VIOLAZIONE DEI DATI PERSONALI
Istruzioni operative per gli enti locali

A domanda risponde Avv. Michele IASELLI

12 Settembre 2019 - dalle ore 15.00 alle 16.00

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54
Web: www.dpoinrete.it
www.asmel.eu

I dati personali conservati, trasmessi o trattati da pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

L’art. 33 del Regolamento dispone che in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 55 senza ingiustificato ritardo, 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. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata (Data breach).

Tale notifica deve come minimo:
a) descrivere la 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;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Garante per la protezione dei dati personali già per il passato aveva adottato una serie di provvedimenti che introducevano in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali *(data breach*) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati.

Provvedimento del Garante n. 161 del 4 aprile 2013 con il quale viene prescritto l'obbligo di comunicazione al Garante (mediante un apposito modello di comunicazione) da parte dei fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli internet point, le reti aziendali).

Provvedimento n. 513 del 12 novembre 2014 dove viene previsto che entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

Provvedimento n. 331 del 4 giugno 2015 dove viene sancito che entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

Provvedimento del 2 luglio 2015 “Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche” con il quale il Garante prescrive, ai sensi dell'articolo 154, comma 1, lett. c), del Codice in materia di protezione dei dati personali, che le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 devono comunicare all’Autorità, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possono avere un impatto significativo sui dati personali contenuti nelle proprie banche dati e che tali comunicazioni dovevano essere redatte secondo uno schema specifico allegato al provvedimento e inviate tramite posta elettronica o posta elettronica certificata.

Proprio di recente il Garante con un Provvedimento del 30 luglio 2019 ha predisposto un modello di notifica che forma parte integrante del provvedimento ed ha sancito che i termini temporali, il contenuto e le modalità della comunicazione delle violazioni di dati personali indicati nei provvedimenti precedenti si intendono eliminati e sostituiti dai termini indicati nel GDPR e ripresi dal Provvedimento stesso.

Con quali modalità deve essere effettuata la notifica?

a) sottoscritta mediante una delle forme di cui all’articolo 20 del CAD

b) ovvero, quando l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), nonché attraverso uno degli altri strumenti di cui all'articolo 64, comma 2-nonies, nei limiti ivi previsti;

c) sottoscritta e presentata unitamente alla copia del documento d'identità;

c-bis) trasmessa dall'istante o dal dichiarante dal proprio domicilio digitale purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con Linee guida, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato.

L’art. 34, invece, prevede un’altra importante incombenza collegata alla precedente e cioè la comunicazione di una violazione dei dati personali all’interessato.
Difatti, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La predetta comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e non è richiesta se:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Modello di notifica del Garante

Policy da adottare in caso di data breach

Privacy e Trasparenza

Nell’ambito della P.A. assume grande rilevanza la delicata problematica rappresentata dal possibile conflitto tra due interessi di rango primario che, in quanto tali, devono ritenersi entrambi meritevoli di costante ed adeguata tutela da parte dell’ordinamento giuridico: quello all’informazione, che si realizza attraverso l’esercizio del diritto di accesso alla documentazione amministrativa e riposa sull’esigenza di trasparenza ed imparzialità dell’azione amministrativa; e quello alla riservatezza dei soggetti terzi, che inerisce alla sfera degli assetti privatistici e si traduce, in ultima analisi, nella necessità di garantire la segretezza di quelle particolari categorie di dati disciplinate dagli artt. 9 e 10 del GDPR.

La giurisprudenza amministrativa ha elaborato un indirizzo interpretativo che privilegia il diritto di accesso, considerando per converso recessivo l'interesse alla riservatezza dei terzi, quando l'accesso stesso sia esercitato per la difesa di un interesse giuridico, nei limiti in cui esso sia necessario alla difesa di quell'interesse (cfr. Cons. Stato, Sez. VI, 20 aprile 2006, n. 2223).

Ma nella Pubblica Amministrazione l'atteggiamento rispetto al trattamento dei dati e delle banche dati è molto cambiato negli ultimi 20 anni, da mero adempimento si è passati ad una dimensione molto più proattiva, perché i dati e talora anche i dati personali escono sempre di più dagli uffici attraverso processi legislativi che tengono conto del loro valore economico. La PA, che fino a qualche tempo fa, gestiva passivamente i dati, oggi vuole renderli sempre più disponibili e trasparenti.

L’art. 7-bis del d.lgs n. 33/2013 nel disciplinare il riutilizzo dei dati pubblicati regola necessariamente i rapporti con la normativa in materia di protezione dei dati personali chiarendo che gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari, di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196 (norma ormai abrogata), comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo ai sensi dell'articolo 7 nel rispetto dei principi sul trattamento dei dati personali.

Si precisa, inoltre, che la pubblicazione nei siti istituzionali di dati relativi a titolari di organi di indirizzo politico e di uffici o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi è finalizzata alla realizzazione della trasparenza pubblica, che integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali sebbene la Corte Costituzionale con sentenza 23 gennaio - 21 febbraio 2019, n. 20 abbia dichiarato l'illegittimità costituzionale della disposizione dell'art. 14, comma 1-bis, del d.lgs. n. 14 marzo 2013, n. 33 nella parte in cui prevede che le pubbliche amministrazioni pubblicano i dati di cui all'art. 14, comma 1, lettera f), dello stesso decreto legislativo anche per tutti i titolari di incarichi dirigenziali, a qualsiasi titolo conferiti, ivi inclusi quelli conferiti discrezionalmente dall'organo di indirizzo politico senza procedure pubbliche di selezione.

La norma ancora prevede che nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

Di conseguenza anche alla luce del GDPR sono ancora da ritenere illuminanti le Linee guida (provvedimento del 15 maggio 2014), con cui il Garante privacy è intervenuto proprio per assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione sul web di atti e documenti.

In particolare prima di procedere alla pubblicazione sul proprio sito web la P.A. deve:

- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;
- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;
- sottrarre all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) i dati sensibili e giudiziari.