Mod. 09.1

PROCEDURA DI RISPOSTA E COMUNICAZIONE DI UNA VIOLAZIONE DI DATI

Codice:	09.1/Procedura Comunicazione Violazione Dati
Edizione:	01
Revisione:	00
Data di revisione:	07/12/2020
Redatta da:	A.C.M Service s.r.l.
Approvata da:	A.C.M Service s.r.l.
Livello di Riservatezza:	II Livello

Mod. 09.1

Data	Revisione	Approvata da	Descrizione della modifica
07/12/2020	00	A.C.M Service s.r.l.	Prima Emissione

Sommario

1. Campo d'applicazione, scopo e destinatari

Questa Procedura fornisce principi generali e un modello di approccio per rispondere a, e mitigare, le violazioni di dati personali (una "violazione dei dati personali") in una o in entrambe le seguenti situazioni:

- Il dato personale identifica gli interessati che risiedono negli Stati Membri dell'Unione Europea (UE) e nelle nazioni all'interno dello Spazio Economico Europeo (SEE), indipendentemente da dove tali dati siano soggetti al trattamento a livello globale; e

- I dati personali sono soggetti a trattamento all'interno dell'UE e/o del SEE, indipendentemente dal paese di residenza dell'interessato.

La Procedura definisce i principi e le azioni generali per gestire con successo la risposta a una violazione di dati e adempiere agli obblighi relativi alla notifica alle Autorità di Controllo e ai singoli individui, come richiesto dal GDPR dell'UE.

Tutti i Dipendenti/il Personale, Collaboratori o dipendenti temporanei/Personale e terzi che lavorano o agiscono per conto dell'Azienda **A.C.M. Service s.r.l.** ("Azienda") devono essere a conoscenza e seguire la presente Procedura in caso di violazione dei dati personali.

2. Documenti di Riferimento

- Il GDPR dell'UE 2016/679 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)
- D. Lgs. 101/2018
- Politica sulla Protezione dei Dati Personali

3. Definizioni

Le seguenti definizioni di termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione europea (o GDPR):

"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;

"Controllore" dei dati: 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.

"Processore" dei dati: una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Controllore.

"Trattamento": 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.

P.IVA 04042820615 – REA 283727 – CCIAA Caserta
Tel. +39 0823 1840454 – Fax +39 0823 1601294
WEB: http://www.acm-service.it – MAIL: info@acm-service.it

“Violazione dei Dati Personali”: 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.

“Autorità di Controllo”: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell’UE.

4. Gruppo di Risposta alle Violazioni dei Dati

Un Gruppo di Risposta alle Violazioni dei Dati deve essere un gruppo multidisciplinare costituito da persone esperte e competenti nel reparto IT, Sicurezza Informatica, Ufficio Legale, Ufficio Legale e Affari Pubblici. Il gruppo può essere un team fisico (locale) o virtuale (sedi multiple) che risponde a qualsiasi sospetta/presunta violazione dei dati personali.

Il Titolare dell’Azienda nomina i membri del Gruppo di Risposta alle Violazioni dei Dati. Il Gruppo deve essere nominato a prescindere dal fatto che una violazione sia avvenuta o meno.

Il gruppo deve garantire la prontezza necessaria per una risposta alla violazione dei dati personali, insieme alle risorse e alla preparazione necessarie (come elenchi di persone da chiamare, sostituzione di ruoli chiave, simulazioni, oltre alla revisione richiesta delle politiche, delle procedure e delle pratiche aziendali).

La missione del gruppo è di fornire una risposta immediata, efficace e esperta a qualsiasi sospetta/ presunta o effettiva violazione dei dati personali che riguardi l’Azienda.

Se richiesto, i membri del gruppo possono anche coinvolgere parti esterne (ad esempio, un fornitore di sicurezza informatica per svolgere attività di informatica forense o un'agenzia di comunicazione esterna per assistere l’Azienda in necessità di comunicazione di crisi).

Il Responsabile del Gruppo di Risposta alle Violazioni dei Dati può scegliere di inserire personale aggiuntivo al gruppo allo scopo di gestire una specifica violazione dei dati personali.

Il Gruppo di Risposta alle Violazioni dei Dati può trattare più di una violazione dei dati personali sospetta/presunta o effettiva alla volta. Sebbene il gruppo centrale possa essere lo stesso per ogni violazione dei dati personali sospetta/presunta o effettiva, non vi è alcun obbligo in tal senso.

Il Gruppo di Risposta alle Violazioni dei Dati deve essere preparato a rispondere a una violazione dei dati personali sospetta/presunta o effettiva 24 ore su 24, 7 giorni su 7, per tutto l'anno. Pertanto, le informazioni di contatto di ciascun membro del Gruppo di Risposta alle Violazioni dei Dati, inclusi i dati personali, devono essere archiviate in un sito centrale e devono essere utilizzati per riunire il gruppo ogni volta che viene ricevuta una notifica di sospetta/presunta o effettiva violazione dei dati personali.

5. I compiti del Gruppo di Risposta alle Violazioni dei Dati

Una volta che una violazione dei dati personali viene segnalata al responsabile del Gruppo di Risposta alle Violazioni dei Dati, il gruppo dovrà implementare quanto segue:

- Convalidare/assegnare un livello di urgenza alla violazione dei dati personali
- Assicurare che sia avviata, condotta, documentata e conclusa un'indagine corretta e imparziale (compresa l'informatica forense, se necessario)
- Identificare i requisiti per la risoluzione e monitorare la soluzione
- Riferire i risultati all'alta direzione
- Coordinarsi con le autorità competenti se necessario
- Coordinare le comunicazioni interne ed esterne
- Assicurarsi che gli interessati siano adeguatamente informati, se necessario.

Il Gruppo di Risposta alle Violazioni dei Dati si riunirà per ogni violazione dei dati personali segnalata (e presunta) e sarà guidato dal Responsabile del Gruppo di Risposta alle Violazioni dei Dati.

6. Il Processo di Risposta alle Violazione dei Dati

Il Processo di Risposta alle Violazione dei Dati viene avviato quando qualcuno si accorge che una sospetta / presunta o effettiva violazione dei dati personali si è verificata e lo comunica a qualsiasi membro del Gruppo di Risposta alle Violazioni dei Dati. Il gruppo è responsabile di determinare se la violazione debba essere considerata una violazione dei dati personali.

Il Responsabile del Gruppo di Risposta alle Violazioni dei Dati è incaricato della documentazione (es. Verbale di riunione) di tutte le decisioni del gruppo principale. Poiché questi documenti potrebbero essere esaminati dalle autorità di controllo, devono essere scritti in modo molto preciso e accurato per garantire la tracciabilità e la responsabilizzazione.

7. Notifica di violazione dei dati personali: Il processore al controllore dei dati

Qualora la violazione dei dati personali o la sospetta violazione dei dati riguardassero i dati personali che vengono elaborati per conto di terzi, il Titolare dell'Azienda che agisce come un processore di dati deve segnalare qualsiasi violazione dei dati personali al rispettivo controllore/controllori dei dati senza indebito ritardo.

Il Titolare invierà una notifica al controllore che includerà quanto segue:

- Una descrizione della natura della violazione
- Le categorie dei dati personali in questione
- Il numero approssimativo degli interessati
- Il nome e le informazioni di contatto del Responsabile del Gruppo di Risposta alle Violazioni dei Dati / Responsabile della Protezione dei Dati

- Le conseguenze della violazione dei dati personali
- Le misure adottate per gestire la violazione dei dati personali
- Qualsiasi informazione relativa alla violazione dei dati

Il **Titolare** registrerà la violazione dei dati nel Registro delle Violazioni dei dati.

8. Notifica della violazione dei dati: il controllore dei dati all'autorità di controllo

Qualora la violazione dei dati personali o sospetta violazione dei dati riguarda i dati personali trattati dell'Azienda come controllore dei dati, il Titolare eseguirà le seguenti azioni:

1) L'Azienda deve stabilire se la violazione dei dati personali debba essere segnalata all'Autorità di Controllo.

2) Al fine di determinare il rischio per i diritti e le libertà dell'interessato in questione, il Responsabile della Protezione dei Dati deve eseguire la Valutazione d'Impatto sulla Protezione dei Dati sull'attività di trattamento interessata dalla violazione dei dati.

3) Se è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà degli interessati, non è richiesta alcuna notifica. Tuttavia, la violazione dei dati dovrà essere registrata.

4) L'Autorità di Controllo deve essere informata senza indebito ritardo, e non oltre le 72 ore, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio per i diritti e le libertà degli interessati colpiti dalla violazione dei dati personali. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo.

Il **Titolare** invierà una Notifica all'Autorità di Controllo che includerà quanto segue:

- Una descrizione della natura della violazione
- Le categorie dei dati personali in questione
- Il numero approssimativo degli interessati
- Il nome e le informazioni di contatto del Responsabile del Gruppo di Risposta alle Violazioni dei Dati / Responsabile della Protezione dei Dati
- Le conseguenze della violazione dei dati personali
- Le misure adottate per gestire la violazione dei dati personali

- Qualsiasi informazione relativa alla violazione dei dati

9. Comunicazione di violazione dei dati personali: il controllore dei dati all'interessato

Il Titolare dell'Azienda deve valutare se la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà dell'interessato. In caso affermativo, il Titolare dell'Azienda, in quanto Responsabile Dei Dati, deve informare gli interessati senza indebito ritardo.

La comunicazione agli interessati deve essere scritta in un linguaggio chiaro e semplice e deve contenere le stesse informazioni elencate nella Sezione 7.

Se, a causa del numero di interessati, è sproporzionatamente difficile informare tutti i soggetti in questione, il **Titolare** dovrebbe adottare le misure necessarie per garantire che le persone interessate siano informate utilizzando canali appropriati e pubblicamente disponibili.

10. Responsabilizzazione

Qualsiasi individuo violi questa Procedura sarà soggetto a misure disciplinari interne (che possono arrivare alla risoluzione del rapporto di lavoro); inoltre potrebbe anche dover affrontare responsabilità civili o penali qualora le sue azioni violino la legge.

11. Gestione delle registrazioni sulla base di questo documento

Nome del documento	Luogo di archiviazione	Persona responsabile dell'archiviazione	Controlli per la protezione del documento	Tempo di archiviazione
Elenchi delle persone da chiamare e sostituzioni	**CARTACEO**: Faldone Dedicato alla Pratica GDPR & Sicurezza conservato in apposito armadio chiuso a chiave. **DIGITALE**: La documentazione in formato digitale viene archiviata sui sistemi informatici della A.C.M. Service s.r.l. (Server interno con sistema di backup automatico) ad opera del personale interno secondo le regole previste dalla Direzione nel rispetto della normativa ex Reg. UE 2016/679.	Amministratore Unico	Soltanto le persone autorizzate possono modificare i file	Permanente

Informazioni di contatto	**CARTACEO**: Faldone Dedicato alla Pratica GDPR & Sicurezza conservato in apposito armadio chiuso a chiave. **DIGITALE**: La documentazione in formato digitale viene archiviata sui sistemi informatici della A.C.M. Service s.r.l. (Server interno con sistema di backup automatico) ad opera del personale interno secondo le regole previste dalla Direzione nel rispetto della normativa ex Reg. UE 2016/679.	Amministratore Unico	Soltanto le persone autorizzate possono modificare i file	Permanente
Decisioni documentate del Gruppo di Risposta alle Violazioni dei dati	**CARTACEO**: Faldone Dedicato alla Pratica GDPR & Sicurezza conservato in apposito armadio chiuso a chiave. **DIGITALE**: La documentazione in formato digitale viene archiviata sui sistemi informatici della A.C.M. Service s.r.l. (Server interno con sistema di backup automatico) ad opera del personale interno secondo le regole previste dalla Direzione nel rispetto della normativa ex Reg. UE 2016/679.	Amministratore Unico	Soltanto le persone autorizzate possono modificare i file	1 anno

Comunicazione di una Violazione dei Dati	**CARTACEO**: Faldone Dedicato alla Pratica GDPR & Sicurezza conservato in apposito armadio chiuso a chiave. **DIGITALE**: La documentazione in formato digitale viene archiviata sui sistemi informatici della A.C.M. Service s.r.l. (Server interno con sistema di backup automatico) ad opera del personale interno secondo le regole previste dalla Direzione nel rispetto della normativa ex Reg. UE 2016/679.	Amministratore Unico	Soltanto le persone autorizzate possono modificare i file	1 anno
Registro delle Violazioni di Dati	**CARTACEO**: Faldone Dedicato alla Pratica GDPR & Sicurezza conservato in apposito armadio chiuso a chiave. **DIGITALE**: La documentazione in formato digitale viene archiviata sui sistemi informatici della A.C.M. Service s.r.l. (Server interno con sistema di backup automatico) ad opera del personale interno secondo le regole previste dalla Direzione nel rispetto della normativa ex Reg. UE 2016/679.	Amministratore Unico	Soltanto le persone autorizzate possono modificare i file	Permanente

12. Validità e gestione del documento

Questo documento è valido a partire 07/12/2020.

Il responsabile per questo documento è il **Titolare**, Amministratore Unico dell'Azienda, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.

Pignataro Maggiore, 07/12/2020

Mod. 09.1

Amministratore Unico dell'Azienda

Massimo De Maio

_____