StorageCraft®

Domande frequenti sul GDPR

D. Chi e che cosa protegge il GDPR?

R. Il GDPR (General Data Protection Regulation, Regolamento generale sulla protezione dei dati) è il nuovo regolamento completo dell'Unione Europea in materia di privacy e protezione dei dati. A grandi linee, il GDPR protegge i "dati personali" degli individui dell'EEA (European Economic Area, Spazio Economico Europeo). Per "individuo" si intende un essere umano o persona fisica. Non ci si riferisce a un'entità. StorageCraft è un'azienda B2B, quindi la maggior parte dei dati personali che incontriamo sono relativi ai dipendenti delle nostre aziende partner oppure sono dati personali contenuti nei backup che elaboriamo attraverso i nostri prodotti e servizi cloud.

D. StorageCraft ha sede negli Stati Uniti. Perché il GDPR si applica a StorageCraft?

R. Sebbene StorageCraft abbia sede negli Stati Uniti, ogni volta che forniamo i nostri servizi ai clienti (o ai loro affiliati) nello Spazio Economico Europeo o forniamo servizi attraverso le nostre filiali irlandesi, in genere viene applicato il GDPR.

D. Cosa sono i "dati personali"?

R. I "dati personali" sono le informazioni che possono essere utilizzate per identificare, direttamente o indirettamente, un individuo. Ad esempio, informazioni o materiale che è possibile considerare "dati personali" sono: nome, numero di telefono, indirizzo, indirizzo e-mail, data di nascita, numero di identificazione (ad esempio numero di patente, codice fiscale o numero di previdenza sociale) e fotografie. I dati personali includono anche identificativi meno ovvi come indirizzi IP e nomi di utenti online.

D. L'e-mail di lavoro o il numero di telefono di lavoro possono essere considerati "dati personali"?

R. Sì. Non importa che queste informazioni siano relative al lavoro. Se le informazioni possono essere utilizzate per identificare direttamente o indirettamente una persona, tali informazioni sono "dati personali" e sono protette dal GDPR.

D. Cos'è l'"accordo per il trattamento dei dati personali" (conosciuto anche come "supplemento al trattamento dei dati personali")?

R. Secondo il GDPR, il "titolare del trattamento" è la parte che stabilisce lo scopo e i mezzi per il trattamento dei dati personali e il "responsabile del trattamento" è la parte che elabora i dati personali per conto di un titolare. Il GDPR richiede che la relazione tra il titolare del trattamento e il responsabile del trattamento sia governata da un accordo scritto. In tale accordo devono essere specificati determinati termini minimi e obbligatori, tra cui "sufficienti garanzie" che il responsabile abbia implementato misure tecniche e organizzative appropriate in relazione al trattamento dei dati personali. Questo accordo è comunemente definito accordo o supplemento per il trattamento dei dati personali ("DPA"). Di solito, si pensa erroneamente che solo per il fatto che i dati personali vengono trasferiti da una parte all'altra sia necessario un DPA. Non è questo il caso. Un DPA è richiesto solo quando un titolare del trattamento trasferisce i dati personali a un responsabile del trattamento affinché il responsabile del trattamento "elabori" i dati personali per e per conto del titolare. Al contrario, se la Parte A non trasferisce né fornisce l'accesso ai dati personali alla Parte B, per cui la Parte B può elaborare i dati personali per la Parte A, non è richiesto un DPA. Se il destinatario dei dati personali non elabora i dati personali per e per conto del beneficiante, ma per il proprio scopo legittimo, ad esempio l'esecuzione di un contratto della Parte B, non è richiesto un DPA.

D. Quali relazioni con i partner di StorageCraft richiedono un DPA?

R. Nella tabella in basso sono riportate le relazioni comuni con i partner di StorageCraft, viene indicato se è richiesto un DPA e vengono specificati i motivi:

Relazione con StorageCraft	L'accordo per il trattamento dei dati personali è necessario?	Spiegazione
Rivenditore di valore aggiunto (VAR – vendita di software perpetuo)	No	Gli unici dati personali che StorageCraft deve ricevere da un VAR sono i nomi e gli indirizzi e-mail dei dipendenti del VAR o dei dipendenti dell'utente finale. StorageCraft non tratta questi dati personali per il VAR o per l'utente finale. A contrario, StorageCraft è un titolare del trattamento di quei dati personali e li elabora per proprio conto, allo scopo di distribuire i propri prodotti al VAR e all'utente finale, rispettando i propri obblighi e la gestione generale delle relazioni.
Provider di servizi gestiti (MSP – vendita di software per sottoscrizioni)	No	Gli unici dati personali che StorageCraft deve ricevere da un MSP sono i nomi e gli indirizzi e-mail dei dipendenti del MSP. StorageCraft non elabora questi dati personali per il MSP. A contrario, è un titolare del trattamento di quei dati personali e li elabora per proprio conto, allo scopo di distribuire i propri prodotti e servizi al MSP, rispettando i propri obblighi.
Contratto per i prodotti Cloud	Sì	Un cliente cloud trasferisce i backup a StorageCraft per il trattamento per conto del cliente cloud. Poiché StorageCraft non sa quali tipi di dati sono contenuti nei backup, presuppone che i backup contengano dati personali. Nella distribuzione di prodotti e servizi cloud, StorageCraft è un responsabile del trattamento (e/o in alcuni casi, un sub-responsabile, se il suo cliente cloud utilizza i servizi cloud di StorageCraft per eseguire il backup dei dati che elabora come responsabile per conto di un altro titolare), in quanto elabora i dati per conto del suo cliente cloud, pertanto è necessario DPA.
Contratto di distribuzione	No	Un distributore può trasferire a StorageCraft i dati personali associati alle aziende della catena di vendita, ad esempio, il proprio rivenditore o l'utente finale. In genere, i dati personali sono composti dai nomi e dagli indirizzi e-mail delle persone che lavorano per il distributore, il rivenditore o l'utente finale. StorageCraft non elabora questi dati personali per il distributore o le altre parti della catena di vendita. A contrario, StorageCraft è un titolare del trattamento di quei dati personali e li elabora per proprio conto, allo scopo di distribuire i propri prodotti al distributore, al VAR o all'utente finale, rispettando i propri obblighi e la gestione generale delle relazioni.

D. StorageCraft ha un responsabile della protezione dei dati?

R. No. Comunemente si pensa che il GDPR richieda che tutte le aziende debbano nominare un responsabile della protezione dei dati. Non è questo il caso. Il GDPR richiede la nomina di un responsabile della protezione dei dati solo in tre casi molto precisi: (a) il trattamento viene eseguito da un'"autorità o da un organismo pubblico", (b) le "attività principali" del titolare o del responsabile del trattamento dei dati personali implicano il monitoraggio regolare, sistematico e su vasta scala degli interessati e/o (c) le "attività principali" del titolare o del responsabile del trattamento dei dati personali consistono nel trattamento su vasta scala di dati personali altamente sensibili. Queste circostanze non si applicano a StorageCraft. Sebbene StorageCraft non sia obbligata a nominare un responsabile dei dati personali, prendiamo la protezione dei dati molto seriamente. La conformità della protezione dei dati è controllata dal reparto legale e da quello IT.

D. Quali sono le misure di sicurezza tecniche e organizzative adottate da StorageCraft in relazione al trattamento dei dati personali?

R. Sebbene StorageCraft non possa rivelare tutti i processi e le procedure di sicurezza, si impegna a proteggere i dati personali in conformità con il GDPR. Un riepilogo delle misure di sicurezza tecniche e organizzative di StorageCraft è incluso in un supplemento ai DPA di StorageCraft (ove richiesto). Una copia di queste misure è disponibile su richiesta.

D. Quali sono le "clausole contrattuali standard"? E le clausole utilizzate da StorageCraft sono conformi al GDPR?

R. Come punto di partenza, il GDPR proibisce qualsiasi trasferimento di dati personali al di fuori dell'EEA, a meno che non siano salvaguardati in modo appropriato. Le "clausole contrattuali standard" (a volte definite "clausole modello") sono uno dei metodi approvati dalla Commissione Europea in base ai quali i dati personali possono essere trasferiti legalmente al di fuori dell'EEA, secondo le opportune misure di salvaguardia. Il valore standard delle clausole contrattuali è tale che, affinché siano valide, devono essere copiate testualmente dalla decisione del 2010 della Commissione Europea che le ha promulgate. Le clausole contrattuali standard utilizzate da StorageCraft fanno parte del relativo DPA e sono conformi ai requisiti della legge sulla privacy dei dati, che include il GDPR.

D. Chi sono i sub-responsabili utilizzati da StorageCraft?

R. Un elenco di sub-responsabili di StorageCraft è disponibile sul sito web di StorageCraft.

D. Se un rivenditore di valore aggiunto acquista prodotti StorageCraft attraverso un distributore, è necessario il consenso dell'utente finale per fornire al distributore i dati personali sui dipendenti dell'utente finale, ad esempio il nome e l'indirizzo e-mail di una persona di contatto che lavora per l'utente finale?

R. I nostri partner devono eseguire le proprie analisi riguardanti gli effetti del GDPR sulle loro pratiche commerciali, inclusi i propri obblighi in qualità di responsabili del trattamento dei dati. Suggeriamo di prestare particolare attenzione all'articolo 6 del GDPR, che identifica le varie basi legali per il trattamento dei dati personali, nonché agli articoli 13 e 14, che identificano gli obblighi di un titolare del trattamento di informare un interessato sull'uso dei propri dati, il che viene in genere garantito attraverso una politica sulla privacy chiara e accessibile. Le persone spesso presumono che il "consenso" sia necessario quando tutto ciò che un titolare del trattamento dei dati ha la necessità di fare è comunicare chiaramente con l'interessato circa l'uso e l'elaborazione dei suoi dati personali. E, ai sensi dell'articolo 6, il consenso è solo una base secondo la quale i dati personali possono essere elaborati. Un titolare del trattamento dei dati può, ma non deve necessariamente, fare affidamento sul consenso quando esiste un'altra base per l'elaborazione. La base per l'elaborazione deve essere valutata attentamente, in quanto incide sugli obblighi del titolare del trattamento dei dati, ai sensi di altre disposizioni del GDPR, ad esempio una richiesta di cancellazione da parte dell'interessato.

D. In che modo la Brexit influisce sui miei dati con i prodotti cloud di StorageCraft?

R. Dato che i negoziati Brexit del Regno Unito con l'Unione Europea sono in corso, gli effetti della Brexit sono alquanto incerti, incluso il suo impatto sulla protezione dei dati. Anche se oggi non possono essere formulate dichiarazioni definitive in relazione alla legge sulla protezione dei dati nel Regno Unito dopo la Brexit, la maggior parte degli indicatori suggerisce che la situazione non cambierà molto.

Il GDPR è entrato in vigore nel maggio 2018 ed è attualmente la legge del Regno Unito. Il governo, preoccupato di incidere negativamente su imprese e cittadini a causa di un'eccessiva incertezza, ha precisato che molte delle leggi europee esistenti continueranno probabilmente ad essere applicate nel Regno Unito anche dopo la Brexit. A prescindere da se ci sarà una Brexit veramente "soft", ma le autorità del Regno Unito per la protezione dei dati hanno recentemente sottolineato il loro impegno costante nei confronti del GDPR. Infatti, in un discorso dell'aprile 2018, il Commissario per l'Informazione del Regno Unito ha dichiarato che continua a suggerire al governo e al parlamento una "riforma legislativa che garantisca elevati standard di protezione dei dati per i cittadini e i consumatori del Regno Unito, ovunque risiedano i loro dati, flussi di dati ininterrotti verso l'Europa e il resto del mondo e certezza legale per gli affari". Ha sottolineato, inoltre, che la protezione dei dati è un "settore prioritario" per il regolamento Brexit e che l'autorità britannica in materia di protezione dei dati (ICO, Information Commissioner's Office) continua a svolgere un ruolo completo nella creazione di orientamenti per il GDPR e ad impegnarsi con il Comitato europeo per la protezione dei dati o "EDPB" (ex Gruppo di lavoro articolo 29). Ha anche notato che il primo ministro May di recente si è espresso favorevolmente circa un ruolo costante per l'ICO, sotto forma di un seggio nel Comitato europeo per la protezione dei dati, con diritti di voto o una relazione altrettanto sostanziale.

Dopo la Brexit, le aziende che vendono prodotti e servizi nel Regno Unito dovranno conformarsi sia al GDPR che alla versione del GDPR del Regno Unito. Ci aspettiamo una sovrapposizione sostanziale, se non addirittura universale, tra i due atti legislativi. Poiché il GDPR rappresenta già la legge del Regno Unito, anche se la Brexit in sé sostanzialmente appare come la conclusione "più difficile" dello spettro Brexit, ci aspettiamo che il Regno Unito sarà un paese adeguato per ricevere dati dall'EEA e viceversa.

Di conseguenza, non riteniamo necessario spostare i dati dai data center di StorageCraft di Dublino o Francoforte o di modificare in altro modo le politiche sui prodotti. Detto ciò, StorageCraft è consapevole della necessità di garantire la conformità con il GDPR e la legge sulla protezione dei dati del Regno Unito post-Brexit. Con l'avvicinarsi della Brexit, staremo a vedere gli effetti, qualora ci siano, che la Brexit può avere sui nostri prodotti e servizi vincenti. Vi terremo aggiornati.

D. In che modo il "diritto di cancellazione" influisce sui dati contenuti nei backup?

R. Uno dei diritti conferiti alle persone interessate è il diritto alla cancellazione, indicato anche come "diritto all'oblio". In determinate circostanze, ciò consente all'interessato di incaricare un titolare del trattamento di cancellare i dati personali dell'interessato.

Come con tutta la legislazione, alcuni problemi non sono trattati specificamente dal GDPR. Questi problemi includono l'interazione tra il diritto di cancellazione e i backup del computer. Con un backup del computer, potrebbe essere impossibile isolare i dati personali di un singolo interessato, eliminarli e mantenere l'integrità del backup. E, anche nei casi in cui ciò è possibile, i costi associati a tale sforzo potrebbero essere del tutto impraticabili. Questo problema richiede chiarimenti legislativi o indicazioni da parte dell'EDPB, in particolare dato che lo stesso GDPR afferma che la capacità di ripristinare i dati personali da un backup del computer è una delle "misure tecniche e organizzative appropriate" che dovrebbero essere implementate per garantire la sicurezza dei dati. (Vedere l'art. 32(1)c.)

Sebbene al momento non vi sia una risposta chiara, l'ICO nel Regno Unito è una delle poche autorità nazionali per la protezione dei dati ad aver risolto il problema. Prima del GDPR, l'ICO ha pubblicato una guida intitolata "Eliminazione di dati personali." In questa guida è stata riconosciuta la difficoltà presentata da una richiesta di cancellazione quando si conservano dati archiviati o di backup. La guida afferma che "l'ICO adotterà un approccio realistico in termini di riconoscimento del fatto che l'eliminazione di informazioni da un sistema non è sempre una questione diretta e che è possibile mettere le informazioni "fuori uso" e "sospendere" i problemi di conformità della protezione dei dati, a condizione che siano messe in pratica alcune misure di salvaguardia". Per l'ICO, i dati personali oggetto di una richiesta di cancellazione sono messi "fuori uso", se non effettivamente eliminati, se il titolare del trattamento:

- Non può utilizzare o non utilizzerà i dati in un modo che riguarda l'interessato;
- Non fornisce ad alcuna altra organizzazione l'accesso ai dati;
- Applica la "protezione tecnica e organizzativa adatta" ai dati e
- Si impegna a eliminare i dati se o quando l'eliminazione diventa possibile.

L'ICO ha continuato a citare questa guida pre-GDPR, affermando che verrà aggiornata "a tempo debito". Dopo il GDPR, l'ICO ha continuato a basarsi su questa guida, sottolineando che, quando si tratta di eliminare i dati contenuti nei backup del computer, mettere i dati "fuori uso" nel modo sopra descritto è un approccio accettabile per rispondere a una richiesta di cancellazione che coinvolge i dati di backup. L'ICO aggiunge che un titolare del trattamento deve essere assolutamente chiaro con le persone riguardo a cosa accadrà ai loro dati quando la richiesta della loro eliminazione sarà soddisfatta, anche per quanto riguarda i sistemi di backup". StorageCraft raccomanda di informare l'interessato del fatto che i suoi dati personali contenuti nel backup non sono stati eliminati, ma messi "fuori uso" attraverso l'applicazione delle suddette condizioni. Fino a quando il GDPR non sarà chiarito, sia dal punto di vista legislativo che attraverso indicazioni da parte dell'EDPB, StorageCraft ritiene che quanto sopra sia la soluzione migliore per il problema.

D. Dove posso saperne di più sull'approccio di StorageCraft alla privacy dei dati?

R. Poco dopo la data effettiva del GDPR, StorageCraft ha pubblicato una politica sulla privacy aggiornata, disponibile sul sito web di StorageCraft. Tale guida è il punto di partenza per qualsiasi richiesta sui dati personali raccolti da StorageCraft e su come utilizziamo tali dati. Per ulteriori domande su problemi e dubbi relativi alla privacy, potete contattarci all'indirizzo privacy@storagecraft.com.

QUESTE DOMANDE FREQUENTI SONO PREPARATE DALLA TECNOLOGIA STORAGECRAFT E SONO UN'ESPRESSIONE DEI PARERI DELL'AZIENDA SULLE QUESTIONI AFFRONTATE.
NON COSTITUISCONO UNA CONSULENZA LEGALE. SI PREGA DI CONSULTARE IL PROPRIO CONSULENTE LEGALE RIGUARDO I PROBLEMI SOLLEVATI IN QUESTA SEDE.

StorageCraft