PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4207 di Giovedì 29 marzo 2018

Linee guida per i responsabili della protezione dei dati

Disponibile l'aggiornamento 2018 della Guida applicativa Nuovo Regolamento Ue 2016/679 sulla protezione dei dati personali.

Il Garante per la protezione dei dati personali mette a disposizione l'**aggiornamento 2018** della Guida all'applicazione del Regolamento UE 2016/679 in materia di protezione dei dati personali.

Il documento - che traccia un quadro generale delle principali innovazioni introdotte dal Regolamento e fornisce indicazioni utili sulle prassi da seguire e gli adempimenti da attuare per dare corretta applicazione alla normativa - è stato in parte modificato e integrato alla luce dell'evoluzione della riflessione a livello nazionale ed europeo. Il testo potrà subire ulteriori aggiornamenti, allo scopo di offrire sempre nuovi contenuti e garantire un aggiornamento costante.

La guida è disponibile sul sito del Garante www.garanteprivacy.it in formato ipertestuale navigabile e in pdf scaricabile.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[USBGDPR] ?#>

Guida all'applicazione del Regolamento UE 2016/679

Il regolamento generale sulla protezione dei dati (RGPD) [1], che esplicherà i propri effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (accountability). I responsabili della protezione dei dati (RPD) saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del RGPD.

In base al RGPD, alcuni titolari del trattamento e responsabili del trattamento sono tenuti a nominare un RPD [2]. Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali.

Anche ove il regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia gli approcci di questo genere.

La figura del RPD non costituisce una novità assoluta. La direttiva 95/46/CE [3] non prevedeva alcun obbligo di nomina di un RPD, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni.

Ancor prima dell'adozione del RGPD, il Gruppo di lavoro ha sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del RPD possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese [4]. Oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.

I RPD non rispondono personalmente in caso di inosservanza del RGPD. Quest'ultimo chiarisce che spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, paragrafo 1). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

Inoltre, al titolare del trattamento o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il responsabile della protezione dei dati è preposto. La nomina di un RPD è solo il primo passo, perché il RPD deve disporre anche di autonomia e risorse sufficienti per svolgere in modo efficace i propri compiti.

Il RGPD riconosce nel RPD uno degli elementi chiave all'interno del nuovo sistema di governance dei dati, e prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici. Le presenti linee guida intendono fare chiarezza sulle pertinenti disposizioni del regolamento al fine di favorire l'osservanza della normativa da parte di titolari del trattamento e responsabili del trattamento; inoltre, le linee guida vogliono essere di ausilio ai RPD nell'esecuzione dei compiti loro attribuiti. Il presente documento contiene anche alcune raccomandazioni, in termini di migliori prassi, che scaturiscono dall'esperienza accumulata in alcuni Stati membri. Il Gruppo di lavoro monitorerà l'attuazione delle linee guida qui presentate e provvederà alle integrazioni che si riveleranno opportune.

Introduzione

2. Nomina di un RPD

2.1. Nomina obbligatoria

2.1.1. "AUTORITÀ PUBBLICA O ORGANISMO PUBBLICO"

"ATTIVITÀ PRINCIPALI"

2.1.3. "LARGA SCALA"

2.1.4. "MONITORAGGIO REGOLARE E SISTEMATICO"

2.1.5. CATEGORIE PARTICOLARI DI DATI E DATI RELATIVI A CONDANNE PENALI E A REATI

2.2. RPD del responsabile del trattamento

2.3. Designazione di un unico RPD per più organismi

2.4. Accessibilità e localizzazione del RPD

2.5. Conoscenze e competenze del RPD

2.6. Pubblicazione e comunicazione dei dati di contatto del RPD

3. Posizione del RPD

3.1. Coinvolgimento del RPD in tutte le questioni riguardanti la protezione dei dati personali

3.2. Risorse necessarie

3.3. Istruzioni e [significato di] "adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente"

3.4. Rimozione o penalizzazioni in rapporto all'adempimento dei compiti di RPD

3.5. Conflitto di interessi

4. Compiti del RPD

4.1. Sorvegliare l'osservanza del RGPD

4.2. Il ruolo del RPD nella valutazione di impatto sulla protezione dei dati

4.3. Cooperazione con l'autorità di controllo e funzione di punto di contatto

4.4. Approccio basato sul rischio

4.5. Il ruolo del RPD nella tenuta del registro delle attività di trattamento

5. ALLEGATO ALLE LINEE GUIDA SUL RPD ? INDICAZIONI ESSENZIALI

1. Chi è tenuto a designare un RPD?

2. Cosa significa "attività principali"?

3. Cosa significa "su larga scala"?

4. Cosa significa "monitoraggio regolare e sistematico"?

5. E' ammessa la designazione congiunta di uno stesso RPD da parte di più soggetti? E a quali condizioni?

6. Dove dovrebbe collocarsi il RPD?

7. Si può designare un RPD esterno?

8. Quali sono le qualità professionali che un RPD deve possedere?

Posizione del RPD

9. Quali sono le risorse che titolare del trattamento o responsabile del trattamento dovrebbero mettere a disposizione del RPD?

10. Quali sono le garanzie che possono consentire al RPD di operare con indipendenza? Cosa significa "conflitto di interessi"?

Compiti del RPD

11. Che cosa si intende per "sorvegliare l'osservanza"

12. Il RPD è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati?

13. Quale ruolo spetta al RPD con riguardo alla valutazione di impatto sulla protezione dei dati e alla tenuta del registro dei trattamenti?

Tratto da:

Guida all'applicazione del Regolamento UE 2016/679 (pdf)

---

[1] 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) (GU L 119, 4.5.2016). Il RGPD è rilevante ai fini del SEE e sarà applicabile una volta incorporato nell'Accordo relativo al SEE.

[2] La nomina di un RPD è obbligatoria anche con riguardo alle autorità competenti di cui all'articolo 32 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 ai 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 (GU L 119, 4.5.2016), alla luce della normativa nazionale di recepimento. Le presenti linee guida guardano con particolare attenzione alla figura del RPD come prevista dal RGPD, ma le indicazioni in esse formulate valgono anche per i RPD previsti dalla direttiva 2016/680 con riferimento alle disposizioni di carattere analogo contenute nei due strumenti.

[3] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GU L 281, 23.11.95).

[4] Si veda
http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150617_appendix_core_issues_ple

Questo articolo è pubblicato sotto una Licenza Creative Commons.