LTA S.r.l.
Via Della Conciliazione 10
00193 Roma
P.IVA e C.F. 14243311009

Web: www.LTAdvisors.it
E-mail: info@LTAdvisors.it
Pec: LTA@raccomandata-ar.com

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

1. *Scopo*

La presente procedura ha lo scopo di gestire il necessario flusso di attività da porre in essere nel momento in cui si sviluppi una violazione di dati personali ai sensi degli articoli 33 e 34 del Regolamento 679/2016/UE.

Per data breach, in italiano "violazione dei dati personali", si intende una violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Il Regolamento Europeo prevede che, in caso di violazione dei dati personali, il titolare del trattamento debba notificare la violazione all'Autorità di controllo competente 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.

La procedura sarà gestita tramite il flusso "data breach" presente in MUA–Motore Unico Amministrativo tramite la compilazione di un questionario on-line e coinvolgerà le diverse unità organizzative che segnaleranno l'avvenuta violazione, la funzione interna competente in materia di protezione dei dati ed il Data Protection Officer (DPO).

2. *Casi nei quali avviare la procedura di gestione della violazione dei dati personali (data breach)*

I casi in cui sarà necessario applicare la presente procedura sono, a titolo esemplificativo e non esaustivo:

- Sottrazione di credenziali di autenticazione
- Furto di PC, Notebook, Tablet, Smartphone contenente dati personali
- Erronea diffusione, pubblicazione, comunicazione di dati personali
- Intrusione non autorizzata in locali in cui sono conservati/archiviati dati personali
- Furto di archivi cartacei e/o digitali
- Accesso non autorizzato nel sistema informativo

- Azione di malware (virus, etc.) che siano riusciti ad eludere le misure di sicurezza aziendali
- Smarrimento di dati personali (archiviati su supporti cartacei e digitali)
- Distruzione di dati personali (archiviati su supporti cartacei e digitali)
- Ecc.

3. *Procedura di gestione della violazione dei dati personali (data breach)*

Nel caso in cui un soggetto venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati.

La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:

A. rilevazione della violazione dei dati personali
B. raccolta di informazioni sulla violazione

PER COMUNI

C. comunicazione della violazione al Sindaco, che procederà personalmente o individuerà tra il personale abilitato chi deve procedere con la compilazione del flusso di MUA;
D. compilazione della prima parte del flusso di data breach fino a chiusura della sezione (step A-B-C)
E. compilazione da parte del DPO della seconda parte del Flusso, e valutazione della necessità di effettuare la comunicazione all'Autorità Garante
F. notifica all'Autorità Garante della violazione subita, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche;
G. eventuale comunicazione della violazione di dati personali all'interessato nel caso vi sia un rischio elevato. (Il documento per la segnalazione agli interessati potrà essere generato tramite il flusso dei "data breach")
H. nel caso in cui si sia valutato di non effettuare comunicazione all'Autorità Garante sarà necessario registrare la violazione all'interno del sistema MUA, tramite lo

svolgimento del Flusso di segnalazione di data breach, al fine di mantenere aggiornato il "Registro degli incidenti". Tale registro sarà reperibile all'interno del sistema nella pagina "Elementi di analisi", alla voce "Regolamento 679/2016/UE - Data breach"

4. *Soggetti deputati ad avviare la procedura di gestione della violazione*

La procedura di gestione della violazione verrà avviata da Roberto Chiodi e, in sua sostituzione, da Rubetti Lidia.
Se la violazione riguarda un asset tecnologico-informatico, è opportuno che venga coinvolto la società esterna incaricata dell'assistenza informatica, al fine di valutare la portata della violazione e descrivere dettagliatamente l'accaduto. È inoltre opportuno che chi avvierà la procedura di gestione della violazione coinvolga il referente (interno o esterno) del servizio che ha subito la violazione.

5. *Modalità di avvio della procedura di gestione della violazione*

L'avvio della procedura di gestione data breach dovrà essere sviluppata seguendo le seguenti fasi:

1. comunicazione/segnalazione dell'evento che può comportare una violazione di dati all'incaricato individuato dall'ente (vedi paragrafo precedente) mezzo mail, cellulare, recapito ufficio, o personalmente
2. l'incaricato dello svolgimento del flusso deve raccogliere, prima dell'avvio del flusso, tutte le informazioni necessarie
3. l'incaricato procede con l'accesso nominativo al sistema MUA attraverso l'indirizzo web https://mua.secoges.com e avvia il flusso "Privacy – Data breach" secondo le istruzioni descritte nell'allegato 1 "Descrizione del flusso data breach"
4. l'incaricato deve rispondere alle domande del questionario presenti in MUA relative a:
    - identificazione e descrizione dell'evento
    - misure tecnologiche e organizzative applicate a protezione dei dati (prima, durante e dopo la violazione)

- informazioni relative ai soggetti individuati per la gestione della procedura; se necessario dovrà farsi affiancare nella sua compilazione da coloro che sono in possesso delle informazioni

5. conclusa la compilazione del questionario l'incaricato chiude il flusso, completandolo e passando l'incarico al DPO
6. *il flusso incarica il DPO, dello svolgimento della seconda parte del flusso*
7. il DPO riceve una mail dal sistema MUA che lo informa che è stato incaricato di svolgere la seconda parte del flusso
8. il DPO accede al sistema MUA attraverso l'indirizzo web https://mua.secoges.com dove trova evidenziato in rosso il pulsante "Attività da svolgere" e attiva il flusso attivo chiamato "Privacy – Data breach"
9. il DPO visualizza all'interno del sistema MUA le informazioni inserite durante la prima parte del flusso;
10. in base alle informazioni inserite il DPO valuta la necessità di fare comunicazione all'Autorità Garante e agli interessati e procede con la compilazione del questionario
11. il DPO procede fino alla chiusura del flusso in MUA:
    11.1. ***Caso A:*** **incidente da inserire nel registro incidenti**
        11.1.1. inserimento della violazione nel registro incidenti
        11.1.2. comunicazione da parte del DPO di chiusura dell'incidente
    11.2 ***Caso B (*****incidente da inserire nel registro incidenti e da notificare all'Autorità Garante (nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche)**
        11.2.1 inserimento della violazione nel registro incidenti
        11.2.2 generazione del modulo di comunicazione di Data Breach, che viene firmato dall'autore (DPO) con il sistema di firma di MUA
        11.2.3 trasmissione della comunicazione di chiusura della procedura da parte del DPO alla PEC protocollo@pec.comune.villachiara.bs.it
        11.2.4 acquisizione mediante download del modulo di segnalazione all'Autorità Garante nel seguente modo:
            - accedere alla sezione "Elementi d'analisi" alla voce "Regolamento

679/2016/UE - Data breach"

- posizionarsi sulla violazione/incidente inserito
- espandere la sezione "File allegati"
- cliccare sul documento da scaricare denominato "Modello di comunicazione al Garante-Data breach"
- la documentazione viene inviata anche mezzo mail agli indirizzi indicati durante lo svolgimento del flusso

11.2.5 sottoscrizione digitale (con firma elettronica qualificata/firma digitale) o con firma autografa (in questo caso il documento deve essere presentato unitamente alla copia del documento di identità del firmatario) da chi effettua la comunicazione

11.2.6 protocollazione del documento

11.2.7 invio tempestivo del documento mezzo pec all'indirizzo protocollo@pec.gpdp.it. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del Titolare del trattamento

11.3 ***Caso C*** **(incidente da inserire nel registro incidenti, da notificare all'Autorità Garante e da comunicare agli interessati (nel caso in cui la violazione comporti un rischio elevato per i diritti e la libertà delle persone fisiche)**

11.3.1 inserimento della violazione nel registro degli incidenti e invio notifica all'Autorità Garante come da punti da 11.2.1 a 11.2.7

11.3.2 comunicazione della violazione di dati personali all'interessato

ALLEGATO 1:

Descrizione del flusso data breach.