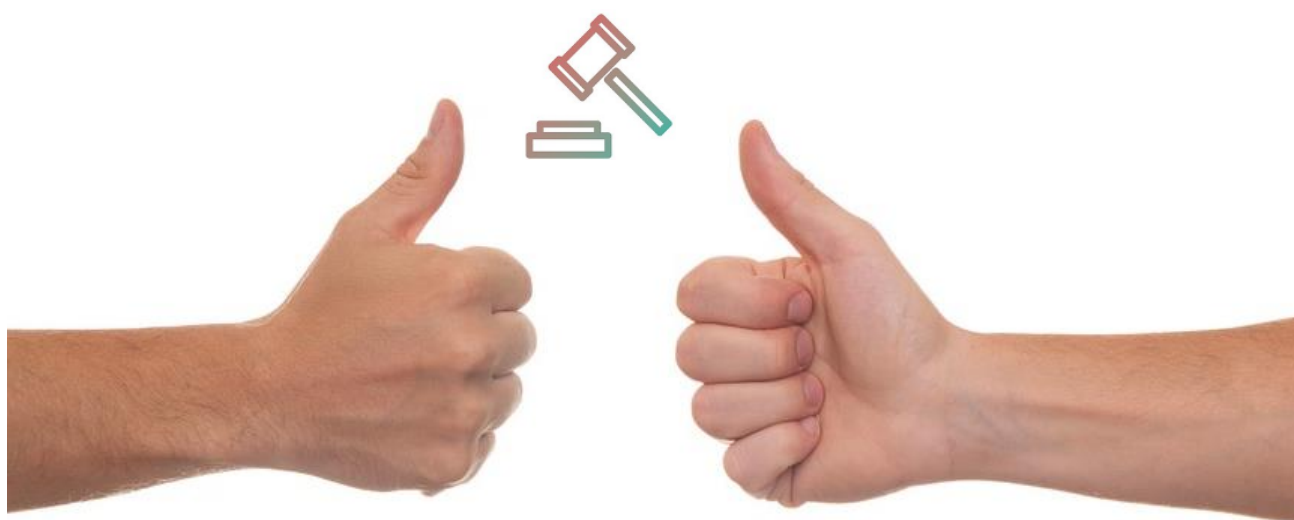


Linea Guida Rapida GDPR







General Data Protection Regulation UE 679/16 in vigore dal 25/05/2018



CRYPTO  TEAM
www.cryptoteam.it

*L'evoluzione tecnologica richiede un quadro normativo in continuo aggiornamento per cui la linea guida ha lo scopo di aiutare le imprese ad una migliore comprensione e consapevolezza e quindi deve essere intesa come mero valore illustrativo (**aggiornamento 30.11.2017**).*

Cosa è la DPIA?

	<p>DATA PROTECTION IMPACT ASSESMENT</p> <p>La sigla DPIA sta per valutazione di impatto sulla protezione dei dati. È un iter previsto dall'articolo 35 del Regolamento UE/2016/679 (GDPR) finalizzato a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di implementare misure idonee a fronteggiarli. Una DPIA può riguardare sia il singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.</p>
	<p>PERCHÉ LA DPIA ?</p> <p>La DPIA è uno strumento di responsabilizzazione necessario a rispettare le prescrizioni del GDPR, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In pratica, la DPIA è una procedura che consente di valutare e dimostrare la conformità delle regole aziendali con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.</p>
	<p>CHI E' IL RESPONSABILE ?</p> <p>La responsabilità della DPIA spetta al titolare del trattamento dati, nonostante la conduzione materiale della valutazione di impatto possa essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare controlla lo svolgimento della valutazione consultandosi con il responsabile della protezione dei dati e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore (es. responsabile della sicurezza dei sistemi informativi e del responsabile IT).</p>
	<p>LA DPIA E' OBBLIGATORIA?</p> <p>Sì, la DPIA è obbligatoria in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito: - trattamenti valutativi o di scoring, compresa la profilazione; - decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni); - monitoraggio sistematico (es: videosorveglianza); - trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche); - trattamenti di dati personali su larga scala; - combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data); - dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.); - utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.); - trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento). La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.</p>
	<p>QUANDO LA DPIA NON E' OBBLIGATORIA?</p> <p>Secondo linee guida del Gruppo Art. 29, la DPIA NON è necessaria per i trattamenti che: - non presentano rischio elevato per diritti e libertà delle persone fisiche; - hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA; - sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche; - sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA; - fanno riferimento a norme e regolamenti, UE o di uno stato membro, per la cui definizione è stata condotta una DPIA.</p>
	<p>QUANDO E' IL MOMENTO DI PROCEDERE ?</p> <p>La DPIA è necessaria prima di procedere al trattamento e deve prevedere un riesame continuo con ripetizione della valutazione a intervalli regolari. Nodali sono gli aggiornamenti e la registrazione cronologica delle modifiche apportate.</p>
<p>Nota Bene</p>	<p>IMPORTANTE SAPERE</p> <p>LA DPIA è il primo documento che viene richiesto durante una verifica Privacy da parte delle Autorità.</p>



Buoni Motivi

1

Aumento delle Attività

La tecnologia sta trasformando l'economia e le relazioni sociali, facilitando gli scambi interni e internazionali.

2

Impresa Sicura

Un'impresa che tratta i dati in conformità alle norme viene percepita come sicura e quindi adeguata ai tempi per sviluppare le proprie attività.

3

Maggiore Fiducia

Integrare maggiori livelli di sicurezza favorisce maggiori consensi e fiducia da parte di clienti, fornitori, partner, corrispondenti, collaboratori, utenti, istituti amministrativi, ecc..

4

Evita Sanzioni

Una buona e scrupolosa conduzione di trattamento dati evita onerose sanzioni (fino a 20 Milioni di €).

5

Libertà di Consenso

Se l'interessato cambia idea dopo aver rilasciato i singoli consensi (oggetto di ogni finalità), anche a distanza di tempo, ha la possibilità di revocarli in modo parziale o totale.

6

Possesso dei Propri Dati

E' possibile rientrare in possesso dei dati trasmessi ad una azienda oppure ad un servizio online e ritrasmetterli ad un nuovo fornitore.

7

Maggiore Visibilità

Nel GDPR visibilità e trasparenza sono una prerogativa sostanziale.

8

Sportello Unico

Se non si è d'accordo sul modo in cui vengono trattati i propri dati l'interessato può rivolgersi alle autorità.

9

Deindicizzazione

In alcuni casi è possibile chiedere ai motori di ricerca di deindicizzare una pagina web o chiedere a un sito web di cancellare le informazioni che ci riguardano (diritto all'oblio).

10

Residenza dei Dati

E' possibile sapere dove risiedono i dati e con chi sono condivisi. A seconda del paese in cui sono trasferiti i dati, si applica il Principio di Adeguatezza, che impedisce il trasferimento in quei paesi che non garantiscono una protezione dei dati conforme al GDPR.