|  |  |
| --- | --- |
|  | COMUNE DI MONTALTO DELLE MARCHEPROVINCIA DI ASCOLI PICENOViale dei Tigli n. 37 63068 Montalto delle Marche (AP) |

**ISTRUZIONE OPERATIVA DATA BREACH**

**All. C del regolamento comunale**

Montalto delle Marche, \_\_\_\_\_\_\_\_\_\_\_\_

L’art. 33 del**Regolamento Europeo 679/2016** (**GDPR**) impone al titolare del trattamento di notificare all’autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L’obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all’interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l’eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L’eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell’obbligo di notifica, invece, pone l’autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l’esercizio dei poteri previsti dall’art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l’art. 83 GDPR.

Per **“Violazione di dati**” si intende 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 (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall’art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l’incidente di sicurezza in genere, quindi, comprendere che l’incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall’incidente vi sono dati personali.

L’art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all’autorità di controllo di verificare il rispetto della norma.

L’art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E’ importante che sia dimostrabile il momento della scoperta dell’incidente, poiché da quel momento decorrono le 72 ore per la notifica.



Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un’alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell’entità dei rischi:

* Rischio assente: la notifica al Garante non è obbligatoria.
* Rischio presente: è necessaria la notifica al Garante.
* Rischio elevato: In presenza di rischi “elevati”, è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l’acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

* coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
* riguardare categorie particolari di dati personali;
* comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
* comportare rischi imminenti e con un’elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
* impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per valutare i fattori che determinano il rischio per le libertà e i diritti degli interessati, il Gruppo di lavoro Articolo 29 (ora EDPB) ha fissato i seguenti parametri:

* tipo di “breach”: il tipo di violazione è un parametro per la valutazione del rischio. La violazione dei dati sanitari di tutti i pazienti di un ospedale è ben diversa dalla perdita dei dati sanitari di un singolo paziente;
* natura, numero e grado di sensibilità dei dati personali violati: l’accesso al nome e all’indirizzo dei genitori di un figlio rappresenta un rischio diverso rispetto all’accesso da parte dei genitori naturali del nome e dell’indirizzo dei genitori adottivi;
* facilità di associare i dati violati ad una persona fisica: può accadere che i dati violati non siano facilmente riconducibili ad una determinata persona fisica;
* gravità delle conseguenze per gli Interessati: quando il titolare del trattamento percepisce il rischio che i dati oggetto della violazione possono essere utilizzati immediatamente contro gli Interessati (es. sostituzione di persona);
* numero di Interessati esposti al rischio: un parametro è sicuramente quello del numero degli Interessati potenzialmente coinvolti;
* caratteristiche del titolare del trattamento: un attacco ad una struttura ospedaliera certamente è diverso dall'attacco ad una piccola azienda.

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

Il titolare deve **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](https://protezionedatipersonali.it/autorita-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.



**VIOLAZIONE DI DATI PERSONALI**

**MODELLO DI COMUNICAZIONE AL GARANTE**

A seguito del recepimento della direttiva 2009/136/Ce ad opera del decreto legislativo 28 maggio 2012, n. 69, i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare al Garante e, in alcuni casi, al contraente o ad altre persone interessate, le violazioni dei dati personali (Data breach) che detengono nell’ambito delle proprie strutture.

 **Titolare che effettua la comunicazione**

Denominazione o ragione sociale: ……………………………………………………………………………………………………

Provincia…………………………………………………Comune……………………………………………………………………………

Cap. …………………………………… Indirizzo ……………………………………………………………………………………………

Nome persona fisica addetta alla comunicazione………………………………………………………………………………

Cognome persona fisica addetta alla comunicazione…………………………………………………………………………

Funzione rivestita………………………………………………………………………………………………………………………………

Indirizzo Email/PEC per eventuali comunicazioni……………………………………………………………………………

Recapito telefonico per eventuali comunicazioni………………………………………………………………………………

Eventuali Contatti (altre informazioni) …………………………………………………………………………………………

**Natura della comunicazione**

☐ Nuova comunicazione

☐ Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)

☐ Ritiro precedente comunicazione

**Breve descrizione del trattamento di dati personali**

**Quando si è verificata la violazione di dati personali?**

☐ Il………………

☐ Tra il……………… e il ………………

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

**Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)**

**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 sui sistemi del titolare 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: ……………………………………………………………………………………………………………………………………………

**Dispositivo oggetto della violazione**

☐ Postazione di lavoro

☐ Dispositivo di acquisizione o dispositivo-lettore

☐ Smart card o analogo supporto portatile

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Rete

☐ Altro: ……………………………………………………………………………………………………………………………………………

**Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:**

**Quante persone sono state colpite dalla violazione di dati personali?**

☐ N. …………………… di persone

☐ Circa …………………… persone

☐ Un numero (ancora) sconosciuto di persone

**Che tipo di dati sono coinvolti nella violazione ?**

☐ Dati anagrafici

☐ Numero di telefono (fisso o mobile)

☐ Indirizzo di posta elettronica

☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)

☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

☐ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari Ancora sconosciuto

☐ Altro:……………………………………………………………………………………………………………………………………………

**Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?**

☐ Basso/trascurabile ☐ Medio ☐ Alto ☐ Molto alto

**Misure tecniche e organizzative applicate ai dati colpiti dalla violazione**

**La violazione è stata comunicata anche agli interessati?**

☐ Sì, è stata comunicata il ……………………

☐ No, perché …………………………………………………………………………………………………………

**Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?**

**Quale canale è utilizzato per la comunicazione ai contraenti (o alle persone interessate)?**

**Quali misure tecnologiche ed organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?**

**La violazione coinvolge contraenti (o altre figure interessate) che si trovano in altri Paesi UE?**

☐ Sì ☐ No

**La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?**

☐ No ☐ Sì

**REGISTRO DELLE VIOLAZIONI**

**Registrazione n° \_\_\_\_\_\_\_\_\_\_ del \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| 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](https://protezionedatipersonali.it/autorita-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 |  |