

Descrizione	Documento interno valido per la verifica della conformità al Regolamento Europeo sulla Protezione dei Dati Personali 679 del 2016
Dati del Titolare	ILE - Ispettoria Salesiana Lombardo Emiliana via Niccolò Copernico, 9 20125 Milano C.F. 80034550154
Luogo e data revisione	Milano, 07/07/2021
Sede riferimento	Istituto Salesiano Salesiano Don Bosco – Varese
Approvazione	Titolare del trattamento
Principali modifiche dalla revisione precedente	Aggiornamento periodico
Referente privacy	Direttore di Ente

Finalità del presente documento

Il presente documento è stato predisposto come **manuale operativo interno** per la gestione delle attività sulla tutela dei dati personali ai fini della conformità al Regolamento 679 del 2016 (GDPR).

Il presente documento è per esclusivo **uso interno e di proprietà** dell'Ente.

Conservazione

Il presente documento, è conservato a cura del Titolare del trattamento, presso la sede del Titolare

Approvazione del documento

Titolare del trattamento

Il legale rappresentante	Firma
Don Ennio Ronchi	

Di seguito sono elencate le figure che hanno un ruolo nella gestione dei dati personali a tutela della “privacy”.

Titolare del trattamento	ILE - Ispettorica Salesiana Lombardo Emiliana via Niccolò Copernico, 9 20125 Milano C.F. 80034550154
Legale rappresentante:	Don Ennio Ronchi
Referente privacy	Direttore di Ente
DPO	Ecoconsult Srl Dott. Bollani Via Goldoni 1 Milano dpo@ecoconsult.it

Descrizione generale dell'attività svolta dall'Ente

Convitto per scuole superiori

Residenza universitaria femminile

Definizioni in riferimento ai diversi soggetti coinvolti nella gestione della privacy

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Referente Privacy: è il direttore di sede e ha il compito di coadiuvare il Titolare del trattamento riguardo ai necessari adempimenti derivanti dalla normativa in materia di privacy. Presidia costantemente i processi applicativi della normativa all'interno della propria sede.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

DPO o Responsabile della protezione dei dati personali: è un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Cooperava con l'Autorità e

costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

Autorizzato al trattamento: persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Interessato: il soggetto dei cui dati è oggetto il trattamento. Si tenga presente che ai sensi del Regolamento 679/16 la figura dell'incaricato al trattamento dei dati non è disciplinata in modo autonomo ma con il generico riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Processi gestionali e documenti collegati

Processi gestionali	Documenti collegati
1. Analisi dei rischi e loro gestione	• Registro dei trattamenti – per il titolare e/o per il responsabile
2. Compilazione del registro dei trattamenti	• Registro dei trattamenti – per il titolare e/o per il responsabile
3. Gestione delle informative	• Informative • Registro delle informative
4. Gestione del consenso specifico	• Informative con consenso come da punto sopra • Liberatoria al diritto di immagine • Modulo per la revoca del consenso
5. Gestione del diritto di accesso e di eventuale aggiornamento dell'interessato	• Modulo di richiesta di accesso ai dati • Modulo di comunicazione dei dati dell'interessato
6. Utilizzo della strumentazione informatica	• Modulo regolamento informatico
7. Incarico al trattamento e formazione del personale	• Lettera di incarico al trattamento dei dati personali comuni • Lettera di incarico al trattamento dei dati personali sensibili. • Registro della formazione sulla gestione dei dati in ottemperanza al GDPR e s.m.i.
8. Gestione dei responsabili esterni	• Autocertificazione per la qualifica dei Responsabili esterni • Lettera di nomina dei responsabili del trattamento esterni • Elenco responsabili esterni • Lettera di nomina del DPO
9. Gestione degli incidenti e di notifica violazione dati	• Registro degli incidenti • Notifica violazione dati

Processi gestionali	Documenti collegati
10. Controllo interno (Audit)	• Piano Audit • Registro Audit • Check list Audit
11. Trasferimento dati all'estero	• Clausole contrattuali standard da titolare a titolare • Clausole contrattuali standard da titolare a responsabile
12. Videosorveglianza	• NominaResponsabileVideosorveglianza • NominaRappresentanteLavoratoriVideosorveglianza • NominaManutentoreImpiantoVideosorveglianza • InformativaVideosorveglianza • InformativaDipendente • Elenco Sedi

Tutti i documenti citati sopra riportano il numero di revisione e sono preventivamente approvati dal direttore di ente (Referente privacy di ente). Tutta la documentazione aggiornata è resa disponibile sul server di ente o può essere richiesta al referente. È compito del referente privacy tenerla sempre aggiornata e renderla disponibile.

1. Analisi dei rischi e loro gestione

Lo scopo di questa sezione è quello di stabilire il metodo per la valutazione dei rischi in riferimento alla gestione dei dati personali e per la loro successiva gestione.

Attraverso la valutazione dei rischi viene anche definito il rischio accettabile per soddisfare le richieste indicate nel Regolamento europeo numero 679 del 2016 sulla protezione dei dati personali. Tale procedura è applicata dal Titolare del trattamento e dai Referenti Privacy, che prendono parte al processo di valutazione del rischio e al relativo trattamento.

Riferimenti normativi

- Regolamento UE 679/2016

Processo di valutazione del rischio ed eventuali interventi per abbassare il rischio

Il processo di valutazione del rischio è effettuato dal titolare, coordinato dai Referenti Privacy, che devono identificare e valutare i fattori di rischio nelle attività di gestione dei dati personali da parte dell'Ente in relazione ai diritti dei soggetti interessati e riguardanti i seguenti aspetti della sicurezza: DISPONIBILITÀ, INTEGRITÀ e RISERVATEZZA.

Il *primo passo* per la valutazione del rischio consiste nell'identificare, attraverso il registro dei trattamenti, tutti i dati, le modalità di registrazione e le risorse che li gestiscono.

- Il *secondo passo* consiste nell'individuare i rischi associati al rischio stesso e all'accadimento dell'evento dannoso e alla conseguente gravità dell'accadimento stesso.

Il *secondo passo* consiste nell'individuare i rischi associati a ciascun dato in base alla probabilità di accadimento e alla conseguente gravità, usando i criteri indicati nelle successive 2 tabelle:

Tabella di probabilità di accadimento

Bassa	1	I controlli di sicurezza esistenti sono sufficienti e hanno finora fornito un adeguato livello di protezione. Non ci sono nuovi incidenti attesi in futuro o comunque la loro probabilità di accadimento è stimata < al 5%
Media	2	I controlli di sicurezza esistenti sono moderati e hanno per lo più fornito un adeguato livello di protezione. Nuovi incidenti sono possibili, ma non sono molto probabili (probabilità di accadimento stimata tra il 5 e il 20%)
Alta	3	I controlli di sicurezza esistenti sono moderati, ma non particolarmente efficienti. Questi incidenti hanno una discreta probabilità di verificarsi in futuro (probabilità di accadimento stimata tra il 20 e il 50%).
Molto Alta	4	I controlli di sicurezza esistenti sono scarsi o inefficaci. Questi incidenti hanno un'alta probabilità di verificarsi in futuro (probabilità di accadimento stimata > 50%)

Tabella di conseguenza o gravità di accadimento

Bassa	1	La perdita di riservatezza, disponibilità e integrità non hanno alcuna influenza sugli interessati
Media	2	La perdita di riservatezza, disponibilità e integrità determina per gli interessati piccoli inconvenienti che supereranno facilmente (es: perdita di tempo, fastidio ...)
Alta	3	La perdita di riservatezza, disponibilità e integrità comporta per gli interessati la possibilità di incontrare significativi disagi, superabili nonostante alcune difficoltà (es. mancanza di comprensione, stress, costi aggiuntivi ...)
Molto Alta	4	La perdita di riservatezza, disponibilità e integrità può avere conseguenze significative, addirittura irreversibili per gli interessati (es: perdita del lavoro, disturbi psicologici a lungo termine ...)

Il *passo successivo* consiste nel valutare il rischio secondo il seguente modello:

1. **Indice di rischio $R = P \times G$** , dove: P misura la probabilità che si verifichi l'evento rischioso e può assumere i seguenti valori: 1 = bassa; 2= media; 3= alta; 4 = molto alta; G misura la gravità delle conseguenze sugli obiettivi al verificarsi del rischio e utilizza la stessa scale delle probabilità.
2. Intervalli per la **valutazione del rischio $R = P \times G$** : $8 < R \leq 16$ (non accettabile); $1 < R \leq 8$ (accettabile)

Indicazioni d'intervento

Con rischio accettabile, ci si può accontentare di tenere sotto controllo il rischio con il monitoraggio, oppure se fattibile, applicare il miglioramento, seguito da monitoraggio; con rischio non accettabile, è necessario intervenire indicando per ogni rischio la corrispondente azione di trattamento finalizzata ad abbassare il rischio stesso; in seguito, occorre monitorare costantemente i risultati.

Verifiche regolari della valutazione del rischio e del suo trattamento

I Referenti Privacy devono rivedere i rischi esistenti e aggiornare la tabella di valutazione dei rischi. La revisione è effettuata almeno una volta l'anno, o più frequentemente, per esempio nel caso di variazioni significative sulla struttura organizzativa, di cambiamenti significativi nella tecnologia, di cambiamento sostanziali delle attività svolte.

Documenti collegati

- Registro dei trattamenti per il titolare e/o per il responsabile, con associata valutazione dei rischi.

2. Compilazione del Registro dei trattamenti

Questo capitolo costituisce una guida per individuare e aggiornare costantemente le attività di trattamento dei dati personali.

I destinatari di tali indicazioni sono i Referenti Privacy e gli incaricati del trattamento.

Riferimenti normativi

- Articolo 30 del GDPR 2016/679 (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla tutela delle persone fisiche in materia di trattamento dei dati personali e che abroga la direttiva 95/46 / CE);
- Leggi nazionali e disposizioni rilevanti per l'implementazione del Regolamento.

Scopo del registro delle attività di trattamento

Al fine di avere un approccio comune verso la responsabilità e l'osservanza delle disposizioni del GDPR e per consentire all'Ente di avere una visione chiara delle sue attività di trattamento, verrà utilizzato un apposito documento: il Registro dei trattamenti.

Il registro dei trattamenti, consente di capire come e perché i dati personali devono essere trattati. È altresì funzionale alla valutazione dei rischi in relazione ai diritti dei soggetti interessati e allo sviluppo di politiche e procedure volte a proteggere i dati in modo adeguato.

È uno strumento centrale per la gestione della privacy ed anche per l'evidenza di adeguatezza verso eventuali verifiche da parte dell'autorità di controllo.

Il Referenti Privacy hanno il compito e la responsabilità di mantenere aggiornato il registro delle attività di trattamento per le rispettivi sedi di competenza.

La tipologia di registro dipenderà dal ruolo che l'Ente ricopre, titolare o responsabile del trattamento. Se agisce sia come titolare sia come responsabile (per diverse attività di trattamento) dovrà predisporre due inventari differenti (uno come titolare del trattamento e uno come responsabile del trattamento).

Agire in qualità di titolare del trattamento

Al fine di assicurare la conformità ai requisiti del GDPR nel registro delle attività di trattamento devono essere incluse le seguenti informazioni:

- Nome e dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati (DPO).
- Finalità delle attività di trattamento.
- Descrizione delle categorie di interessati e delle categorie di dati personali
- I destinatari a cui sono stati o saranno comunicati i dati personali, compresi i destinatari in paesi terzi
- Trasferimenti dei dati personali verso un paese terzo, inclusa l'identificazione di tali paesi.
- I termini proposti per la cancellazione delle diverse categorie di dati
- Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative
- Uffici dove avvengono le attività di trattamento
- Nome del sistema (inteso come software, servizio o archivio) che elabora i dati
- La valutazione dei rischi legati al trattamento del dato
- Se il Titolare tratta dati insieme ad altre realtà, specificare il nome di queste ultime (definizione del contitolare).

Agire in qualità di responsabile del trattamento

Nei casi in cui si agisce in qualità di responsabile del trattamento, si deve predisporre un registro delle attività di trattamento per tutte le categorie delle attività di trattamento svolte per conto del titolare, contenente almeno le seguenti informazioni:

- Nome e contatti del responsabile o dei responsabili e di ogni titolare in nome del quale il responsabile sta operando e, dove applicabile, del rappresentante del titolare o del responsabile del trattamento e del Data Protection Officer
- Le categorie di trattamento trattate per conto di ogni titolare
- Ove applicabile, trasferimenti dei dati personali ad una terza parte (sub-responsabile).
- La valutazione dei rischi legati al trattamento del dato
- Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Compilare e conservare il registro delle attività di trattamento

Alla compilazione dell'inventario delle attività di trattamento contribuiscono gli incaricati.

Gli incaricati riportano regolarmente ai rispettivi Referenti Privacy qualsiasi aggiunta, eliminazione o modifica nei dati esistenti o nel loro trattamento.

I Referenti Privacy devono assicurarsi che i tutti i trattamenti dei dati siano costantemente aggiornati.

I Referenti Privacy agiranno come punto di riferimento qualora gli incaricati abbiano difficoltà ad individuare i dati personali necessari alla propria attività.

Documenti collegati

- Registro dei trattamenti – per il titolare e/o per il responsabile

3. -Gestione delle informative

Quando i dati riguardanti altri individui sono raccolti e utilizzati non per uso strettamente personale ma per altre finalità, il trattamento dei dati personali deve rispettare alcune regole, in particolare l'obbligo di informazione dell'interessato.

Modalità operative e responsabilità

Per ogni attività di trattamento che comporti la raccolta di dati di soggetti terzi, siano essi dipendenti, clienti, utenti o fornitori si devono individuare:

- I destinatari dell'informativa
- Tipo di informative (con o senza consenso)
- Il n. di revisione
- Le tempistiche di consegna dell'informativa
- Il luogo di conservazione dei dati
- Il tempo di conservazione dei dati

Tali informazioni e l'elenco dettagliato delle informative predisposte sono documentate sul registro delle informative.

Tutte le informative devono essere scritte in un linguaggio semplice e comprensibile da chiunque.

Documenti collegati

- Registro delle informative aggiornato
- Informative

4. Gestione del consenso specifico

Raccolta e conservazione del consenso

Il consenso dell'interessato alle attività di trattamento dei dati personali è indispensabile al fine di legittimare le attività di trattamento dei dati da parte del titolare del trattamento dei dati.

Modalità operative e responsabilità

Il titolare del trattamento deve mappare tutte le attività di raccolta dei dati, identificando quelle che vanno oltre la finalità diretta e richiedono un consenso specifico, come le attività promozionali, di direct marketing o di invio di newsletter.

Per ogni attività individuata è necessario chiarire le modalità di gestione del consenso specifico. La raccolta del consenso (e la conseguente possibilità di revoca dello stesso), deve essere gestita attraverso appositi form e le richieste di consenso devono essere scritte in un linguaggio semplice e comprensibile da chiunque.

Revoca del consenso

L'interessato al trattamento dei dati ha il diritto di revocare il proprio consenso al trattamento con la stessa facilità con cui lo ha accordato. Per tale motivo le modalità di revoca devono essere di facile accesso. Tale attività può avvenire da parte di un dipendente, di un cliente o utente che esercita i propri diritti ed è permesso anche mediante una richiesta via mail. Non tutti i dati possono tuttavia essere revocati.

Modalità operative e responsabilità

Per facilitare l'interessato ad esprimere la revoca del proprio consenso al trattamento dei dati il Titolare mette a disposizione un apposito modulo disponibile presso la segreteria.

Entro 30 giorni i dati personali dell'interessato che ha espresso la revoca del consenso devono essere cancellati dal sistema.

I moduli di revoca o le mail di richiesta di revoca devono essere conservati in apposito raccoglitore e/o spazio dedicato del server.

Documenti collegati

- Informative degli interessati con consenso come da precedente punto 3 di questo manuale
- Modulo per la revoca del consenso

5. Gestione del diritto di accesso e di eventuale aggiornamento dell'interessato

L'interessato al trattamento dei dati ha il diritto di accedere alle informazioni che lo riguardano. Per tale motivo è importante stabilire le modalità di gestione di tali richieste.

Modalità operative e responsabilità

Se si agisce in qualità di titolare del trattamento nei confronti del soggetto interessato che effettua la richiesta, allora questa si baserà sulle disposizioni della presente procedura; se si agisce in qualità di responsabile del trattamento, il referente privacy inoltrerà la richiesta al titolare del trattamento in nome del quale la società tratta i dati personali del soggetto interessato che ha effettuato la richiesta.

La richiesta di accesso dati dell'interessato dà diritto agli interessati di visionare o richiedere copia dei propri dati personali. Le possibili richieste di accesso ai dati possono arrivare da ogni interessato.

Una richiesta di accesso dati dell'interessato può essere effettuata con le seguenti modalità: e-mail o comunicazione postale.

Solitamente, le richieste verbali in merito alle informazioni dell'interessato non sono ritenute valide.

La gestione delle richieste di accesso ai dati prevede diverse fasi:

1. Ricezione della richiesta: alla ricezione di una richiesta di accesso ai dati, il referente privacy darà conferma di quanto ricevuto.
2. Verifica dell'identità: il referente privacy deve verificare l'identità di coloro che effettuano le richieste di accesso ai dati per assicurarsi che le informazioni vengano fornite solo a chi ha

diritto di riceverle. Se il richiedente non è l'interessato, è richiesta un'autorizzazione scritta della persona che l'ha delegata.

3. Comunicazione al richiedente: se le informazioni presentate dalla persona che ha ricevuto la richiesta sono sufficienti, il referente privacy comunicherà al richiedente che la sua domanda riceverà riscontro entro 30 giorni dalla data in cui i documenti richiesti sono stati ricevuti. Il richiedente sarà informato a mezzo scritto nel caso in cui ci fossero ritardi a causa di altri eventi intersorsi.
4. Revisione delle informazioni: il referente privacy contatterà e richiederà all'ufficio interessato le informazioni così come domandato nella richiesta di accesso dati dell'interessato. L'ufficio deve comunicare le informazioni rispettando la scadenza fissata dal referente privacy, che provvede a la revisione delle informazioni. Il referente privacy stabilirà se ci sono informazioni soggette a deroga o se è richiesto il consenso da parte di terzi. Il referente privacy deve assicurarsi che le informazioni vengano esaminate in modo tale da poter rispettare la scadenza dei 30 giorni e richiederà all'ufficio coinvolto di compilare un modulo di divulgazione dei dati dell'interessato per documentare la conformità al requisito della scadenza.
5. Risposta alle richieste di accesso: il referente privacy fornirà per iscritto all'interessato la risposta definitiva insieme - a seconda dei casi - alle informazioni recuperate dagli uffici o una dichiarazione attestante che l'Ente non detiene le informazioni richieste o che si applica una deroga. Il referente privacy si assicura che venga inviata al richiedente una risposta scritta. Questa può essere data via e-mail, a meno che il richiedente non abbia specificato un'altra preferenza per la modalità di risposta (ad esempio via posta). L'Ente fornirà informazioni solo tramite canali sicuri.
6. Archiviazione: dopo che la risposta è stata inviata al richiedente, la richiesta di accesso ai dati è considerata soddisfatta ed archiviata.

Documenti collegati

- Richiesta di accesso ai dati
- Comunicazione dei dati dell'interessato

6. Utilizzo della strumentazione informatica

La progressiva diffusione di nuove tecnologie informatiche espone ad ulteriori rischi nel trattamento dei dati personali con ricadute negative sia per il proprietario dei dati sia per l'Ente.

Pertanto, l'Ente ha provveduto, con riferimento alle misure di sicurezza imposte per il trattamento dei dati personali dal Regolamento europeo n. 679/2016, a dare idonee indicazioni e istruzioni a tutto il personale interessato dalle predette misure. Inoltre, tutto il personale interessato dovrà attenersi a quanto indicato nel Regolamento informatico consegnato ed eventualmente disponibile a richiesta dell'interessato.

7. Incarico al trattamento e formazione del personale

Per garantire un livello di protezione adeguato dei dati, il personale che ha accesso permanente o regolare agli stessi deve essere formalmente incaricato del trattamento e ricevere appropriate istruzioni e formazione.

Modalità operative e responsabilità

Tutto il personale che ha accesso permanente o regolare ai dati deve ricevere adeguata formazione e informazione sui requisiti del Regolamento e sulle procedure implementate per garantire la conformità a tale normativa ed assicurare agli interessati il corretto trattamento dei loro dati e il rispetto dei loro diritti e libertà fondamentali.

La formazione viene svolta anche mediante una lettera di responsabilizzazione e di incarico al trattamento.

La formazione può essere svolta nella modalità giudicata più appropriata alle proprie esigenze. Tale attività deve essere registrata nell'apposito registro allegato alla procedura.

Documenti collegati

- Lettera di individuazione dei soggetti incaricati al trattamento dei dati personali comuni
- Lettera di individuazione dei soggetti incaricati al trattamento dei dati personali sensibili.
- Registro della formazione sulla gestione dei dati in ottemperanza al GDPR e s.m.i

8. Gestione dei Responsabili esterni

Definizione di Responsabile esterno del trattamento

Per Responsabile esterno del trattamento dati si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Modalità operative e responsabilità

Il Titolare del trattamento tiene aggiornata la mappa dei soggetti incaricati al fine di individuare con immediatezza e semplicità quali attività di trattamento sono state affidate in outsourcing.

Per ogni soggetto a cui viene affidato l'incarico di Responsabile esterno del trattamento dei dati deve essere dimostrata la conformità ai requisiti del GDPR, conformità che deve essere verificata dal titolare o dal Referente Privacy appositamente nominato tramite sottoscrizione da parte del fornitore dell'autocertificazione predisposta dall'Ente o attraverso altro documento sostitutivo predisposto dallo stesso fornitore.

L'incarico di Responsabile esterno deve essere affidato tramite specifico accordo tra le parti, mediante la lettera di nomina ai responsabili esterni del trattamento, che, una volta sottoscritta, deve essere archiviata e conservata a cura del Referente Privacy.

Tutti i soggetti che ricoprono il ruolo di Responsabili esterni devono essere inseriti in uno specifico elenco, che è compilato e aggiornato dal Referente Privacy

Nel caso in cui l'ufficio incaricato della gestione dei fornitori identifica un soggetto come fornitore di una attività che comporta il trattamento di dati personali, provvede ad informare il titolare o il Referente Privacy della necessità di procedere alla qualifica del fornitore come Responsabile esterno del trattamento per il suo successivo inserimento nell'elenco dei responsabili esterni.

Nel caso in cui sia obbligatoria la nomina del Responsabile per la Protezione dei Dati (D.P.O.), il Titolare consegna al soggetto individuato la lettera di nomina del Responsabile della Protezione e ne ottiene copia firmata per accettazione.

Documenti collegati

- Autocerificazione per la qualifica dei Responsabili esterni
 - Lettera di nomina dei responsabili del trattamento esterni
 - Elenco responsabili esterni
 - Lettera di nomina del DPO
-

9. Gestione degli incidenti e di notifica violazioni dati

Questo capitolo fornisce le indicazioni volte alla gestione degli incidenti di sicurezza che determinano una "violazione di dati personali" intendendosi con quest'ultima: *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"*.

Dal momento in cui il titolare viene a conoscenza del verificarsi di un "incidente di sicurezza dei dati" deve valutare, se tale incidente possa portare ad una violazione di dati personali.

Se l'incidente è avvenuto a causa di qualsiasi azione od omissione del responsabile del trattamento, quest'ultimo deve determinare se ci si trova davanti ad una violazione di dati personali o meno. In caso positivo il responsabile del trattamento è tenuto ad informare di tale violazione il titolare del trattamento, senza ingiustificato ritardo. Il titolare del trattamento si considererà venuto a conoscenza della violazione dal momento di tale notifica da parte del responsabile.

Se da tale valutazione ed anche da un'eventuale veloce indagine emerge con ragionevole certezza che tale incidente ha determinato una violazione di dati personali, il titolare del trattamento deve capire se tale violazione possa portare alla presenza di rischi per i diritti e le libertà delle persone fisiche.

Se dalla valutazione del caso concreto emerge che la violazione non determina rischi per i diritti e le libertà delle persone fisiche, il titolare non deve effettuare nessuna notifica all'autorità di controllo o alle persone fisiche.

Si ritiene particolarmente utile segnalare che in tutti i casi di violazione dei dati, e quindi anche quando non scatta l'obbligo di notifica, il titolare è tenuto a documentare la violazione sul registro delle violazioni.

Nel caso in cui emerga che la violazione abbia determinato rischi per i diritti e le libertà delle persone fisiche il titolare deve effettuare, entro 72 ore dal momento in cui ne è venuto a conoscenza, la notifica all'autorità di controllo competente (Garante della Privacy).

In tale notifica devono essere indicati i seguenti elementi:

- Descrizione della natura della violazione
- Nome e dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni.
- Descrizione delle probabili conseguenze della violazione dei dati personali.
- Descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

Inoltre, se la violazione presenta un *rischio elevato* per i diritti e le libertà delle persone fisiche il titolare del trattamento comunica le violazioni anche all'interessato senza ingiustificato ritardo. Per stabilire la presenza di un rischio elevato, si deve valutare oggettivamente la probabilità e la gravità del rischio per i diritti e le libertà delle persone fisiche nel caso concreto che si è verificato.

Attraverso tale notifica agli interessati devono essere fornite le seguenti informazioni:

- Natura della violazione.
- Nome e dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni.
- Descrizione delle probabili conseguenze della violazione dei dati personali.
- Descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

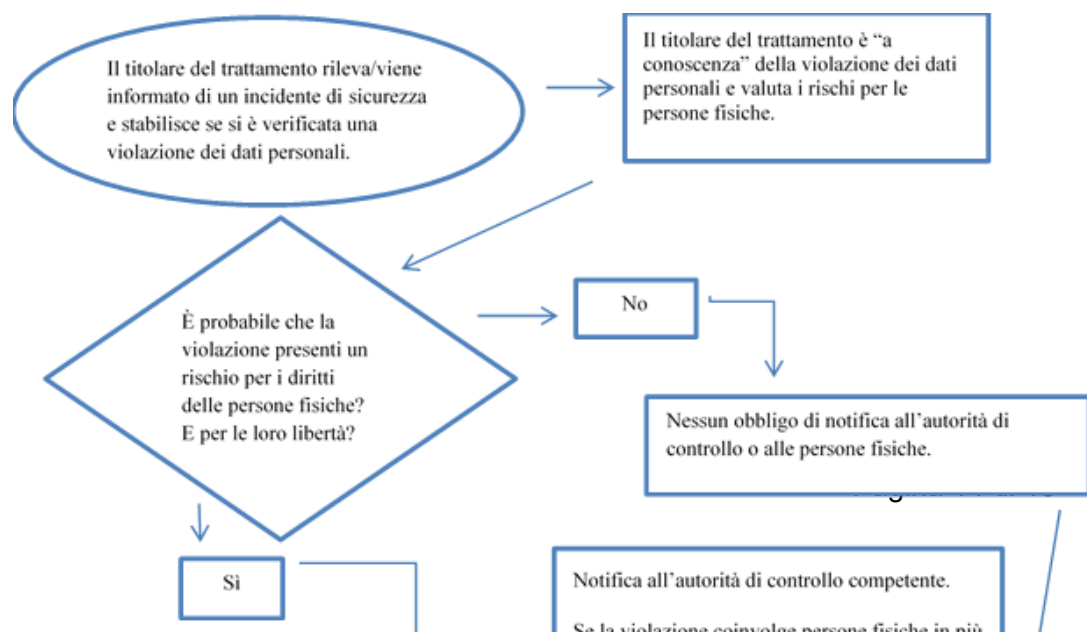
Tale notifica dovrebbe essere fatta adottando uno spirito collaborativo con l'autorità di controllo che potrebbe anche impartire indicazioni in merito alle modalità con cui effettuare tale notifica.

La notifica agli interessati deve essere effettuata attraverso messaggi dedicati, ossia non insieme ad altre informazioni (come aggiornamenti regolari inviati agli interessati o newsletter, altro).

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

- 1) Il titolare del trattamento ha messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi quali la cifratura.
- 2) Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.
- 3) Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o misura simile tramite la quale gli interessati sono informati con analoga efficacia.

Il diagramma di flusso riportato nella pagina seguente ed elaborato dal Garante per la protezione dei dati personali, riporta schematicamente i passaggi sopra descritti (Fonte: Gruppo di lavoro articolo 29 per la protezione dei dati. "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679.").



Con la presente tabella si riportano alcuni esempi non esaustivi al fine di aiutare il titolare a prendere le decisioni migliori in tema di notifica all'autorità di controllo ed agli interessati.

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

Documenti collegati

- Registro degli incidenti
- Notifica violazione dati

10. Controllo interno (Audit)

Il controllo interno (audit) è uno strumento essenziale per verificare la correttezza e l'efficacia dei processi. Esso rappresenta inoltre uno strumento molto efficace per verificare se le attività di raccolta, gestione e controllo dei dati personali sono conformi alle normative vigenti (GDPR) e alla documentazione interna dell'organizzazione; rappresenta inoltre uno strumento efficace anche per individuare aree di miglioramento ed eventuali necessità di formazione interna.

L'obiettivo degli audit interni è quello di verificare se le procedure, i controlli, i processi e le modalità di elaborazione dei dati personali siano conformi alle normative vigenti e alla documentazione interna dell'Ente, ed effettivamente attuate e mantenute.

Piano di audit interni

Il numero di audit da condurre in un determinato periodo di tempo, deve essere tale da garantire una copertura totale di tutte le attività legate al trattamento dei dati personali. Gli audit interni sono pianificati in base alla valutazione dei rischi e ai risultati degli audit precedenti.

I referenti privacy definiscono il programma annuale di audit.

Conduzione di un singolo audit interno

Se un audit è condotto da un team composto da più persone, il responsabile dell'audit è colui identificato come Team Leader.

Gli aspetti che devono essere verificati e valutati durante l'audit interno sono i seguenti:

- Requisiti delle politiche, delle procedure di gestione dei dati personali dell'Ente
- Risultati dei precedenti audit interni
- Risultati dell'analisi dei rischi, dei controlli, della valutazione di impatto della protezione dei dati.
- Controlli applicabili mutuati dall'Allegato A della ISO 27001 elencati nella checklist degli audit interni

Come risultato degli audit interni devono essere documentati tutti i seguenti passaggi:

- L'auditor interno deve registrare tutte le evidenze nel report degli audit interni
- Se vengono riscontrate non conformità, l'auditor interno deve riportarle in forma scritta al Titolare del trattamento.

Documenti collegati

- MOD0101 – Piano di Audit
- MOD0102 – Report Audit Interno
- MOD0103 – Checklist Audit

11. Procedura di gestione del trasferimento dei dati ai paesi terzi

Il trasferimento dei dati all'estero può essere effettuato solo se vengono garantiti adeguati livelli di protezione dei dati e tutte le attività sono normate mediante accordi specifici.

Modalità operative e responsabilità

Il GDPR permette il trasferimento dei dati personali verso un paese terzo solo se sono soddisfatte determinate condizioni, in primis suddetto paese terzo deve essere in grado di garantire, secondo l'Unione Europea, un "adeguato" livello di protezione dei dati personali.

In assenza di una decisione di adeguatezza della Commissione europea, la Società dovrà trasferire i dati personali al di fuori degli Stati non appartenenti all'UE utilizzando clausole contrattuali standard.

Clausole contrattuali standard**Utilizzo dei modelli prescritti dall'UE**

La Commissione Europea ha definito delle clausole contrattuali standard che devono essere utilizzate quando si effettuano dei trasferimenti di dati personali al di fuori dell'UE/AEE.

Il contenuto di tali clausole non deve essere modificato a meno di un'espressa autorizzazione del Data Protection Officer o dell'Autorità di controllo competente. Ogni modifica non autorizzata renderà nullo il trasferimento transfrontaliero dei dati.

Le clausole contrattuali stabiliscono obblighi sia per l'esportatore che per l'importatore dei dati al fine di assicurare che il trasferimento protegga i diritti e le libertà degli interessati.

Il referente privacy ha il compito di monitorare il sito internet della Commissione europea (http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm) così come gli altri canali di comunicazione al fine di individuare tempestivamente ogni nuova versione delle clausole contrattuali standard ed aggiornare quelle utilizzate dalla Società.

Le clausole sono di due tipi:

- **Clausole contrattuali standard da titolare a titolare:** da utilizzare nei casi in cui la società agisce in qualità di titolare del trattamento e inoltra i dati ad un altro soggetto che si trova al di fuori dell'AEE che agisce anch'esso in qualità di titolare
- **Clausole contrattuali standard da titolare a responsabile:** da utilizzare nei casi in cui la società agisce in qualità di titolare del trattamento e inoltra i dati ad un altro soggetto che si trova al di fuori dell'AEE che agisce in qualità di responsabile.

Documenti collegati

- MOD0501 - Clausole contrattuali standard da titolare a titolare
- MOD0502 - Clausole contrattuali standard da titolare a responsabile

12. Procedura di gestione della videosorveglianza

La videosorveglianza è un sistema che implica la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini. Ciò configura un trattamento di dati personali pertanto deve essere gestito in maniera tale da tutelare i diritti e le libertà fondamentali degli interessati al trattamento dei dati personali.

Modalità operative e responsabilità

Per ogni sistema di videosorveglianza installato, è necessario verificare:

- Preventiva richiesta all'Ispettorato del Lavoro è il primo atto in caso di presenza di dipendenti
- Presenza degli appositi cartelli informativi
- Numero delle telecamere installate
- Posizionamento delle telecamere
- Numero dei monitor
- Numero delle apparecchiature di registrazione

Documenti collegati

- MOD0401_NominaResponsabileVideosorveglianza
- MOD0402_NominaRappresentanteLavoratoriVideosorveglianza
- MOD0403_NominaManutentoreImpiantoVideosorveglianza
- MOD0404_InformativaVideosorveglianza
- MOD0405_InformativaDipendente

- MOD 0406_Elenco Sedi