FLUSSO DI NOTIFICA DI *DATA BREACH*

Nel presente documento è descritto il flusso di notifica delle violazioni dei dati personali che presentano un rischio per i diritti e le libertà delle persone fisiche (*Data Breach*) in conformità a quanto previsto dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("Regolamento Generale sulla Protezione dei Dati" - d'ora in avanti "RGPD").

Ai sensi dell'articolo 4 del RGPD per "violazione dei dati personali" 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.

Il flusso inizia con l'identificazione di una possibile "violazione dei dati personali" nell'ambito della gestione di un evento di sicurezza e si conclude con l'invio della notifica di avvenuto *Data Breach* all'Amministrazione Titolare affinché quest'ultima possa adempiere agli obblighi previsti dagli articoli 33 e 34 del RGPD.

Il flusso prevede l'interazione e lo scambio di informazioni tra Sogei, il Responsabile Protezione Dati della stessa (d'ora in avanti "RPD"), l'Amministrazione Titolare interessata dall'evento e il RPD della stessa, al fine di consentire all'Amministrazione Titolare di adempiere alle prescrizioni previste dal RGPD.

1. DESCRIZIONE DEL FLUSSO

Il flusso di notifica all'Amministrazione Titolare prevede i passi di seguito elencati.

- Il CERT Sogei (struttura aziendale preposta al trattamento degli incidenti di sicurezza informatica), nel corso della gestione di un incidente di sicurezza, rileva una possibile "violazione dei dati personali". Il CERT Sogei comunica all'Amministrazione Titolare e al RPD della stessa che è in corso la valutazione di un incidente di sicurezza, fornendo, altresì, una prima sommaria descrizione dell'incidente e assegnando un identificativo univoco allo stesso. Il CERT Sogei invia le informazioni scrivendo a USSRI@pec.mite.gov.it, ITC@pec.mite.gov.it e rpd@pec.minambiente.it. Nel caso in cui sia l'Amministrazione Titolare a venire a conoscenza di un incidente di sicurezza

caratterizzato da una possibile "violazione dei dati personali" che necessita dell'intervento di Sogei, l'Amministrazione Titolare informa il CERT Sogei e il proprio RPD scrivendo a cert@sogei.it e ufficiodpo@sogei.it. Il CERT Sogei avvia la verifica fornendo eventualmente informazioni aggiuntive a quelle ricevute e assegnando un identificativo unico all'incidente.

- Il CERT Sogei verifica la presenza o meno della "violazione di dati personali".
- In caso di esito negativo della verifica, il CERT Sogei termina il processo, comunicando all'Amministrazione Titolare ed al suo RPD la chiusura dell'incidente caratterizzato dall'identificativo precedentemente comunicato e le motivazioni.
- In caso di esito positivo della verifica (ossia è stata accertata la "violazione di dati personali" ed è stata valutata la gravità dell'evento da intendersi come la stima del potenziale impatto sugli interessati derivante dalla violazione), il CERT Sogei comunica immediatamente e senza ingiustificato ritardo e in modo dettagliato il *Data Breach* all'Amministrazione Titolare e contestualmente al relativo RPD, riportando le informazioni di propria competenza, indicate nel successivo paragrafo 2. La suddetta comunicazione viene inviata dalla casella PEC del CERT Sogei (cert@pec.sogei.it) verso le caselle PEC dell'Amministrazione Titolare e del RPD della stessa o, laddove non disponibili, verso le caselle di posta elettronica ordinaria di questi ultimi.
- l'Amministrazione Titolare, ricevuta la notifica di *Data Breach* e sentito il proprio RPD, valuta il livello di gravità della "violazione di dati personali" proposto da Sogei. Nel caso in cui la "violazione di dati personali" comporti un rischio per i diritti e le libertà delle persone fisiche, provvede a completare la notifica con le informazioni di propria competenza e ad inviare la stessa all'Autorità di Controllo entro 72 ore dalla conoscenza dell'avvenuta compromissione dei dati personali, dandone contestualmente riscontro al CERT Sogei e al RPD di quest'ultima. Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, provvede, altresì, a corredarla con le motivazioni del ritardo.

Eventuali richieste di ulteriori informazioni o modifiche alla notifica all'Autorità di Controllo, necessarie durante le attività di risoluzione dell'incidente, saranno concordate tra l'Amministrazione Titolare, il CERT Sogei e i rispettivi RPD.

Il CERT Sogei dovrà mantenere un'accurata documentazione di tutte le "violazioni di dati personali" registrate, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione sarà integrata con le eventuali azioni intraprese dall'Amministrazione Titolare e opportunamente comunicate al CERT Sogei.

2. CONTENUTI DELLA NOTIFICA DI DATA BREACH ALL'AMMINISTRAZIONE TITOLARE

Le informazioni previste dal RGPD saranno raccolte e riportate nella notifica di avvenuto *Data Breach*.

Il CERT Sogei utilizzerà il modulo disponibile sul sito dell'Autorità di Controllo per fornire le informazioni necessarie all'Amministrazione Titolare, comprendenti almeno le seguenti:

- tipologia di incidente;
- descrizione del servizio impattato e/o della banca/banche dati oggetto di violazione di dati personali;
- intervallo temporale dell'incidente;
- luogo dell'incidente;
- misure tecniche di sicurezza applicate ai dati violati;
- misure attivate per il contenimento e la prevenzione;
- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- descrizione della probabile conseguenza della violazione dei dati personali;
- descrizione delle misure di sicurezza adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.