Politica per la protezione dei dati personali e per la sicurezza delle informazioni e resilienza dei sistemi

SOMMARIO

Introduzione

Scopo

Questa Politica è stata redatta per testimoniare l'impegno dell'Organizzazione nella tutela dei dati personali e nella protezione e resilienza dei sistemi informativi e delle reti. Il suo obiettivo principale è assicurare un trattamento trasparente, sicuro e conforme alle normative nazionali e comunitarie vigenti.
Parallelamente, la Politica mira a mantenere elevati standard di sicurezza, disponibilità, integrità, riservatezza e resilienza dei sistemi informativi e delle reti, conformemente alla normativa applicabile.
Il fondamento di questa Politica è un approccio basato sulla fiducia degli stakeholder, mirato a salvaguardare la reputazione dell'Organizzazione e garantire una gestione efficace ed efficiente delle attività operative. È previsto, inoltre, un approccio multirischio per l'identificazione, la valutazione e la mitigazione dei rischi relativi alla sicurezza informatica, volto a rafforzare la resilienza delle infrastrutture critiche e assicurare la continuità operativa dell'Organizzazione.

Ambito di Applicazione

La presente Politica si applica a tutti i dati raccolti, trattati, conservati o trasferiti dall'Organizzazione, indipendentemente dal loro formato o origine. Essa include i dati riferibili a clienti, dipendenti, fornitori e qualsiasi altra parte interessata.
La Politica vincola tutte le unità organizzative e i relativi collaboratori, nonché i soggetti terzi che trattano dati anche personali per conto dell'Organizzazione; inoltre, disciplina tutte le attività e i processi legati alla sicurezza e alla gestione del rischio dei sistemi informativi e delle reti, offrendo così un approccio integrato alla protezione dei dati e alla resilienza delle infrastrutture informatiche.

Responsabilità e Governance

La responsabilità della gestione e del rispetto della presente Politica ricade in primo luogo sulla Direzione, che ne garantisce l'attuazione e l'integrazione nei processi organizzativi.
Tuttavia, la protezione dei dati è un dovere condiviso, e tutti i collaboratori che trattano dati personali o meno hanno la responsabilità di comprendere e aderire a questa Politica e a tutti i documenti che ne danno attuazione. Allo stesso modo, tutti i soggetti coinvolti nell'utilizzo, gestione o amministrazione dei sistemi informativi e delle reti sono tenuti a osservare le misure di sicurezza previste, contribuendo attivamente alla protezione dell'integrità, della disponibilità e della riservatezza delle infrastrutture digitali dell'Organizzazione.

Principi Fondamentali

Fondamenti Legali e Normativi della Protezione dei Dati

L'Organizzazione si impegna a rispettare tutte le leggi e i regolamenti applicabili alla protezione dei dati personali. In particolare, questa Politica è in linea con i seguenti principi fondamentali:

1. **liceità, correttezza e trasparenza**: i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. **limitazione della finalità**: i dati sono raccolti per scopi specifici, espliciti e legittimi, e non trattati ulteriormente in modo incompatibile con tali scopi;
3. **minimizzazione dei dati**: i dati raccolti sono adeguati, pertinenti e limitati a ciò che è necessario rispetto agli scopi per i quali sono trattati;

4. **esattezza**: i dati sono accurati e, se necessario, aggiornati; vengono adottate tutte le misure ragionevoli per garantire che i dati inesatti, rispetto agli scopi per i quali sono trattati, siano cancellati o rettificati senza indugio;
5. **limitazione della conservazione**: i dati sono conservati in una forma che consente l'identificazione degli interessati per un periodo non superiore al conseguimento degli scopi per i quali i dati sono trattati;
6. **integrità e riservatezza**: i dati sono trattati in modo da garantire una sicurezza adeguata dei dati personali, inclusa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danno accidentali, mediante l'adozione di misure tecniche o organizzative appropriate.

Fondamenti Legali e Normativi della Sicurezza dei Sistemi informativi e delle reti

L'Organizzazione si impegna a rispettare tutte le leggi e i regolamenti applicabili alla Sicurezza dei sistemi informativi e delle reti. In particolare, questa Politica è in linea con i seguenti principi fondamentali:

1. **gestione multirischio**: l'Organizzazione adotta un approccio basato sulla valutazione continua e sulla gestione integrata dei rischi (approccio multirischio), incorporato nei processi. Tale approccio consente di identificare, analizzare e mitigare in modo coordinato rischi di natura diversa, tenendo conto delle interdipendenze tra i sistemi, delle minacce emergenti e degli impatti potenziali sulla continuità operativa e sulla sicurezza delle reti e dei servizi critici;
2. **resilienza e continuità operativa**: la resilienza operativa è promossa attraverso la definizione e l'attuazione di strategie di risposta agli incidenti e piani di continuità operativa; l'obiettivo è garantire il mantenimento o il rapido ripristino dei servizi critici anche in caso di attacchi informatici, guasti tecnologici o altre minacce rilevanti;
3. **proporzionalità delle misure**: le misure tecniche e organizzative sono adottate in modo proporzionato, tenendo conto del ruolo dell'Organizzazione a livello regionale, nazionale o internazionale, della disponibilità di fornitori alternativi sul mercato per il medesimo prodotto o servizio, nonché dell'impatto potenziale che un incidente potrebbe avere sia sui servizi erogati dall'Organizzazione, sia sulle Organizzazioni a valle della catena di fornitura;
4. **verifica dell'affidabilità delle risorse umane**: la cybersecurity è integrata nelle pratiche di gestione delle risorse umane: l'obiettivo è garantire che l'accesso ai sistemi informativi e di rete sia consentito solo al personale autorizzato, individuato previa valutazione dell'esperienza, competenze e affidabilità;
5. **verifica della supply chain**: la sicurezza informatica si estende anche ai fornitori che forniscono servizi ICT, nonché beni e servizi critici per l'operatività dell'Organizzazione; l'obiettivo è garantire che eventuali vulnerabilità o rallentamenti nella catena di fornitura non compromettano la disponibilità, l'integrità o la continuità dei sistemi e dei servizi dell'Organizzazione;
6. **sicurezza by Design e Privacy by Design**: le misure di sicurezza sono adattate fin dalle fasi iniziali di progettazione e sviluppo dei sistemi informativi e di rete, integrando le pratiche di sicurezza e privacy nei processi dell'Organizzazione;
7. **monitoraggio continuo e gestione delle anomalie**: sono implementati sistemi di monitoraggio continuo per rilevare tempestivamente anomalie e potenziali attacchi, con la capacità di rispondere in modo rapido ed efficace;
8. **gestione degli incidenti:** vengono adottate procedure strutturate per l'identificazione, la gestione e la segnalazione degli incidenti di sicurezza, assicurando una risposta tempestiva ed efficace.

Conformità Pragmatica

L'Organizzazione adotta un approccio pragmatico alla conformità, con l'obiettivo di integrare i requisiti normativi in maniera che supportino gli obiettivi costituitivi dell'Organizzazione. Ciò implica:

1. **valutazione continua**: monitoraggio costante delle normative in materia di protezione dei dati e cybersicurezza per assicurare che le procedure e le prassi in essere siano sempre aggiornate e conformi;
2. **integrazione tecnologica**: utilizzo di strumenti e tecnologie avanzate per semplificare la conformità; questo include non solo sistemi automatizzati per la gestione degli adempimenti tra cui il tracciamento e gestione delle richieste degli interessati tenuta dei registri e della documentazione in genere, soluzioni per la gestione delle vulnerabilità, il monitoraggio della sicurezza dei sistemi informativi e il supporto alla reportistica verso le autorità competenti.

L'Organizzazione a tal scopo adotta un Sistema di gestione integrato relativo alla protezione dei dati e alla sicurezza delle informazioni e resilienza dei sistemi volto a delineare le modalità per mantenere l'effettiva conformità normativa in materia di protezione dei dati personali e sicurezza delle informazioni.

Minimizzazione dei Dati ed Efficienza

La raccolta di dati personali deve essere limitata a ciò che è strettamente necessario per i fini legittimi. Questo include:

1. analisi della necessarietà dei dati: prima della raccolta di dati, deve essere effettuata un'analisi per determinare la necessità e la pertinenza dei dati rispetto agli scopi individuati;
2. pulizia dei dati: periodicamente, i dati non più necessari per scopi legittimi vengono eliminati o anonimizzati.

Trasparenza e Comunicazione Chiara

L'Organizzazione si impegna a comunicare in modo chiaro e trasparente le pratiche relative al trattamento dei dati. Ciò comprende:

1. informative: devono essere fornite informative sulla privacy che siano facilmente accessibili e comprensibili, anche in forma schematica, spiegando come e perché i dati personali sono raccolti e utilizzati;
2. comunicazione proattiva delle attività svolte: gli interessati devono essere informati in caso di modifiche significative nelle pratiche di trattamento dei dati o nelle politiche di privacy.

Diritti degli Interessati

L'Organizzazione riconosce e rispetta tutti i diritti degli interessati in conformità alle normative comunitarie e nazionali. Si adottano procedure semplificate per:

1. accesso ai Dati: consentire agli interessati di accedere facilmente ai propri dati personali;
2. rettifica e cancellazione: fornire meccanismi semplici per la rettifica o la cancellazione dei dati personali;
3. opposizione al trattamento: consentire agli interessati di opporsi al trattamento dei loro dati quando ricorrano determinate circostanze.

Gestione dei Dati e Processi dell'Organizzazione

L'integrazione efficace della protezione dei dati nei processi dell'Organizzazione è fondamentale. Ciò include:

1. valutazione del rischio: condurre valutazioni del rischio regolari per identificare e mitigare i potenziali rischi associati al trattamento dei dati;
2. procedure flessibili: sviluppare politiche che permettano adeguamenti in base alle mutevoli esigenze dell'Organizzazione e normative.

Sicurezza dei Dati, dei sistemi informativi e delle reti

Misure di Sicurezza

Per proteggere i dati personali da accessi non autorizzati, alterazioni, divulgazioni o eliminazioni, e per la gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete, l'Organizzazione, implementa misure di sicurezza adeguate, che includono:

1. protezioni tecniche: adozione di soluzioni fisiche e tecnologiche come, la chiusura degli armadi, la crittografia, il controllo degli accessi fisici e logici per proteggere le reti dell'Organizzazione da accessi non autorizzati, danni o interruzioni, la classificazione e la gestione sicura degli asset, il tutto assicurando che tali misure siano efficaci ma non ostacolino le attività operative quotidiane. Sono approvati e censiti account nominativi individuali nel rispetto del principio *need to know*, con controlli degli accessi basati sui ruoli. Sono inoltre implementati strumenti per il rilevamento e la risposta agli incidenti, la protezione da software malevoli, la gestione delle patch e dei cambiamenti nonché i test per la valutazione delle vulnerabilità e della capacità di difesa. L'Organizzazione adotta misure per la continuità operativa, tra cui piani di gestione delle crisi e dei disastri e politiche di backup e ripristino dei dati;
2. procedure organizzative: definizione di procedure chiare per la gestione dei dati e la sicurezza dei sistemi informativi e delle reti, compresi i protocolli per la condivisione dei dati all'interno e all'esterno dell'Organizzazione, la classificazione dei dati e la gestione dei ruoli e dei privilegi;
3. manutenzione e dismissione: l'Organizzazione si impegna alla regolare manutenzione per la sicurezza dei sistemi informativi e di rete al fine di massimizzare la disponibilità e l'integrità dei servizi IT. Alla fine del ciclo di vita, la dismissione dei sistemi informativi e di rete avviene secondo procedure sicure, in modo da prevenire ogni rischio di accesso non autorizzato;
4. protezione delle comunicazioni e relazioni con terze parti: la protezione del trasferimento delle informazioni è gestita attraverso misure tecniche e organizzative adeguate, al fine di mantenere la riservatezza e integrità e tramite la formalizzazione di accordi che includano requisiti per la sicurezza delle comunicazioni e la gestione del rischio legato ai fornitori.

Gestione Proattiva delle Violazioni e degli Incidenti

In caso di violazione dei dati personali o di incidenti di sicurezza, l'Organizzazione segue una procedura ben definita:

1. rilevamento e risposta rapida: identificazione e risposta tempestiva alle violazioni per minimizzare l'impatto;
2. notifica di violazioni: comunicazione delle violazioni alle autorità di controllo e agli interessati, come richiesto dalla legge;
3. notifica degli incidenti: comunicazione tempestiva degli incidenti di sicurezza informatica alle autorità di controllo, come richiesto dalla legge;

4. revisione e prevenzione: analisi delle cause delle violazioni o degli incidenti e implementazione di misure tecniche e/o organizzative atte a prevenire incidenti futuri o a limitare i danni causati dagli stessi;
5. miglioramento continuo e gestione dei *near miss*: implementazione di un processo strutturato per l'identificazione, la registrazione e l'analisi delle violazioni, degli incidenti e dei *near miss*, finalizzato all'individuazione proattiva delle vulnerabilità e all'adozione di azioni correttive e migliorative per rafforzare continuamente il sistema di gestione della sicurezza e della protezione dei dati anche personali.

Trasferimenti Internazionali

Il trasferimento internazionale di dati personali è gestito con attenzione per garantire la conformità con le leggi pertinenti contemperando la preferenza per fornitori e tecnologie UE alla scelta di tecnologie e soluzioni eventualmente disponibili extra-UE. In ogni caso verranno valutate preferenzialmente:

1. clausole contrattuali: utilizzo di clausole contrattuali standard e altre misure legali per garantire la protezione dei dati quando vengono trasferiti al di fuori dell'Unione Europea;
2. valutazioni di adeguatezza: valutazione delle leggi sulla protezione dei dati nei paesi destinatari per assicurare un livello adeguato di protezione;
3. valutazione del rischio ICT: nei casi di trasferimento o affidamento a soggetti extra-UE di servizi ICT critici (es. cloud, gestione dati, infrastrutture), è prevista una valutazione dei rischi per la sicurezza dei sistemi e delle reti.

Formazione e Consapevolezza

Per garantire che tutti i collaboratori comprendano l'importanza della protezione dei dati e sappiano come trattare i dati personali in modo sicuro, l'Organizzazione offre:

1. programmi di formazione regolari: formazione continua su temi quali la sicurezza dei dati, le migliori pratiche di protezione dei dati, la sicurezza informatica, la gestione degli incidenti e le pratiche di igiene informatica;
2. materiale formativo: disponibilità di risorse formative, come manuali e guide online, per supportare la comprensione e l'attuazione delle politiche in materia di protezione dei dati e sicurezza dei sistemi informativi e delle reti;
3. formazione dedicata alla direzione: la direzione e i responsabili di funzione ricevono una formazione mirata e differenziata, focalizzata sugli aspetti strategici e decisionali della gestione della sicurezza informatica e della protezione dei dati.

Monitoraggio, Valutazione, Aggiornamento e Miglioramento

Per assicurare che le politiche e le pratiche rimangano efficaci e pertinenti, l'Organizzazione si impegna a:

1. audit, valutazioni e monitoraggio: condurre audit interni e valutazione dei rischi, sia in ambito privacy che cybersicurezza, per monitorare la conformità normativa e l'efficacia delle pratiche di protezione dei dati e dei sistemi informativi e di rete. L'Organizzazione attua un processo continuo di monitoraggio e analisi degli eventi per rilevare minacce e gestire tempestivamente gli incidenti;
2. aggiornamenti continui: aggiornare le politiche e le procedure per riflettere i cambiamenti normativi, tecnologici, organizzativi e di contesto in modo da garantire che la protezione dei dati e dei sistemi informativi e di rete rimanga effettiva. In particolare, le politiche rilevanti sono riesaminate e, se opportuno, aggiornate, almeno annualmente, o comunque qualora si verifichino incidenti significativi, evoluzioni normative, variazioni organizzative o mutamenti

nell’esposizione alle minacce e ai relativi rischi. Gli esiti del riesame della politica sono documentati in un registro aggiornato;

3. miglioramento continuo: promuovere un ciclo virtuoso di miglioramento continuo, basato sull’analisi dei risultati degli audit, sul monitoraggio delle prestazioni, sul recepimento di segnalazioni o incidenti, e sull’evoluzione delle minacce. Questo approccio consente di affinare costantemente le misure di sicurezza, incrementare la consapevolezza del personale e rafforzare la resilienza complessiva dell’Organizzazione.

Padova, 12/09/2025

Nooo Agency S.r.l.