Versione	Oggetto della revisione	Emesso a cura di	Rilascio e approvazione
1.0	Prima redazione	DPO	3 gennaio 2023

DESTINATARI
Destinatari della presente procedura sono il Titolare del trattamento e tutti i dipendenti e collaboratori dell'Ordine degli Ingegneri della città metropolitana di Venezia.

SCOPO
La presente procedura regolamenta la gestione degli eventi di Data Breach o quelli che vengono, in prima battuta considerati come tali. Si considerano eventi di Data Breach tutti gli eventi che comportano in modo accidentale o illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali come di seguito meglio precisato.

DEFINIZIONI ED ACRONIMI
RGPD: Regolamento dell'Unione europea in materia di trattamento dei dati personali n. 2016/679
Ordine: Ordine degli Ingegneri della città metropolitana di Venezia
Referente Privacy: persona fisica che all'interno dell'Ordine ha li compito di assicurarsi dell'applicazione degli obblighi privacy;
Autorizzati al trattamento: persone fisiche che all'interno dell'Ordine sono autorizzate a trattare dati personali;
"*Dato personale*" *(art 4 punto 1 RGDP)*: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), 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;
"*Trattamento*" (art 4 punto 2 RGDP): 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, li raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
"*Titolare del trattamento*" (art 4 punto 7 RGDP): la persona fisica o giuridica, l'autorità pubblica, li servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
"*Responsabile del trattamento"* (art 4 punto 8 RGDP): 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 "RPD*"): Il Data Protection Officer (o Responsabile della protezione dei dati) nominato dall'Ordine;
"*Data Breach*" o "*Violazione dei dati personali*" (art 4 punto 12 RGDP): indica qualsiasi 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;
"Distruzione dei dati": si intende un evento a seguito del quale i dati personali non esistono più o non sono più disponibili in una forma che ne permetta l'uso da parte del Titolare;
"Perdita dei dati": si intende un evento a seguito del quale il dato personale può ancora esistere, ma il Titolare ha perso qualsiasi controllo o possibilità di accedere allo stesso o non è più nella disponibilità del Titolare

“Trattamento non autorizzato o illecito": si intende un'azione che include la divulgazione dei dati o l'accesso da parte di un soggetto che non è autorizzato a riceverli o ogni altra forma di trattamento che viola il RGPD.

RIFERIMENTI

- artt. 33 e 34 del RGPD;
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del RGPD, adottate dal Gruppo di Lavoro Art. 29 in data 3 ottobre 2017 e successivamente emendate in data 6 febbraio 2018.

GESTIONE DEGLI EVENTI DI DATA BREACH

Ai fini di garantire una corretta gestione degli eventi di Data Breach è stato istituito un “Comitato Data Breach” costituito dai seguenti soggetti:

- Presidente dell’Ordine;
- Referente Privacy;
- RPD (in funzione meramente consultiva e non decisionale).

Il Comitato Data Breach avrà il compito di:

- Ricevere le comunicazioni di eventi di Data Breach;
- Valutare tali eventi e qualificarli individuando il livello di rischio verso gli interessati in base all’analisi dei rischi svolta;
- Individuare eventuali soluzioni immediate di ripristino e tutela;
- Predisporre le eventuali necessarie notifiche di Data Breach al Garante Privacy e/o agli Interessati.

SEGNALAZIONE DEGLI EVENTI DI DATA BREACH

E’ fatto obbligo a tutti i destinatari di questa procedura di segnalare **immediatamente** (entro massimo 2 ore dalla scoperta) tutti i possibili eventi di data breach.

Le segnalazioni dovranno avvenire secondo la seguente procedura:

- gli autorizzati del trattamento dovranno segnalare l’evento al Referente Privacy;
- Il Referente Privacy dovrà segnalare l’evento al Comitato Data Breach;
- le società esterne che trattano dati per conto dell’Ordine in qualità di Responsabili/Contitolari del trattamento dovranno segnalare l’evento di Data Breach al Titolare del trattamento.

MODALITA’ E CONTENUTO DELLA SEGNALAZIONE DEGLI EVENTI DI DATA BREACH

L’evento di Data Breach dovrà essere segnalato in via preliminare telefonicamente, e successivamente per iscritto tramite e-mail, allegando, compilandolo con le informazioni disponibili, il **Modulo di segnalazione Data Breach** allegato alla presente procedura.

VALUTAZIONE E GESTIONE DELL’EVENTO DA PARTE DEL COMITATO DATA BREACH

Raccolta la segnalazione, attraverso le forme e modalità sopra indicate, il ricevente membro del Comitato Data Breach avvisa il Presidente il quale provvede ad avvisare e/o convocare sia gli altri membri del Comitato sia eventuali altri soggetti potenzialmente coinvolti nell’evento sulla base delle informazioni disponibili.

A seguito di ciò il Comitato Data Breach:

- analizza l’evento sulla base delle informazioni ricevute e valuta se lo stesso rientri o meno inella definizione di Data Breach, tenendo presente che, in caso di dubbio deve assumere un atteggiamento prudenziale a difesa dei diritti dell’interessato;
- in caso positivo analizza l’esistenza di eventuali rischi per gli interessati ed il grado di rischio, valutando le conseguenze dell’evento in base ai parametri individuati ed in particolare: tipologia della violazione, tipologia/natura dei dati personali colpiti, portata della violazione (n. e/o % interessati e n. dati), arco temporale coinvolto, interessati coinvolti e facilità o meno di identificazione degli interessati, data base coinvolti, gravità delle conseguenze per gli interessati, attualità dei dati violati, considerando i rischi di riservatezza, integrità, disponibilità;
- se necessario, procede nella raccolta di eventuali ulteriori informazioni al fine di chiarire la veridicità, la portata e la reale sussistenza dell’evento segnalato;
- valuta eventuali azioni correttive per contenere gli effetti dell’evento e ne ordina l’implementazione;

- verbalizza l'analisi svolta e l'esito, comprese le misure individuate e le proprie osservazioni in merito alla necessità di effettuare la notificazione al Garante e/o agli Interessati, predisponendo bozza dei relativi testi; in ogni verbale sottoscritto dai partecipanti alla riunione devono essere indicati chi partecipa, le decisioni assunte nel corso dell'incontro, lo stato di avanzamento delle decisioni assunte nel corso di incontri precedenti;
- compila e mantiene aggiornato un registro degli incidenti di Data Breach;
- archivia tutta la documentazione raccolta per ogni singolo evento di Data Breach e la mantiene per 10 anni.

NOTIFICAZIONE AL GARANTE PRIVACY

Nel caso di un Data Breach con esito di livello di rischio elevato sussisterà probabilmente un rischio per i diritti e le libertà degli interessati ai sensi dell'art 33 RPGD e pertanto in caso di violazione sarà necessario effettuare la notifica dell'evento all'Autorità di controllo (Garante della Privacy), senza ingiustificato ritardo, entro massimo 72 ore dalla venuta a conoscenza dell'evento di Data Breach.
Qualora la notifica non sia effettuata entro tale termine, sarà necessario corredare la notifica dei motivi del ritardo.

Nel caso di un Data Breach con esito di livello di rischio medio dovranno essere effettuati i necessari approfondimenti sui rischi specifici residui per gli interessati, valutando di volta in volta se ricorrono i presupposti necessari o meno per la notifica al Garante.
L'art. 33 del GDPR evidenzia come le violazioni per le quali sia considerato improbabile un rischio per i diritti e le libertà delle persone fisiche, non richiedano la necessaria notifica all'Autorità di controllo (per esempio, la comunicazione di dati personali che siano già disponibili pubblicamente non costituisce un probabile rischio per gli individui).

Nei casi in cui risulti necessaria la notifica, il Comitato Data Breach procede alla predisposizione delle bozze dei testi delle notifiche, al Garante Privacy e/o agli interessati, che dovranno essere emesse, in caso di valutazione positiva da parte dello stesso, a cura del Presidente.
Qualora invece il Data Breach sia occorso al Responsabile o al Contitolare del trattamento, il Responsabile, attenendosi alle istruzioni presenti nella Nomina, avvisa esclusivamente il Titolare del trattamento restando disponibile successivamente ad ogni necessaria precisazione richiesta dallo stesso.

La notifica da indirizzare al Garante deve contenere almeno le seguenti informazioni:
- descrizione della natura della violazione dei dati (laddove possibile categorie e numero approssimativo di interessati, categorie e numero approssimativo di registrazioni dei dati in questione);
- nome e dati di contatto del DPO;
- descrizione delle probabili conseguenze del Data Breach;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche per attenuarne i possibili effetti negativi.

Se non è possibile fornire le informazioni suddette contestualmente alla prima notifica da svolgersi entro 72 ore, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

NOTIFICA AGLI INTERESSATI

Per i Data Breach classificati con livello di rischio elevato, il Comitato Data Breach dovrà altresì valutare se sussistono rischi elevati per i diritti e le libertà degli interessati valutando in particolare, secondo quanto indicato dall'art 34 del GDPR, se:
- siano state adottate le misure tecniche e organizzative adeguate di protezione e se tali misure fossero 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;
- siano state adottate successivamente misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- l'eventuale comunicazione agli interessati oggetto della violazione richiederebbe sforzi sproporzionati.

Se almeno una tra le condizioni le prime due condizioni è soddisfatta, non è richiesta la comunicazione all'interessato.

Se l'ultima condizione è soddisfatta e non è soddisfatta almeno una tra le prime due condizioni, il Titolare dovrà ricorrere ad una comunicazione pubblica, o a una misura simile, per mezzo della quale gli interessati sono informati con analoga efficacia.
L'eventuale comunicazione di violazione dovrà avvenire senza ingiustificato ritardo.

La notifica da indirizzare agli interessati deve contenere in modo chiaro e comprensibile le seguenti informazioni:
- descrizione della natura della violazione dei dati personali (laddove possibile categorie e numero approssimativo di interessati, categorie e numero approssimativo di registrazioni dei dati in questione);
- nome e dati di contatto del DPO;
- descrizione delle probabili conseguenze del Data Breach;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche per attenuarne i possibili effetti negativi.

TEMPISTICHE
1. Le comunicazioni di avviso di evento Data Breach devono essere effettuate immediatamente, senza indugio alcuno dall'avvenuta conoscenza dell'evento. Per "immediatamente" si considera un tempo massimo di 2 ore dalla conoscenza dell'evento;
2. La convocazionedel Comitato Data Breach e la valutazione dell'evento con esito finale deve essere effettuata entro massimo 48 ore dalla venuta a conoscenza del Data Breach;
3. Le eventuali comunicazioni al Garante ed agli interessati di avvenuto Data Breach devono essere effettuate entro massimo 72 ore dall'evento di Data Breach.

REGISTRO DATA BREACH
Il Referente Privacy dovrà mantenere aggiornato il registro Data Breach contenente: le violazioni occorse ai dati personali, le circostanze ad essa relative, le sue conseguenze, i provvedimenti adottati per porvi rimedio utilizzando il **modulo di registro di DataBreach allegato**.

CONTENUTO DELLE NOMINE DEI RESPONSABILI / CONTITOLARI DEL TRATTAMENTO
Nell'atto della nomina dei responsabili e contitolari del trattamento deve essere indicato:
- la specificazione dei tempi di comunicazione all'Ordine del Data Breach individuata in un tempo "immediato/senza indugio e nel massimo di 24 ore";
- le conseguenze nel caso di mancata o ritardata comunicazione;
- la disponibilità a collaborare con il Titolare fornendo tutte le informazioni da lui richieste sul Data Breach.

RISERVATEZZA DOCUMENTO
Il presente documento si intende riservato e non divulgabile all'esterno dei destinatari indicati .

Allegati:
1) modulo per la segnalazione di Data Breach;
2) registro di Data Breach.

Il Titolare del trattamento

_____

MODULO COMUNICAZIONE VIOLAZIONE DATI PERSONALI

Autore della segnalazione al Comitato Data Breach del Titolare del trattamento
□ SOGGETTO INTERNO

Nome e Cognome _____

Ruolo_____

Telefono_____

E-mail _____

□ SOGGETTO ESTERNO

Denominazione e ragione sociale_____

Qualificazione rispetto al Titolare:□ RESPONSABILE □ CONTITOLARE □ TITOLARE AUTONOMO

Nome e Cognome del segnalante_____

Telefono_____

E-mail_____

Data ed ora della violazione (specificare se l'evento è avvenuto in tempo indeterminato e specificare se l'evento è ancora in corso)

_____
_____

Tipologia Evento e Causa individuata

_____
_____
_____

Indicazione dei dati oggetto di violazione

- Dati anagrafici
- Dati di contatto (indirizzi e-mail, PEC, numeri di telefono)
- Dati di accesso e identificazione (username, password, codici identificativi,…)
- Dati relativi a minori
- Dati che rivelano l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale
- Dati genetici o biometrici
- Dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona

- Dati giudiziari relativi a condanne o reati
- Copie su supporto informatico di documenti analogici
- Altro:_____

Descrizione della violazione

_____
_____
_____
_____

Indicazione della applicazione, sistema, dispositivo o infrastruttura impattata dalla violazione (specificare database, sistema operativo, indirizzo IP, host name, sito fisico età) e ubicazione degli stessi

_____
_____
_____

Descrizione della tipologia di violazione

□ Lettura (presumibilmente i dati non sono stati copiati)

□ Copia (i dati sono ancora presenti su sistemi del titolare)

□ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

□ Cancellazione (i dati non sono più presenti sui sistemi e non li ha neppure l'autore della violazione)

□ Furto

□ Violazione di riservatezza

□ Violazione di integrità

□ Violazione della disponibilità dei dati

□ Divulgazione non autorizzata di dati personali

□ Perdita o furto di dispositivi di archiviazione digitale

□ Perdita o furto di materiale cartaceo

□ Tentativo di intrusione

□ Malaware

□ Accesso non autorizzato

□ Altro:_____

Status del data breach e contromisure in essere per il contenimento – dettaglio delle misure previste per ridurre il rischio di danni alle persone (es. utilizzo di password, crittografia etc)

_____
_____
_____
_____

Future misure da adottare per ridurre il rischio di reiterazione (es. modifiche al processo, formazione del personale, aggiornamento dei sistemi,…)

_____
_____
_____
_____

Indicazione e recapiti dell'interessato o dei soggetti interessati cui si riferiscono i dati oggetto di Data Breach

_____
_____

Numero persone colpite dalla violazione dei dati personali

□ N. _____ persone
□ Circa _____ persone
□ Un numero (ancora) sconosciuto di persone

Livello di gravità della violazione dei dati personali trattati nell' ambito della banca dati

□ Basso /trascurabile

□ Medio

□ Alto

□ Molto alto

Venezia,_____ Firma _____

REGISTRO DI DATA BREACH

Ordine degli Ingegneri della città metropolitana di Venezia

nome DPO	dott. ing. Silvia Castelli

note del DPO	Si raccomanda di registrare in questo registro ogni evento di Data Breach, anche nel caso in cui si ritenga che la violazione non abbia conseguenze sui diritti degli interessati e non ne venga conseguentemente fatta notifica al garante della Privacy.

CODICE	**SEGNALAZIONE**				**VIOLAZIONE**					**INTERESSATI e DATI**				**CONSEGUENZE**	**RIMEDI**		**ATTENUAZIONE**		**TEMPI**	**NOTIFICA AL GARANTE**				**COMUNICAZIONE AGLI INTERESSATI**				**NOTE**	**ESTENSORE**
codice evento	**data e ora**	**segnalante**	**unità organizzativa coinvolto**	**organi informati**	**luogo violazione**	**modalità violazione**	**sistemi/apparati/reti/ banche dati oggetto di data breach**	**natura della violazione dei dati personali**	**altri elementi utili alla descrizione violazione**	**categorie di interessati**	**numero approssimativo di interessati**	**categorie dei dati personali**	**numero approssimativo di registrazioni dei dati personali**	**conseguenze della violazione dei dati personali**	**misure adottate per porre rimedio alla violazione**	**misure di cui si propone l'adozione per porre rimedio alla violazione**	**misure adottate per por attenuare i possibili effetti negativi**	**misure di cui si propone l'adozione per attenuare i possibili effetti negativi**	**tempo ripristino**	**rischio per i diritti e le libertà delle persone fisiche:**	**invio di notificazione alla DPA**	**ragioni dell'invio di notificazione parziale**	**ragioni del ritardo della notificazione alla DPA**	**ragioni di omessa notifica alla DPA**	**Indicare se ricorre rischio elevato per i diritti e le libertà delle persone fisiche**	**comunicazione agli interessati:**	**modalità della comunicazione agli interessati**	**ragioni della omessa comunicazione agli interessati**	**note**	**nome e cognome estensore**
Il codice dell'evento è un numero progressivo a partire da 1 seguito dalle ultime due cifre dell'anno solare in cui è accaduto l'evento (ad esempio 01/22)	circostanze cronologiche della segnalazione	indicare se designati o autorizzati del titolare o responsabile esterno o terzi	indicare ufficio/unità organizzativa interessata dalla violazione	indicare ufficio/unità organizzativa destinataria della segnalazione	indicare circostanze di luogo della violazione della sicurezza	descrivere il flusso delle azioni in cui è consistita la violazione	indicare le infrastrutture o gli applicativi coinvolti nelle violazioni	indicare se si tratta di violazione della riservatezza, delle integrità, e/o della disponibilità dei dati ("**violazione della riservatezza**": divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali; "**violazione dell'integrità**": modifica non autorizzata o accidentale dei dati personali; "**violazione della disponibilità**": perdita, accesso o distruzione accidentali o non autorizzati di dati personali.)	indicare ogni altra circostanza utile alla analisi della violazione	indicare in particolare se si tratta di soggetti vulnerabili	indicare un dato quantitativo, anche approssimato	indicare se si tratta di dati particolari, di dati relativi a condanne o reati o altri tipi di dati	indicare un dato quantitativo, anche approssimato	indicare eventuali pregiudizi e danni materiali o immateriali- patrimoniali o reputazionali - patiti dagli interessati (ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo)	indicare precauzioni già adottate che eliminano le conseguenze	indicare precauzioni in corso di adozione che eliminano le conseguenze	indicare precauzioni già adottate che riducono le conseguenze	indicare precauzioni in corso di adozione che riducono le conseguenze	indicare tempo della chiusura dell'episodio della violazione	indicare improbabile/non improbabile (considerare: 1) Tipo di violazione; 2) Natura, carattere sensibile e volume dei dati personali; 3) Facilità di identificazione delle persone fisiche; 4) Gravità delle conseguenze per le persone fisiche; 5) Caratteristiche particolari dell'interessato; 6) Caratteristiche particolari del titolare del trattamento di dati; 7) Numero di persone fisiche interessate; 8) Aspetti generali.	indicare sì/no; in caso affermativo indicare data e ora; se totale o parziale; in tale caso, il numero ordinale della notifica (prima, seconda, ecc.) o se ultima	indicare circostanze relative all'accertamento della violazione che giustifichino notificazioni parziali (ad esempio necessità di effettuare ulteriori indagini; se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l'autorità di controllo. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.)	indicare circostanze relative all'accertamento della violazione che giustifichino il ritardo posteriore a 72 ore in quanto qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata dei motivi del ritardo	indicare ragioni di improbabilità del rischio per gli interessati(ad esempio dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica; dati personali resi sostanzialmente incomprensibili ai soggetti non autorizzati e se esiste una copia o un backup; dati personali correttamente crittografati)	indicare tipo di rischio e ragioni per cui tale rischio sia elevato	indicare sì/no; in caso affermativo indicare data e ora; se effettuata su ordine della DPA	indicare mezzo di comunicazione utilizzato e modalità di assistenza agli interessati (si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard; esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituisce un mezzo efficace. A seconda delle circostanze, utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto. usare formati alternativi appropriati e lingue pertinenti)	(inserire una delle ipotesi di cui all'art. 34, par. 3, lett. a), b), c) del GDPR (ad esempio,a seconda dei casi: cifratura allo stato dell'arte oppure mediante tokenizzazione;immediata individuazione e avvio di un'azione contro il soggetto che ha avuto accesso ai dati personali prima dell'utilizzo; comunicazione pubblica o prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta)	note aggiuntive	nome e cognome di chi ha compilato la riga di documento