ALLEGATO 1

ISTRUZIONI FLUSSO DATA BREACH

1. Il data breach

Per data breach, ovvero nella versione italiana del GDPR, "violazione dei dati personali" si intende una 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".
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.

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/smarrimento di PC, Notebook, Tablet, Smartphone contenenti dati personali;
- erronea diffusione, pubblicazione o 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).

3. Modalità di avvio del flusso di gestione delle violazioni (data breach)

Avvio del flusso di gestione del data breach:

1. l'incaricato allo svolgimento del flusso dovrà raccogliere, prima dell'avvio del flusso, le informazioni che verranno richieste all'interno di quest'ultimo, oppure farsi affiancare nella sua compilazione da coloro che sono in possesso di queste informazioni;
2. l'incaricato accederà al sistema MUA attraverso l'indirizzo web https://asst-val.muacloud.it/;
3. l'incaricato inserirà le proprie credenziali di autenticazione;
4. l'incaricato cliccherà il pulsante all'interno della home page denominato "Workflow per ambito normativo";
5. l'incaricato cliccherà sul simbolo "+" accanto alla dicitura "Pacchetto GDPR – Enti Sanitari";
6. l'incaricato cliccherà sulla dicitura "Privacy – Data breach";
7. rispondere alle domande del questionario.

Descrizione del flusso del data breach

Step A. Identificazione e descrizione dell'evento:

Indicare la tipologia di comunicazione che si sta facendo all'Autorità Garante, il flusso chiederà che tipo di notifica si sta effettuando: • Preliminare (il Titolare del trattamento avvia una procedura di segnalazione senza avere un quadro completo della violazione e si riserva di effettuare una successiva notifica integrativa); • Completa; • Integrativa (il Titolare del trattamento integra una precedente modifica). Nel caso di notifica integrativa il flusso permetterà di importare le informazioni della preliminare. Se si sta

facendo una segnalazione integrativa il flusso richiederà, se noto, il numero di fascicolo assegnato alla precedente notifica dall'Autorità Garante.

Selezionare gli strumenti hardware, software o locali fisici oggetto della violazione/incidente (se il sistema non è ancora stato popolato con queste informazioni il flusso permetterà di inserire l'elemento che ha subìto la violazione). Se associati, il sistema permette di indicare quali trattamenti collegati all'elemento violato sono stati oggetto della violazione.
Nel caso in cui i collegamenti non siano stati ancora effettuati, il flusso dà la possibilità di indicare quali trattamenti sono stati oggetto di violazione.

Descrivere l'evento che ha condotto alla violazione subìta

Indicare quando è avvenuta la violazione

Indicare la data e l'ora in cui il Titolare del trattamento è venuto a conoscenza della violazione

Indicare le modalità con le quali il Titolare è venuto a conoscenza della violazione (per il tramite del responsabile del trattamento o in altro modo)

Indicare se nel trattamento sono coinvolti ulteriori soggetti esterni. Il flusso permette di scegliere un soggetto tra quelli presenti in elenco "Enti Esterni" oppure di inserire un nuovo soggetto.
Le informazioni che dovranno essere inserite sono:

- Denominazione (indicare il nome e cognome in caso di persona fisica);
- Codice fiscale/Partita Iva;
- Ruolo: Co-titolare, Responsabile esterno ai sensi dell'Art. 28, Rappresentante del Titolare non stabilito nell'Ue.

Indicare le possibili cause della violazione. Scegliere fra le possibilità presenti:

- Azione intenzionale interna;
- Azione accidentale interna;
- Azione intenzionale eterna;
- Azione accidentale esterna;
- Sconosciuta;
- Altro.

Scegliendo "Altro" il flusso permette di indicare altre possibili cause della violazione.

Indicare la natura della violazione scegliendo una o più delle seguenti risposte:

- Perdita di confidenzialità (diffusione/accesso non autorizzato o accidentale);
- Perdita di integrità (modifica non autorizzata o accidentale);

- Perdita di disponibilità (impossibilità di accesso, perdita, distruzione non autorizzata o accidentale).

Per ognuna delle risposte selezionate il flusso chiede di specificare ulteriormente la natura della violazione e indicare le possibili conseguenze della violazione sugli interessati (è possibile selezionare più di una risposta)

Indicare il volume dei dati violati (ad esempio il numero di referti, numero di record di un database, numero di transizioni registrate).
Se il numero non è conosciuto selezionare la voce "Un numero (ancora) non definito di dati".

Indicare il numero di interessati coinvolti nella violazione.
Se il numero non è conosciuto selezionare la voce "Un numero (ancora) sconosciuto di interessati".

Indicare le possibili categorie di interessati coinvolte nella violazione.
Nel caso in cui precedentemente siano stati individuati i trattamenti oggetto della violazione, il sistema riproporrà le relative categorie di interessati.
Nel caso in cui non siano stati selezionati i trattamenti, sarà necessario indicare le possibili categorie d'interessati, scegliendo dal menù in elenco (è possibile selezionare più di una risposta).

Step B: Misure tecnologiche e organizzative applicate a protezione dei dati (prima, durante e dopo la violazione)

Indicare le misure tecnologiche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti nella violazione.

Indicare le misure tecniche e organizzative adottate (o di cui si propone l'adozione futura) per porre rimedio alla violazione e ridurne gli effetti negativi per gli ingressati.

Nella descrizione distinguere fra le misure già adottate e quelle in corso di adozione.

Indicare le misure tecniche e organizzative adottate (o di cui si propone l'adozione futura) per prevenire simili violazioni future.

Step C. Ulteriori informazioni

Indicare il nominativo del soggetto deputato all'invio della notifica al Garante della Privacy (scegliere nel menù in elenco). Nel caso in cui queste informazioni non siano presenti nel sistema verranno richieste.

- Cognome e nome del segnalante;
- E-mail;
- Recapito telefonico per eventuali comunicazioni;
- Funziona rivestita.

Dati relativi al Titolare del trattamento

- Denominazione;
- Codice fiscale/Partita Iva;
- Stato;
- Indirizzo;
- CAP;
- Città;
- Provincia;
- E-mail;
- Pec.

Il flusso incarica il DPO, dello svolgimento della seconda parte del flusso. Coloro che verranno incaricati riceveranno una comunicazione tramite mail dell'avvenuto incarico.

Se le persone incaricate fossero più di una, il primo che avvierà il flusso ne otterrà l'incarico esclusivo notificando agli altri utenti l'avvenuta presa in carico.

Step D. Comunicazione della violazione

In base alle informazioni inserite il DPO valuta la necessità di fare comunicazione all'Autorità Garante. Qualora si voglia notificare la violazione al Garante, il sistema genera il documento sulla base del modello predisposto dall'Autorità Garante.

In ogni caso, il sistema registra tutte le informazioni al fine di implementare il registro delle violazioni

↓

Indicare se la comunicazione è effettuata ai sensi:

- Dell'Art.33 Gdpr;
- Dell'Art. 26 D.lgs 51/2018

↓

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione.
Nel caso in cui sia stato individuato il DPO indicare il numero di protocollo assegnato alla comunicazione all'Autorità Garante dei dati di contatto del DPO.
In alternativa, indicare il soggetto da contattare:

- Cognome e Nome;
- E-mail;
- Recapito telefonico per eventuali comunicazioni;
- Funzione rivestita.

↓

Nel caso in cui la comunicazione venga effettuata oltre le 72 ore, il flusso chiederà di motivare il ritardo.

↓

Descrivere l'incidente alla base della violazione

↓

Descrivere le categorie di dati personali oggetto della violazione

Indicare tipologie di dati coinvolti nella violazione.
Se durante la prima parte del flusso sono stati selezionati dei trattamenti, il flusso leggerà e preselezionerà le tipologie di dati già indicate sul trattamento.

Indicare per ogni tipo di dato scelto o collegato ai trattamenti coinvolti nella violazione le specifiche categorie di dati.

Indicare la stima della violazione.
Indicare le motivazioni della scelta.

Step E. Comunicazione agli interessati

Indicare i potenziali effetti negativi sugli interessati della violazione.

- Se si seleziona uno dei rischi in elenco il flusso chiederà di indicare se ci sono delle motivazioni per cui non deve essere fatta comunicazione agli interessati. Per ognuna delle voci selezionate indicare le motivazioni.
- Se tra le voci si seleziona "Nessun rischio", il flusso dirà che non vi è necessità di fare comunicazione agli interessati.
- Se si seleziona uno dei rischi presente in elenco, ma se non sono presenti le condizioni per cui non vi è necessità di fare comunicazione, il flusso indicherà che non vi è la necessità di effettuare la comunicazione agli interessati.

Nel caso si sia presa la decisione di effettuare la comunicazione agli interessati inserire il testo della comunicazione che si intende dare agli interessati.

Nel caso si sia presa la decisione di effettuare la comunicazione agli interessati indicare la modalità con cui è stata data o si darà comunicazione agli interessati.

Nel caso si sia presa la decisione di effettuare la comunicazione agli interessati il flusso genererà il documento da inviare agli interessati.

Nel caso si sia presa la decisione di fare comunicazione all'Autorità Garante verrà generato il *facsimile* di comunicazione di data breach.

Il flusso invierà la documentazione generata agli indirizzi mail dichiarati. La documentazione generata sarà scaricabile accedendo alla sezione "Elementi d'analisi" alla voce "Regolamento 679/2016/UE - Data breach", selezionare l'evento per cui si intende scaricare la documentazione, che sarà presente nella sezione "File allegati".
Nel caso in cui sia stato valutato di non effettuare la notifica all'Autorità Garante verrà comunque inviata notifica della conclusione del flusso e della decisione di non fare comunicazione

all’Autorità Garante.

Indicare gli indirizzi e-mail a cui sarà inviata l’eventuale documentazione generata dal flusso e la comunicazione di conclusione del flusso.

Step F. Chiusura dell’incidente

Descrivere il modo di risoluzione della violazione/incidente, nel caso sia stato risolto.

Indicare la data di risoluzione della violazione/incidente, nel caso sia stato risolto.