Consiglio di Stato-Tribunali Amministrativi Regionali

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

Qui 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 (riferimenti artt. 33 e 34).

Il flusso prevede l'interazione e lo scambio di informazioni tra la Società…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. *La Società* …che nel corso della gestione di un incidente di sicurezza, rileva una possibile "violazione dei dati personali" (*Data Breach*) *notifica* all'Amministrazione Titolare (competente struttura di sicurezza informatica o struttura equivalente della stessa) e al RPD della stessa che è in corso la valutazione di un incidente di sicurezza, fornendo, altresì, una prima sommaria descrizione dell'incidente ed assegnando un identificativo univoco allo stesso. Nel caso in cui sia l'Amministrazione Titolare a rilevare un incidente di sicurezza, caratterizzato da una possibile "violazione dei dati personali" (*Data Breach*), che necessita dell'intervento della *Società,* la competente struttura di sicurezza informatica (o struttura equivalente) dell'Amministrazione informa *la Società* e il proprio RPD. *La Società* avvia la verifica fornendo eventualmente informazioni aggiuntive a quelle ricevute ed assegnando un identificativo unico ad esso.
2. *La Società* verifica la presenza o meno della "violazione di dati personali".
3. In caso di esito negativo della verifica, *la Società* termina il processo, notificando all'Amministrazione Titolare (competente struttura di sicurezza informatica o struttura equivalente della stessa) 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 acclarata la "violazione dei dati personali"), *la Società* informa immediatamente e senza ritardo la propria competente struttura di vertice Quest'ultima, senza ingiustificato ritardo e in modo dettagliato, comunica il *Data Breach* all'Amministrazione Titolare (competente struttura di sicurezza informatica o struttura

equivalente) e, contestualmente, al RPD della stessa e al RPD *della Società*, completando le informazioni di propria competenza di cui al successivo paragrafo 2 e trasmettendone la notifica all'Amministrazione Titolare.

5. L'Amministrazione Titolare che ha ricevuto la notifica di "*Data Breach*", sentito il proprio RPD, valuta il livello di gravità della "violazione dei dati personali". avvenuta sui dati personali contenuti nelle banche dati disponibili nella propria titolarità. Nel caso in cui la "violazione dei dati personali" comporta 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 *della Società* 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 l'Amministrazione Titolare, la struttura di vertice *della Società* e i rispettivi RPD.

La Società 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 allo stesso.

2. Notifica all'autorità di controllo

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

La Società inserirà nella notifica le seguenti informazioni, ove note, 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;
- 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 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;

a cura dell'Amministrazione Titolare dovranno essere inserite nella successiva comunicazione all'Autorità di Controllo le informazioni previste all'articolo 33, paragrafo 3, del Regolamento e indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali.