	**A.12.3 Back-Up**
Back-ups	**P.2**	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	**A.12.3 Back-Up**
Back-ups	**P.3**	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	**A.12.3 Back-Up**
Back-ups	**P.4**	I backup completi devono essere eseguiti regolarmente.	**A.12.3 Back-Up**
Dispositivi mobili / portatili	**Q.1**	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	**A. 6.2 Dispositivi mobili e teleworking**
Dispositivi mobili / portatili	**Q.2**	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.	**A. 6.2 Dispositivi mobili e teleworking**
Dispositivi mobili / portatili	**Q.3**	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.	**A. 6.2 Dispositivi mobili e teleworking**
Sicurezza del ciclo di vita delle applicazioni	**R.1**	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.2**	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.3**	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.4**	Dovrebbero essere seguiti standard e pratiche di codifica sicure.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.5**	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Cancellazione / eliminazione dei dati	**S.1**	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.	**A. 8.3.2 Smaltimento di supporti e 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**
Cancellazione / eliminazione dei dati	**S.2**	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	**A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**

Sicurezza fisica	**T.1**	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	**A.11 - Sicurezza fisica e ambientale**

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	IDENTIFICATORE DELLA MISURA DI SICUREZZA	DESCRIZIONE DELLA MISURA DI SICUREZZA	PERTINENTE ALLA CERTIFICAZIONE ISO / IEC 27001: 2013 CONTROLLO
Policy di sicurezza e procedure per la protezione dei dati personali	**A.3**	L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate	**A.5 Policy di sicurezza**
Policy di sicurezza e procedure per la protezione dei dati personali	**A.4**	La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.	**A.5 Policy di sicurezza**
Policy di sicurezza e procedure per la protezione dei dati personali	**A.5**	Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.	**A.5 Policy di sicurezza**
Ruoli e responsabilità	**B.3**	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.	**A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni**
Politica di controllo degli accessi	**C.2**	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.	**A.9.1.1 Politica di controllo degli accessi**
Politica di controllo degli accessi	**C.3**	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).	**A.9.1.1 Politica di controllo degli accessi**
Gestione risorse / asset	**D.3**	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	**A.8 Gestione delle risorse**
Gestione delle modifiche	**E.3**	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.	**A. 12.1 Procedure operative e responsabilità**
Responsabili del trattamento	**F.4**	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.	**A.15 Rapporti con i fornitori**

Gestione degli incidenti / Personal data breaches	**G.3**	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.	**A.16 Gestione degli incidenti di sicurezza delle informazioni**
Business continuity	**H.2**	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	**A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa**
Business continuity	**H.3**	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.	**A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa**
Obblighi di confidenzialità imposti al personale	**I.2**	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.	**A.7 Sicurezza delle risorse umane**
Formazione	**J.2**	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.	**A.7.2.2 Consapevolezza, educazione e formazione alla sicurezza delle informazioni**
Controllo degli accessi e autenticazione	**K.5**	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.	**A.9** Controllo degli accessi
Controllo degli accessi e autenticazione	**K.6**	Le password degli utenti devono essere memorizzate in una forma "hash".	**A.9** Controllo degli accessi
Generazione di file di log e monitoraggio	**L.3**	necessario Dovrebbe essere necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.	**A.12.4 Registrazione e monitoraggio**
Generazione dei file di log e monitoraggio	**L.4**	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.	**A.12.4 Registrazione e monitoraggio**
Generazione dei file di log e monitoraggio	**L.5**	Un sistema di monitoraggio dovrebbe generare i file log e produrre report sullo stato del sistema e notificare potenziali allarmi.	**A.12.4 Registrazione e monitoraggio**
Sicurezza del server / database	**M.3**	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.	**A. 12 Sicurezza delle operazioni**
Sicurezza del server / database	**M.4**	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.	**A. 12 Sicurezza delle operazioni**
Sicurezza del server / database	**M.5**	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	**A. 12 Sicurezza delle operazioni**
Sicurezza della Postazione di lavoro	**N.6**	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza della rete / comunicazione	**O.2**	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.	**A.13 Sicurezza delle comunicazioni**

Sicurezza della rete / comunicazione	**O.3**	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.	**A.13 Sicurezza delle comunicazioni**
Sicurezza della rete / comunicazione	**O.4**	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.	**A.13 Sicurezza delle comunicazioni**
Back-ups	**P.5**	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.	**A.12.3 Back-Up**
Back-ups	**P.6**	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.	**A.12.3 Back-Up**
Back-ups	**P.7**	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.	**A.12.3 Back-Up**
Back-ups	**P.8**	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.	**A.12.3 Back-Up**
Dispositivi mobili / portatili	**Q.4**	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.	**A. 6.2 Dispositivi mobili e telelavoro**
Dispositivi mobili / portatili	**Q.5**	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.	**A. 6.2 Dispositivi mobili e telelavoro**
Dispositivi mobili / portatili	**Q.6**	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.	**A. 6.2 Dispositivi mobili e telelavoro**
Dispositivi mobili / portatili	**Q.7**	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.	**A. 6.2 Dispositivi mobili e telelavoro**
Sicurezza del ciclo di vita delle applicazioni	**R.6**	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.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.7**	Devono essere eseguiti test periodici di penetrazione.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.8**	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.9**	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Cancellazione / eliminazione dei dati	**S.3**	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.	**A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**
Cancellazione / eliminazione dei dati	**S.4**	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.	**A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**

Sicurezza fisica	**T.2**	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.	**A.11 – Sicurezza fisica e ambientale**
Sicurezza fisica	**T.3**	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	**A.11 – Sicurezza fisica e ambientale**
Sicurezza fisica	**T.4**	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.	**A.11 – Sicurezza fisica e ambientale**
Sicurezza fisica	**T.5**	Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.	**A.11 – Sicurezza fisica e ambientale**
Sicurezza fisica	**T.7**	Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere attivati nella sala server.	**A.11 Sicurezza fisica e ambientale**
Sicurezza fisica	**T.8**	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.	**A.11 – Sicurezza fisica e ambientale**

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	IDENTIFICATORE DELLA MISURA DI SICUREZZA	DESCRIZIONE DELLA MISURA DI SICUREZZA	PERTINENTE ALLA CERTIFICAZIONE ISO / IEC 27001: 2013 CONTROLLO
Procedure e policy di sicurezza per la protezione dei dati personali	**A.6**	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.	**A.5 Security policy**
Ruoli e responsabilità	**B.4**	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.	**A.6.1.1 Information security roles and responsibilities**
Ruoli e responsabilità	**B.5**	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.	**A.6.1.1 Information security roles and responsibilities**
Policy di controllo degli accessi	**C.4**	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff	**A.9.1.1 Access control policy**
Gestione risorse / asset	**D.4**	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.	**A.8 Asset management**
Responsabili del trattamento	**F.5**	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.	**A.15 Rapporti con i fornitori**
Gestione degli incidenti / Violazione dei dati	**G.4**	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti	**A.16 Gestione degli incidenti di sicurezza**

personali (data breaches)		l'evento e le successive azioni di mitigazione intraprese.	
Business continuity	**H.4**	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.	**A.17 Aspetti di sicurezza nella gestione della business continuity**
Business continuity	**H.5**	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.	**A.17 Aspetti di sicurezza nella gestione della business continuity**
Obblighi di confidenzialità imposti al personale	**L.3**	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).	**A7 Sicurezza delle risorse umane**
Formazione	**J3**	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.	**A.7.2.2. Consapevolezza, educazione e formazione alla sicurezza delle informazioni**
Controllo degli accessi e autenticazione	**K.7**	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.	**A.9 Controllo degli accessi**
Controllo degli accessi e autenticazione	**K.8**	Dovrebbe essere una soggetto ad autenticazione ogni dispositivo (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale	**A.9 Controllo degli accessi**
Sicurezza Server/Database	**M.6**	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.	**A.12 Operazioni di sicurezza**
Sicurezza della postazione di lavoro	**N.7**	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).	**A.14.1 Requisiti di sicurezza nei sistemi**
Sicurezza della postazione di lavoro	**N.8**	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.	**A.14.1 Requisiti di sicurezza nei sistemi**
Sicurezza della postazione di lavoro	**N.9**	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.	**A.14.1 Requisiti di sicurezza nei sistemi**
Sicurezza della rete / comunicazioni	**O.5**	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.	**A.13 Sicurezza delle comunicazioni**
Sicurezza della rete / comunicazioni	**O.6**	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.	**A.13 Sicurezza delle comunicazioni**
Sicurezza della rete / comunicazioni	**O.7**	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC)	**A.13 Sicurezza delle comunicazioni**
Back-ups	P.9	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.	A.12.3 Back-Up

Dispositivi Mobili/Portatili	**Q.8**	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte)	**A.6.2 Dispositivi mobile e telelavoro**
Dispositivi Mobili/Portatili	**Q.9**	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.	**A.6.2 Dispositivi mobile e telelavoro**
Cancellazione/Eliminazione dei dati	**S.5**	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.	**A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**
Cancellazione/Eliminazione dei dati	**S.6**	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali.	**A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**

ENISA

European Union Agency for Network and Information Security

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias

Marousi 151 24, Attiki, Greece

TP-02-18-047-EN-N

P O Box 1309, 710 01 Heraklion, Greece Tel: +30 28 14 40 9710 info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-251-6

DOI: 10.2824/569768