DATA BREACH POLICY
PROCEDURA DI NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI

1. PREMESSE

L'Ente, ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Ente e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.
L'omessa notifica di Data Breach all'Autorità di Controllo e l'omessa comunicazione agli interessati, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo all'Ente di una sanzione amministrativa pecuniaria, ai sensi dell'art. 83 GDPR, fino a 10 milioni di euro o per le imprese, fino al 2% del "fatturato" mondiale annuo totale dell'esercizio precedente se superiore, anche accompagnata da una misura correttiva ai sensi dell'art. 58 paragrafo 2.

2. SCOPO

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni dei dati personali trattati dall'Ente in qualità di Titolare del trattamento (di seguito "Titolare del trattamento"). Queste procedure sono ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.

3. COS'E' UNA VIOLAZIONE DEI DATI (DATA BREACH)

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - 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.
Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- perdita o distruzione accidentale o non autorizzata dei dati personali;
- alterazione accidentale o non autorizzata dei dati personali;
- infedeltà del personale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- accesso accidentale (ad esempio: dato personale inviato per errore a terzo non autorizzato);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";

- virus o altri attacchi al sistema informatico o alla rete informatica;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

4. A CHI SONO RIVOLTE QUESTE PROCEDURE?

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (di seguito genericamente denominati Destinatari esterni);

di seguito, genericamente denominati "Destinatari".
Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.
Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

5. A QUALI TIPI DI DATI SI RIFERISCONO QUESTE PROCEDURE?

Queste procedure si riferiscono a:

- dati personali trattati "da" e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati a mezzo di qualsiasi altro sistema adottato dall'ente.

Per «dato personale» si intende: 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.

6. GESTIONE COMUNICAZIONE DI DATA BREACHES

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da soggetti dallo stesso espressamente designati con decreto sindacale.
In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.
Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il Suo superiore gerarchico o il Dirigente/Responsabile del S.A. dell'Ente, il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento o il/i suo/suoi designato/i mediante la compilazione dell'Allegato A – Modulo di comunicazione Data Breach da inviare a mezzo mail all'indirizzo servizi.informatici@comune.mondovi.cn.it e info@comune.mondovi.cn.it e ad avvertire immediatamente telefonicamente sia l'Ufficio Servizi Informatici ai numeri 0174/559281-306 che il Titolare del trattamento (in persona del sindaco p.t., in qualità di legale rappresentante dell'Ente) al numero 0174/559250.
Il Titolare del trattamento o il/i suo/suoi designato/i provvederanno ad avvertire immediatamente il DPO.

7. GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti cinque step:

- **Step 1**: Identificazione e indagine preliminare
- **Step 2**: Contenimento, recovery e risk assessment
- **Step 3**: Eventuale notifica all'Autorità Garante
- **Step 4**: Eventuale comunicazione agli interessati
- **Step 5**: Documentazione della violazione.

STEP 1: IDENTIFICAZIONE E INDAGINE PRELIMINARE

L'Allegato A, debitamente compilato, permetterà al Titolare del trattamento o al/ai suo/suoi designato/i di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2).
Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o il/i suo/suoi designato/i dovranno coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile dell'Ufficio Servizi Informatici o un suo delegato, in caso di assenza.
Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A, quali:

- la data di scoperta della violazione (tempestività);
- il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

STEP 2: CONTENIMENTO, RECOVERY E RISK ASSESSMENT

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o il/i suo/suoi designato/i dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (ad esempio, riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento o il/i suo/suoi designato/i valuteranno la gravità della violazione, utilizzando l'Allegato B - Modulo di valutazione del Rischio connesso al Data Breach che dovrà essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 e 34 GDPR. In presenza di soggetti designati, tale valutazione verrà in ogni caso condivisa con il Titolare del trattamento, in persona del Sindaco p.t., legale rappresentante dell'Ente.
Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio *semplice*, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio *elevato*.

STEP 3: EVENTUALE NOTIFICA ALL'AUTORITÀ GARANTE

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Ente dovrà provvedervi, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza.

STEP 4: EVENTUALE COMUNICAZIONE AGLI INTERESSATI

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Ente dovrà provvedervi, senza ingiustificato ritardo.
Quanto al contenuto di tale comunicazione, il Titolare del trattamento dovrà:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento dovrà sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e- mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

STEP 5: DOCUMENTAZIONE DELLA VIOLAZIONE

Il Titolare del trattamento ha l'obbligo di documentare le violazioni di dati personali subite, tramite un apposito registro delle violazioni.
Il registro dovrà contenere:

- data e ora della violazione;
- sorgente dell'informazione sulla violazione;
- conseguenze della violazione (quantità dei dati personali e degli interessati coinvolti dalla violazione);
- data o ora della notifica della violazione all'autorità di controllo;
- motivo per il quale la violazione è stata ritardata o non è stata comunicata all'autorità di controllo;
- cause della violazione;
- provvedimenti adottati a seguito della violazione.

Tale documentazione dovrà essere fornita al Garante in caso di accertamenti.

8. VALIDITA'

Il presente Disciplinare ha validità a partire da: 11/04/2019
Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di mutazioni legislative. Ogni variazione del presente Disciplinare sarà comunicata agli soggetti autorizzati al trattamento.

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

Qualora scopra un Data Breach, è pregato di informare immediatamente il Suo superiore gerarchico o il Dirigente /Responsabile del S.A. dell'Ente, il quale, a sua volta, dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo email: servizi.informatici@comune.mondovi.cn.it e info@comune.mondovi.cn.it

DOMANDA	RISPOSTA
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione *(specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)*:	
Nome della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): *In caso di destinatario esterno indicare la ragione sociale:*	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Responsabile della funzione:	
Data:	

Avvertimento

Si prega di avvertire ***immediatamente***:

- l'Ufficio Servizi Informatici ai numeri 0174/559281-306;
- il Titolare del trattamento al numero 0174/559250.

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

Una volta ricevuta la comunicazione di Data Breach mediante l'All. A, il Titolare del trattamento o il/i suo/suoi designato/i compilano il presente Allegato B - Modulo di valutazione del Rischio connesso al Data Breach, che dovrà essere esaminato unitamente all'Allegato A.

ASSESSMENT DI GRAVITÀ	A CURA DEL DPO INSIEME CON L'UFFICIO IT E IL RESPONSABILE DELL'UFFICIO COINVOLTO DELLA VIOLAZIONE
Dispositivi oggetto del Data Breach *(computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).*	
Modalità di esposizione al rischio *(tipo di violazione)*: **lettura** *(presumibilmente i dati non sono stati copiati)*, **copia** *(i dati sono ancora presenti sui sistemi del titolare),* **alterazione** *(i dati sono presenti sui sistemi ma sono stati alterati),* **cancellazione** *(i dati non sono più presenti e non li ha neppure l'autore della violazione),* **furto** *(i dati non sono più sui sistemi del titolare e li ha l'autore della violazione),* **altro.**	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori dell'Ente: operation, research, financial, legal, liability or reputation?	
Qual è la natura dei dati coinvolti? Compilare le sezioni sottostanti: • Dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: ✓ origine razziale o etnica; ✓ opinioni politiche, convinzioni religiose o filosofiche; ✓ appartenenza sindacale; ✓ dati genetici; ✓ dati biometrici; ✓ dati giudiziari; • Informazioni relative alla salute o all'orientamento sessuale di una persona.	

• Informazioni che possono essere utilizzate per commettere furti d'identità *(i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);* • Informazioni personali relative a soggetti fragili *(i.e. anziani, disabili, minori);* • Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone; • Altro: (*specificare…*)	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? *(i.e. La pseudonimizzazione e la cifratura dei dati personali)*	
Il Titolare del trattamento ha aderito ad un codice di condotta approvato ai sensi dell'art. 40 Regolamento (UE) o un meccanismo di certificazione di cui all'art. 42 Regolamento (UE)?	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione (1, 2 o 3) e motivazioni	
Notificazione del Data Breach all'Autorità Garante	**Comunicazione del Data Breach ad altri soggetti (i.e. casa madre)**
Comunicazione del Data Breach agli interessati	**Comunicazione del Data Breach ad altri soggetti (i.e. casa madre)**
Comunicazione del Data Breach ad altri soggetti (i.e. casa madre)	**Comunicazione del Data Breach ad altri soggetti (i.e. casa madre)**