Roma, 16.09.2019

Ufficio: DOR/PF
Protocollo: 201900007561/AG
Oggetto: Provvedimento del Garante sulla notifica delle violazioni dei dati personali - 30 luglio 2019.
Circolare n. 11714
4.1
IFO SI

AI PRESIDENTI DEGLI ORDINI
DEI FARMACISTI

e p.c. AI COMPONENTI IL COMITATO
CENTRALE DELLA F.O.F.I.

LORO SEDI

Provvedimento Garante su notifica violazione dei dati personali.

Si fa seguito alle circolari federali nn. 11225 del 20 novembre 2018, nn. 10907 del 4 aprile 2018 e 11453 del 3 aprile u.s., per informare che il Garante della Privacy, con provvedimento del 30 luglio 2019 [9126951] (cfr. all. 1), ha indicato le informazioni da fornire, in caso di violazione dei dati personali (cd. *data breach*), nella notifica di cui all'art. 33 del Regolamento UE 2016/679.

Nella scheda allegata (cfr. all. 2), in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento (UE) 2016/679, si specificano i seguenti punti:

COSA E' UNA VIOLAZIONE DEI DATI PERSONALI (data breach)?

La violazione dei dati personali è 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;

Alcuni possibili esempi:

- ✓ l'accesso o l'acquisizione dei dati personali da parte dei terzi non autorizzati;
- ✓ il furto o la perdita di dispositivi informatici (PC portatili, telefonini aziendali) contenenti dati personali;
- ✓ la deliberata alterazione di dati personali;
- ✓ l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- ✓ la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- ✓ la divulgazione non autorizzata dei dati personali.

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

In caso di violazione dei dati personali, il titolare del trattamento (quindi, anche gli Ordini provinciali e i titolari di farmacie e parafarmacie) 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.

Inoltre, il titolare del trattamento, a prescindere dalla notifica al Garante, deve annotare tutte le violazione dei dati personali, ad esempio predisponendo un apposito registro.

CHE TIPO DI VIOLAZIONI DI DATI PERSONALI VANNO NOTIFICATE?

Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

CHE INFORMAZIONI DEVE CONTENERE LA NOTIFICA AL GARANTE?

La notifica deve contenere le informazioni previste all'art. 33, par. 3, del Regolamento (UE) 2016/679 e indicate nell'allegato al Provvedimento del Garante in oggetto.

In particolare, la notifica deve almeno:

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.

Qualora si utilizzi per la notifica il modello allegato al provvedimento (cfr. all. 3), è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione.

COME INVIARE LA NOTIFCA AL GARANTE?

La notifica deve essere inviata al Garante tramite posta elettronica all'indirizzoprotocollo@pec.gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa.

LE AZIONI DEL GARANTE

L'Autorità può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative

applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale.

Cordiali saluti.

IL SEGRETARIO
(Dr. Maurizio Pace)

IL PRESIDENTE
(On. Dr. Andrea Mandelli)

All. 3