Flusso di notifica di *Data Breach* all'Autorità di Controllo

Di seguito si riporta una descrizione del flusso di notifica delle violazioni dei dati personali che presentino 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 all'Autorità di Controllo della notifica di avvenuto *Data Breach* secondo quanto previsto dal RGPD (riferimento artt. 33 e 34).

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'Autorità di Controllo da parte dell'Amministrazione Titolare prevede i seguenti passi:

1. Il CERT Sogei (ossia la 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 (*Data Breach*). Il CERT Sogei notifica dell'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. 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 (*Data Breach*) che necessita dell'intervento di Sogei, l'Amministrazione Titolare informa il CERT Sogei e il proprio RPD. Il CERT Sogei avvia la verifica fornendo all'Amministrazione Titolare tutte le informazioni necessarie ai fini della valutazione dell'eventuale violazione e assegnando un identificativo unico ad esso.

2. Il CERT Sogei verifica la presenza o meno della violazione di dati personali.

3. In caso di esito negativo della verifica, il CERT Sogei termina il processo, notificando all'Amministrazione Titolare e al relativo RPD la chiusura

dell'incidente caratterizzato dall'identificativo precedentemente comunicato e le motivazioni.

4. In caso di esito positivo della verifica (ossia è stata accertata la violazione dei 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 informa immediatamente e senza ritardo la propria competente struttura di vertice (Direttore Security, Safety e Industrial Relations). Quest'ultima, senza ingiustificato ritardo e in modo dettagliato comunica il *Data Breach* all'Amministrazione Titolare e contestualmente al relativo RPD, completando le informazioni di propria competenza di cui al successivo paragrafo 2 e trasmettendone la notifica all'Amministrazione Titolare.

5. L'Amministrazione Titolare, ricevuta la notifica di *Data Breach*, sentito il proprio RPD e assistito dal CERT Sogei, valuta il livello di gravità della violazione dei dati personali, proposto da Sogei stessa, avvenuta sui dati personali contenuti nelle banche dati disponibili nella propria titolarità. Nel caso in cui la violazione dei 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, di cui al successivo paragrafo 2 e ad inviare la stessa all'Autorità di Controllo entro 72 ore dalla conoscenza dell'avvenuta compromissione dei dati personali, dandone contestualmente riscontro alla struttura di vertice Sogei (Direttore Security, Safety e Industrial Relations) 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'evento saranno concordate tra il Titolare e il Responsabile del trattamento 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 connesse, le relative conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione sarà integrata con le eventuali azioni intraprese dall'Amministrazione Titolare e opportunamente comunicate allo stesso.

2. NOTIFICA ALL'AUTORITA' DI CONTROLLO DESIGNATA ANCHE AI FINI DELL'ATTUAZIONE DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI (UE) 2016/679 (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI)

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

Il CERT Sogei inserirà nella notifica le seguenti informazioni, che saranno comunicate all'Amministrazione Titolare:

- 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;
- circostanze 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;
- proposta di comunicazione di violazione di dati personali all'/agli interessato/i in base ad un'analisi della gravità della violazione (qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche) e non ricorrendo alcuna delle condizioni di cui all'articolo 34, comma 3, del RGPD, che escludono la necessità di comunicazione della violazione all'interessato.

È a cura dell'Amministrazione Titolare inserire nella successiva comunicazione all'Autorità di Controllo le seguenti informazioni necessarie:

- nome e dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
- validazione ed eventuale integrazione della descrizione del CERT Sogei di una probabile conseguenza della violazione dei dati personali;
- eventuale ulteriore integrazione delle misure di sicurezza adottate da Sogei e di quelle, indicate dal CERT Sogei, adottate o di cui si propone l'adozione da parte dell'Amministrazione Titolare per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- dati organizzativi di riferimento e relativi recapiti dell'Amministrazione Titolare;
- livello di gravità della violazione;
- eventuale comunicazione agli interessati e relative modalità;
- qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, le motivazioni del ritardo.

Il Titolare notificherà la violazione all'Autorità di Controllo comunicando le informazioni previste dall'art. 33 paragrafo 3 del Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 ed indicate nel provvedimento del Garante sulla notifica delle violazioni dei dati personali pubblicato sul sito della predetta Autorità, dandone comunicazione anche al CERT Sogei.