Procedura segnalazione Violazione dati personali

Data Breach

Titolare del trattamento dati: OMCeO di Como

Il presente documento si prefigge lo scopo di indicare ai consiglieri, dipendenti, fornitori e collaboratori dell'Ordine le opportune modalità di gestione dei data breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016.

In questo documento si illustra la procedura da seguire per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione dei data breach, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare per il tramite del referente privacy
- modalità e profili di segnalazione all'Autorità Garante
- valutazione dell'evento accaduto
- eventuale comunicazione agli interessati.

Al termine del presente documento sono presenti due sezioni (glossario e normativa di riferimento) al fine di agevolare l'utilizzo della procedura descritta.

INFORMAZIONI DOCUMENTO:

Titolo	Procedura segnalazione violazione dei dati personali		
Data di emissione	16/06/2025	**Versione**	1.0

Attività di segnalazione, raccolta informazioni, valutazione notifica della violazione

N°	Attività	Chi	A chi	Quando	Come
1	Rilevazione e segnalazione di data breach	Tutto il personale, collaboratori, fornitori, responsabili	Al referente privacy dell'Ordine o in sua assenza al responsabile dell'area.	Appena se ne viene a conoscenza.	Utilizzando le vie più brevi (telefono, di persona, e-mail)
2	Raccolta informazioni sulla violazione	Il referente privacy dell'Ordine assieme ai soggetti coinvolti nella violazione (il responsabile dell'area nel caso non possa essere immediatamente disponibile), deve dare istruzioni precise alla persona che l'ha contattato per iniziare subito la raccolta delle informazioni, indicando dove reperire il modello predisposto a tale scopo)		Appena ricevuta la comunicazione	Utilizzando il modello fornito e raccogliendo informazioni dai soggetti coinvolti nella segnalazione e nel trattamento dei dati violate
3	Comunicazione del data breach	Il referente privacy o il responsabile dell'Area (in mancanza di tali figure la stessa persona che ha rilevato la violazione)	Al Titolare e al RPD	Appena ottenute informazioni di base sulla violazione	Via e-mail
4	Valutazione d'impatto	Titolare, RPD, AdS, soggetti coinvolti		Appena ricevuta la comunicazione	Applicando la metodologia indicata
5	Individuazione delle azioni correttive	RPD, AdS, soggetti coinvolti		Appena terminata la valutazione d'impatto	Analizzando i risultati della valutazione d'impatto
6	Comunicazione delle valutazioni effettuate e delle	RPD, referente privacy, responsabile dell'area	Al Titolare		Tramite una breve relazione

	azioni da intraprendere				
7	Notifica della violazione (se è necessaria)	Titolare	Al Garante	Entro 48 ore dalla rilevazione	Mediante la modulistica predisposta dal Garante (vedi allegato)
8	Comunicazione agli interessati coinvolti (se è necessaria)	Titolare	Alle persone fisiche i cui dati sono stati violati	Nei termini indicati nella valutazione d'impatto	Comunicazione diretta alle singole persone o mediante pubblicazione in sito a loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate
9	Disposizioni per l'attuazione delle misure correttive (se individuate)	Responsabili delle Aree coinvolte, AdS	Ai soggetti incaricati di svolgere le attività	Nei termini indicati nella valutazione d'impatto	Devono essere indicate in dettaglio le operazioni da svolgere, chi è l'incaricato, i tempi di attuazione; prevedere eventuali operazioni di verifica dell'efficacia delle misure correttive
10	Recepimento della risposta del Garante alla notifica (se effettuata)	Titolare, RPD, responsabili delle aree coinvolte, AdS	Ai soggetti incaricati di svolgere le attività		Disposizioni per l'attuazione delle eventuali misure correttive indicate dal Garante; effettuazione di ulteriori indagini per approfondire le informazioni raccolte

Attività relative alla registrazione dell'incidente

N°	Attività	Chi	A chi	Quando	Come
1	Registrazione della violazione/aggiornamenti	RPD		Appena ricevuta la comunicazione	Compilando l'apposito registro con la descrizione della violazione, delle azioni intraprese e annotando i successivi aggiornamenti
2	Registrazione della risposta del Garante	RPD		Appena ricevuta la comunicazione	Annotando sul registro gli estremi della risposta del Garante e le eventuali prescrizioni in essa contenute
3	Registrazione della prosecuzione/chiusura dell'incidente	RPD		Stabilite le disposizioni per l'attuazione delle misure correttive e al termine delle stesse	Registra la chiusura dell'incidente se non necessita di ulteriori indagini o riporta le istruzioni per le ulteriori indagini

Attività inerenti alla prosecuzione delle indagini

Da eseguire nel caso sia necessario acquisire ulteriori informazioni

N°	Attività	Chi	A chi	Quando	Come
1	Prosecuzione delle indagini	RPD, referente privacy, responsabile dell'area coinvolto, soggetti coinvolti nella violazione e nei trattamenti di dati violati, AdS		A seguito di indicazione da parte del Garante o del titolare; se previsto nella prima valutazione d'impatto; nel caso che le informazioni raccolte risultino incomplete o mancanti	Raccogliendo le informazioni mancanti, o approfondendo quelle note per rilevare eventuali impatti non riscontrati nella prima indagine
2	Esecuzione di una nuova valutazione d'impatto	Titolare, RPD, referente privacy, responsabile area coinvolta, AdS, soggetti coinvolti		Al momento che si ritiene di aver raccolto tutte le informazioni possibili sulla violazione	
3	Comunicazione dei risultati del proseguimento delle indagini	RPD, referente privacy, responsabile dell'area coinvolta, AdS	Titolare	Appena terminato il lavoro	Tramite relazione sui risultati della valutazione d'impatto e sulle azioni necessarie, allegando il materiale informativo raccolto
4	Aggiornamento della notifica al Garante (se necessario)	Titolare	Garante	Appena sono disponibili i nuovi dati o secondo i termini stabiliti dal Garante	Mediante la modulistica predisposta o come indicato dal Garante
5	Comunicazioni agli interessati (se necessario)	Titolare	Interessati	Nei tempi stabiliti nella valutazione d'impatto	Contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati

GLOSSARIO E ACRONIMI

- **Archivio:** qualsiasi insieme strutturato di Dati Personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.
- **Aree Sensibili:** sono quei luoghi fisici o della Rete in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio.
- **Autorità di Controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;
- **Consenso dell'Interessato** o **Consenso**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;
- **Dati Biometrici:** i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **Dati Comuni:** sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;
- **Dati Genetici:** i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **Dati Giudiziari:** Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- **Dati Particolari:** Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- **Dati relativi alla Salute:** i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**Interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Destinatario/i**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;
- **Device Fissi**: si intendono gli strumenti informatici non facilmente removibili dal perimetro dell'Ordine quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;
- **Device Mobili**: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro dell'Ordine quali pen drive (chiavette USB), SD cards, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale;
- **RPD (Responsabile Protezione Dati) – DPO (Data Protection Officer)**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;
- **GDPR** o **Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.
- **Incaricato/i o Persona/e Autorizzata/e:** si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a

chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori dell'Ordine e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti di proprietà dell'Ordine o Strumenti Personali operino sulla Rete ovvero siano a conoscenza di informazioni dell'Ordine rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi dell'Ordine, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

- **Limitazione Di Trattamento:** il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;
- **Processo Decisionale Automatizzato:** decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;
- **Profilazione:** qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **Pseudonimizzazione:** il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;
- **Rappresentante:** la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;
- **Responsabile del Trattamento** o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;
- **Rete:** rappresenta il perimetro digitale dell'Ordine contenente Dati Personali e/o informazioni riservate comprensivo della rete interna (intranet) e della rete esterna (internet) a cui ci si può collegare via rete LAN, Wi-Fi o VPN.
- **Strumenti di proprietà dell'Ordine**: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dall'Ordine alle Persone Autorizzate al fine di svolgere le proprie mansioni;
- **Strumenti Personali**: i Device Mobili di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;
- **Terzo:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le Persone Autorizzate al Trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile;
- **Titolare del Trattamento** o **Titolare:** 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 o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **Trattamento** o **Trattato/Trattati:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **Trattamento Transfrontaliero:** a) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del Trattamento o Responsabile del Trattamento

nell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

- **Violazione Dei Dati Personali** ovvero **Data Breach:** è 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;

Normativa di riferimento

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
   a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   c) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. l titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34

Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e 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;

b) 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 di cui al paragrafo 1;
   c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.