

8 mayo 2018

Il Garante per la protezione dei dati ha messo a disposizione un software per la realizzazione di una valutazione d'impatto sulla protezione dei dati

Milano, 07 maggio 2018 - Il Garante per la protezione dei dati ha messo a disposizione un software per la realizzazione di una valutazione d'impatto sulla protezione dei dati ('DPIA', Data Privacy Impact Assessment) secondo le prescrizioni del Regolamento UE 679/2016 e le indicazioni fornite dal WP29 (Il Gruppo Art. 29, ovvero il gruppo dei Garanti europei della privacy) nelle proprie Linee-guida. Si tratta della versione in lingua italiana del software già elaborato dal CNIL, l'autorità francese per la protezione dei dati, nel gennaio 2018.

Il tool è stato pensato come un percorso guidato per le realtà di piccole-medie dimensioni, per fotografare e gestire i trattamenti dei dati con rischio elevato. Quindi, come specificato dal Garante, si tratta di un supporto di orientamento allo svolgimento di un DPIA da non intendere "come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate".

Il Garante ha inserito nel proprio sito il collegamento per scaricare gratuitamente il software (<https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>) nonché, per facilitare l'utilizzo del DPIA software, il relativo tutorial.

Il Garante ricorda che la valutazione d'impatto sulla protezione dei dati implica la verifica della rischiosità complessiva che il trattamento previsto può comportare per i diritti e le libertà degli interessati, le azioni intraprese e la rischiosità residua: conseguentemente, "il concetto di rischio non si esaurisce nella considerazione delle possibili violazioni o minacce della sicurezza dei dati".

Come ormai noto, il DPIA costituisce un importante strumento in termini di responsabilizzazione (il c.d. *principio di accountability*) poiché consente al Titolare del trattamento di dimostrare l'adozione di misure adeguate nella propria attività di trattamento in conformità con le nuove norme in materia di protezione dei dati personali, pena l'applicazione di sanzioni amministrative fino a 10 milioni di euro. Ai sensi dell'art. 35 del GDPR, il DPIA va effettuato in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il WP29, con le sue Linee-guida, ha individuato nove criteri specifici da cui far discendere l'obbligatorietà del DPIA: qualora un trattamento comprenda almeno due dei nove rischi individuati, è necessario procedere con una valutazione d'impatto. Nulla vieta a ciascun Titolare del trattamento di effettuare un DPIA anche se ricorre uno solo dei criteri prescritti dal WP29.

DISCLAIMER

Il presente comunicato è divulgato a scopo conoscitivo per promuovere il valore dell'informazione giuridica. Non costituisce un parere e non può essere utilizzato come sostitutivo di una consulenza, né per sopperire all'assenza di assistenza legale specifica.