Acronis

DOMANDE FREQUENTI SUL GDPR

DOMANDE FREQUENTI

D: Che cos'è il GDPR?

R: Il regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea (UE) è una nuova legge dell'Unione destinata a rafforzare la protezione dei dati privati di proprietà dei residenti dell'Unione europea. Sostituisce l'attuale mosaico di leggi nazionali sulla privacy delle informazioni con un unico insieme di regole direttamente applicate da ciascun stato membro della UE.

D: Quando entra in vigore il GDPR?

R: Il 25 maggio 2018.

D: Il GDPR riguarda soltanto le aziende con sede nella UE?

R: La risposta a questa convinzione errata è "No". Qualsiasi azienda con clienti nella UE o che acquisisce o gestisce in altro modo i dati personali di tali clienti è tenuta a sottostare al GDPR.

D: Che cosa intende il GDPR per "dati personali"?

R: Per "dati personali" si intendono tutte le informazioni che possono essere utilizzate per identificare una persona. Tutto ciò va ben oltre la definizione storica di informazioni identificabili personalmente e comprende nome, indirizzo email, post dei social media, informazioni fisiche, fisiologiche o genetiche, informazioni mediche, ubicazione, dati bancari, indirizzo IP, cookie e identità culturale.

D: Che cosa disciplina esattamente il GDPR?

R: Il GDPR regola la raccolta, l'archiviazione, il trasferimento e/o l'uso di tutti i dati personali (definiti collettivamente come elaborazione) che appartengono ai residenti dalla UE. Qualsiasi organizzazione che elabori i dati personali di residenti della UE, incluso l'eventuale monitoraggio della loro ubicazione o delle loro attività, ad esempio con cookie dei browser, rientra nel campo d'applicazione della legge, anche se l'organizzazione che si occupa dell'elaborazione non risiede fisicamente nella UE.

I regolamenti distinguono tra "titolari del trattamento" e "responsabili del trattamento" in qualità di chi si occupa dei dati personali. L'organizzazione che stabilisce cosa fare con i dati personali e che determina la ragione per farlo è il titolare del trattamento. Qualsiasi terzo di cui un titolare del trattamento si avvale per il trattamento dei dati personali, ad es. un fornitore di servizi di storage cloud, è un responsabile del trattamento.

D: Che effetto ha il GDPR sui diritti alla privacy?

R: Il GDPR potenzia fortemente i diritti alla privacy dei residenti UE e impone degli obblighi significativi a tutela di tali diritti su qualsiasi azienda, istituto o persona fisica che si occupi di tali dati personali. I nuovi requisiti a cui devono attenersi i responsabili del trattamento sono:

- **Diritti dei soggetti interessati:** i residenti UE esercitano un controllo maggiore sui propri dati personali, tra cui il diritto di richiedere che il responsabile del trattamento fornisca loro copie di tali dati, corregga gli errori in essi presenti e li elimini completamente su richiesta.
- **Prova di conformità:** i responsabili del trattamento devono applicare politiche e procedure per la sicurezza dei dati e conservare record dettagliati sulle loro attività di elaborazione dei dati.
- **Notifiche sulle violazioni dei dati:** i responsabili del trattamento devono segnalare le compromissioni dei dati alle rispettive autorità di controllo GDPR e segnalare le compromissioni gravi ai soggetti interessati coinvolti.
- **Sanzioni per la mancata conformità:** i legislatori del GDPR possono imporre sanzioni pecuniarie salate alle aziende non conformi in base alla gravità della compromissione e ai danni sostenuti.

D: Il GDPR impone che i dati personali debbano restare all'interno della UE?

R: Non esattamente, ma spostare dati personali al di fuori della UE (definito come "trasferimento transfrontaliero dei dati") e attenersi al GDPR possono non essere compatibili. È necessario tenere conto di alcune regole. Per prima cosa, i trasferimenti di dati sono generalmente consentiti verso qualsiasi paese di destinazione che sia incluso nell'elenco di destinazioni della UE dotate di sicurezza "adeguata", vale a dire dove le tutele della privacy dei dati soddisfano gli standard dell'Unione europea. In alcuni casi, potrebbe essere l'intero paese a non essere considerato adeguato, mentre i singoli territori o settori al suo interno potrebbero esserlo. Dall'inizio del 2018, l'elenco approvato comprendeva tutti i paesi membri della UE, tre paesi non della UE che fanno parte dello Spazio economico europeo (SEE) (Islanda, Lichtenstein e Norvegia) e alcuni altri paesi e territori (Andorra, Argentina, Canada, Isole Faroe, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera e Uruguay).

I trasferimenti di dati sono anche consentiti verso le destinazioni che soddisfano gli standard UE per le "norme vincolanti d'impresa". In base a questo principio, i trasferimenti di dati personali sono consentiti se effettuati da specifiche persone giuridiche all'interno di un'azienda e, in certi casi, da gruppi di aziende indipendenti coinvolte in attività economiche congiunte. Per essere idonee, le norme vincolanti d'impresa devono essere approvate da un'autorità di controllo appropriata e devono soddisfare gli standard di coerenza della UE.

Sono consentite anche altre destinazioni per i dati se rispettano determinati "codici di condotta" e "metodi di certificazione", in genere redatti da un'associazione di settore o da uno dei suoi enti rappresentativi, e soltanto con l'approvazione dei legislatori GDPR.

Anche altri trasferimenti di dati sono legittimi se ricadono nella definizione di "deroghe specifiche", ovvero eccezioni allo standard normativo. Gli esempi includono trasferimenti di dati:

- A cui il soggetto interessato acconsente espressamente e comprende i rischi connessi.
- Dove il responsabile del trattamento deve adempiere a un obbligo contrattuale o soddisfare un diritto in sede giudiziaria.
- Che sono giudicati nel pubblico interesse o nell'interesse vitale dell'interessato.
- Che sono nel "legittimo interesse" del titolare del trattamento dei dati, nella misura in cui tale interesse non sostituisca i diritti dell'interessato. Il titolare del trattamento dei dati deve valutare le circostanze del trasferimento e adottare misure ragionevoli per tutelare i dati personali.

In breve, è generalmente più semplice, sicuro ed economico per la maggior parte delle aziende non spostare i dati personali al di fuori della UE e del suo breve elenco di paesi approvati. Siate pronti a sostenere alcune spese straordinarie e a impegnarvi per spostare i dati personali altrove; siate anche pronti a dimostrare alle autorità di controllo GDPR tutto ciò che avete fatto per proteggere i dati. Se decidete di affidarvi alle norme vincolanti d'impresa, ai codici di condotta, ai metodi di certificazione e/o alle deroghe specifiche per giustificare altri tipi di trasferimenti transfrontalieri dei dati, fate in modo di poter contare su un consulente legale.

D: In che modo il GDPR influenza le nostre risposte alle violazioni della sicurezza?

R: Il GDPR prevede che titolari e responsabili del trattamento eseguano la distribuzione di sistemi per garantire la difesa, il monitoraggio e la segnalazione di potenziali compromissioni della sicurezza, e per implementare e documentare tecnologia, politiche e procedure a supporto della prevenzione, del rilevamento, della segnalazione e della notifica delle compromissioni. Nuovi e più rigidi requisiti per la divulgazione si applicano a qualsiasi incidente abbia come conseguenza l'accesso, il trasferimento, l'alterazione o la distruzione dei dati personali da parte di persone non autorizzate, sia accidentalmente che intenzionalmente.

Gli incidenti di protezione delle privacy possono essere causati da guasti tecnologici (ad es. blocco del disco rigido), da errori umani accidentali (ad es. eliminazione o danno accidentali ai file degli utenti da parte del personale IT) o da violazioni intenzionali dannose (ad es. un attacco ransomware da parte di criminali informatici che crittografano i dati personali e chiedono il pagamento di un riscatto per sbloccarli).

In breve, i titolari e i responsabili del trattamento devono impegnarsi di più per identificare gli incidenti di sicurezza che hanno un impatto sui dati personali, segnalarli alle autorità di controllo entro 72 ore dal rilevamento e, nel caso di grave danno, furto o smarrimento dei dati personali, notificare rapidamente anche i soggetti interessati.

D: Quali nuovi diritti degli utenti devono supportare i titolari del trattamento?

R: Il GDPR conferisce ai soggetti interessati un controllo e una visibilità molto maggiori sull'uso che i titolari del trattamento fanno dei loro dati personali. I titolari del trattamento sono tenuti a soddisfare le richieste degli utenti (senza alcun costo per gli utenti) di sapere quali elementi dei loro dati personali hanno acquisito, di fornire loro tali dati in un formato facilmente accessibile, di correggere eventuali errori identificati dagli utenti e di cancellare i dati personali su richiesta (il cosiddetto "diritto all'oblio").

D: Chi è il responsabile della protezione dei dati? Titolari e responsabili del trattamento sono tenuti a designarlo?

R: Il responsabile della protezione dei dati è un dipendente o consulente di cui molti titolari e responsabili del trattamento dovranno designare in qualità di responsabile primario della supervisione della conformità al GDPR. Gli enti pubblici devono attenersi a uno standard più alto: quasi tutti infatti dovranno designare un responsabile della protezione dei dati. Le aziende private devono designare un responsabile della protezione dei dati se elaborano grandi quantità di dati personali che rivelano l'etnia o gruppo etnico, le opinioni politiche, le credenze religiose o filosofiche, i dati genetici o biometrici e/o le condanne penali dei soggetti interessati.

Il responsabile della protezione dei dati deve essere un professionista della conformità esperto nella legislazione sulla protezione dei dati e sulle best practice. Il suo compito è quello di notificare ai titolari del trattamento, ai responsabili del trattamento e ai dipendenti dell'azienda i loro obblighi ai sensi del GDPR, per monitorare la conformità, e di agire da collegamento con l'autorità di controllo.

D: Cosa succede se come titolari e/o responsabili del trattamento veniamo sorpresi a non rispettare le normative del GDPR?

R: Le sanzioni per la mancata conformità al GDPR non sono di poco conto. La vostra autorità di controllo locale può comminare una sanzione pecuniaria fino a € 10 milioni o al 2% del fatturato annuo, a seconda di qual è l'importo maggiore, per quelli che vengono definiti reati di primo livello, come la mancata conservazione di record scritti o la mancata implementazione delle opportune misure tecniche e organizzative per soddisfare gli obiettivi di conformità. Le sanzioni pecuniarie possono arrivare fino a € 20 milioni o al 4% del fatturato globale annuo, a seconda di qual è l'importo maggiore, per reati più gravi quali compromissioni dei dati di dimensioni importanti e la mancata protezione dei dati personali da furto, alterazione o eliminazione.

Le sanzioni pecuniarie si applicano tanto ai titolari quanto ai responsabili del trattamento. Le autorità di controllo possono assegnare una sanzione pecuniaria in maniera proporzionale al titolare del trattamento e ai suoi responsabili del trattamento, con la valutazione della misura in cui ciascuno è responsabile della violazione in base ai provvedimenti adottati per garantire la conformità al GDPR.

Oltre a queste preoccupanti sanzioni pecuniarie, le aziende che ignorano o sottovalutano volontariamente i propri obblighi di conformità al GDPR sono passibili di un potenziale danno duraturo alla propria reputazione aziendale, oltre a procedimenti legali intentati da privati per danno "materiale o immateriale" se i dati personali sono stati compromessi. Le stesse sanzioni pecuniarie e non valgono anche per i responsabili del trattamento terzi se questi elaborano i dati personali per conto di un'altra azienda. Quando si considera l'aumento esponenziale delle compromissioni dei dati in anni recenti...

Ad esempio, gli attacchi ransomware sono passati da un fatturato illecito pari a USD 800.000/anno nel 2015 a una proiezione potenziale di 8-10 miliardi di dollari nel 2018 per mancata conformità solo per quanto riguarda le compromissioni segnalate.

D: L'obiettivo di conseguire la conformità al GDPR sembra inarrivabile. Da dove si comincia?

R: Come fornitore di soluzioni di protezione dei dati, Acronis ritiene che concentrarsi sull'aggiornamento dell'archiviazione dei dati e sull'infrastruttura di backup sia un passo fondamentale verso la conformità al GDPR. Essere in grado di specificare esattamente dove sono archiviati i dati, impedire le compromissioni come gli attacchi ransomware e proteggere i dati con una forte crittografia dei dati in movimento e a riposo sono punti di partenza fondamentali con un impatto concreto e positivo sulla posizione di conformità al GDPR.

Ma non dovreste fare affidamento su di noi quando decidete come affrontare la sfida della conformità al GDPR. È essenziale che vi dotiate anche di capaci consulenti legali e professionali.

Queste domande frequenti hanno finalità unicamente informative. Non sono destinate a fornire e non devono essere utilizzate o interpretate come una consulenza legale. Non agite e non evitate di agire basandovi sul contenuto delle presenti domande frequenti senza avere prima avuto una consulenza legale o professionale di altro tipo.

Acronis

Per maggiori informazioni, visitate **https://www.acronis.com/it-it/gdpr/**

Copyright © 2002-2018 Acronis International GmbH. Tutti i diritti riservati. Acronis e il logo Acronis sono marchi registrati di Acronis International GmbH negli Stati Uniti e/o in altri paesi. Tutti gli altri marchi o marchi registrati sono proprietà dei rispettivi titolari. Soggetto a modifiche tecniche. Le immagini potrebbero non corrispondere al prodotto reale. Si declina qualsiasi responsabilità per possibili errori. 2018-02