Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]

***ATTENZIONE: A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità pubblicato all'indirizzo https://servizi.gpdp.it/**

VEDI ANCHE: Deliberazione del 27 maggio 2021

[doc. web n. 9126951]

Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]

Registro dei provvedimenti
n. 157 del 30 luglio 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» (di seguito "Codice");

VISTO il decreto legislativo 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito "d.lgs. n. 51/2018");

CONSIDERATO che 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 (art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del d.lgs. n. 51/2018);

VISTE le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018;

VISTA la Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adottata ai sensi dell'art. 64 del Regolamento, dal Comitato europeo per la protezione dei dati in data 12 marzo 2019;

RILEVATO che in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante 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 (artt. 33 e 55 del Regolamento, art. 2-bis del Codice);

RILEVATO che il titolare del trattamento è tenuto altresì a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero (artt. 26 e 37, comma 6, del d.lgs. n. 51/2018);

CONSIDERATO che al Garante è attribuito il compito di promuovere la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal Regolamento e dal d.lgs. n. 51/2018 (art. 57, par. 1, lett. d, del Regolamento; art. 37, comma 2, lett. b, del d.lgs. n. 51/2018);

RITENUTO opportuno, in un'ottica di semplificazione del corretto adempimento degli obblighi amministrativi posti in capo al titolare del trattamento, indicare le informazioni da fornire al Garante, in caso di violazione dei dati personali, nella notifica di cui all'art. 33 del Regolamento, le quali sono individuate nell'allegato modello, che forma parte integrante del presente provvedimento;

CONSIDERATO, altresì, che in relazione a determinate tipologie di trattamento o categorie di titolari del trattamento, ai sensi della disciplina previgente l'applicazione del Regolamento, sono stati prescritti termini temporali, contenuto e modalità della comunicazione delle violazioni di dati personali, in particolare nel provvedimento sulle misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche del 2 luglio 2015 (v. punto 1, in www.gpdp.it, doc. web n. 4129029); nelle linee guida in materia di Dossier sanitario del 4 giugno 2015 (v. punto 2, doc. web n. 4084632); nel provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 (v. punto 2, doc. web n. 3556992); nel provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali del 4 aprile 2013 (doc. web n. 2388260), nonché nel provvedimento recante prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie del 12 maggio 2011 (v. punto 5.2, doc. web n. 1813953);

RITENUTO, alla luce dell'art. 33 del Regolamento, che le diverse informazioni da comunicare al Garante come previste nei provvedimenti e nelle linee guida citati devono intendersi eliminate e sostituite da quelle indicate nel paragrafo 3 del medesimo articolo e nel presente provvedimento,

RITENUTO che pure i diversi termini previsti nei provvedimenti e nelle linee guida summenzionati devono intendersi eliminati e sostituiti da quelli stabiliti dall'art. 33 del Regolamento, per cui la notifica al Garante dovrà essere effettuata dal titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza della violazione dei dati personali, con le modalità di cui all'art. 65 del d.lgs. 7 marzo 2005, n. 82 (recante il «Codice dell'amministrazione digitale»), mediante i sistemi telematici indicati nel sito istituzionale del Garante;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Antonello Soro;

TUTTO CIO' PREMESSO

ai sensi dell'art. 57, par. 1, lett. d), del Regolamento e dell'art. 37, comma 2, lett. b), del d.lgs. n. 51/2018:

a) i soggetti tenuti alla notifica delle violazioni dei dati personali forniscono al Garante, nell'adempiere all'obbligo previsto dall'art. 33 del Regolamento e dall'art. 26 del d.lgs. n. 51/2018, le informazioni di cui all'allegato modello, che forma parte integrante del presente provvedimento, con le modalità di cui all'art. 65 del d.lgs. n. 82/2005, mediante i sistemi telematici indicati nel sito istituzionale del Garante;

b) i termini temporali, il contenuto e le modalità della comunicazione delle violazioni di dati personali indicati nel provvedimento sulle misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche del 2 luglio 2015 (punto 1), nelle linee guida in materia di Dossier sanitario del 4 giugno 2015 (punto 2), nel provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 (punto 2); nel provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali del 4 aprile 2013, nonché nel provvedimento recante prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie del 12 maggio 2011 (punto 5.2), si intendono eliminati e sostituiti dalla lett. a) del presente provvedimento, secondo i termini di cui in motivazione.

Roma, 30 luglio 2019

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia