Distruggere i documenti in modo intelligente

Per una generazione conforme alle norme del GDPR

Perché una politica di sicurezza cartacea è parte integrante della vostra conformità GDPR.

Esclusione di responsabilità
Nulla di quanto contenuto nel presente documento deve essere interpretato come consulenza legale. Le organizzazioni devono consultare il proprio consulente legale per quanto riguarda la conformità con il regolamento generale sulla protezione dei dati o con qualsiasi altra legge o regolamento applicabile.

CONFORMATI AL **GDPR***

*la distruzione dei documenti supporta la conformità al GDPR

Informazioni su questo documento

Questa documentazione fornisce **una panoramica di ciò che il GDPR si propone di raggiungere**, dei problemi che comporta per le organizzazioni e offre una soluzione quadro per le imprese da utilizzare per favorire il rispetto di questa nuova normativa.

Lo scopo di questo documento è quello di fornire un'introduzione al Regolamento Generale sulla Protezione dei Dati (GDPR) dell'UE e al suo impatto sulle diverse aziende, in modo da poter creare un quadro di riferimento per una politica di sicurezza cartacea per la propria impresa, ora che queste normative sono entrate in vigore.

Cos'è il GDPR? Questo regolamento richiede alle organizzazioni di applicare buone pratiche in materia di sicurezza dei dati elettronici e cartacei e, in caso di violazione dei dati, di informare le persone interessate o potenzialmente interessate.

Il campo di applicazione del GDPR si estende a livello mondiale a tutte le organizzazioni che controllano o elaborano dati personali sugli individui nell'UE, indipendentemente dalla loro presenza geografica. I requisiti GDPR si applicano sia ai dati personali elettronici che a quelli cartacei e ciò significa che tutte le organizzazioni devono soddisfare i requisiti GDPR se trattano dati di carattere personale provenienti dall'UE.

Sebbene la sicurezza dei dati elettronici sia giustamente al primo posto per diverse organizzazioni, molte di esse non affrontano adeguatamente la questione della sicurezza dei dati cartacei. In effetti, due terzi degli uffici ammettono di non distruggere informazioni riservate[1]. Ciò espone le organizzazioni al rischio di non essere conformi con il GDPR e le persone interessate al rischio di frode e furto d'identità. Con questo obiettivo in mente, Rexel, un marchio leader nel campo delle macchine distruggidocumenti, incoraggia le organizzazioni a rivedere le loro politiche e pratiche di sicurezza relative sia ai dati cartacei sia a quelli elettronici.

Una panoramica

Il GDPR cerca di proteggere il diritto alla privacy degli individui in Europa, siano essi cittadini dell'UE o meno. Questi diritti alla privacy includono, ma non sono limitati a:

Trasparenza
Il diritto di ricevere informazioni chiare sulle modalità di trattamento dei dati personali da parte delle organizzazioni.

Consenso
Il diritto di controllare il modo in cui le organizzazioni utilizzano le informazioni personali.

Sicurezza
Il diritto di ottenere informazioni su come le organizzazioni proteggono adeguatamente i dati personali.

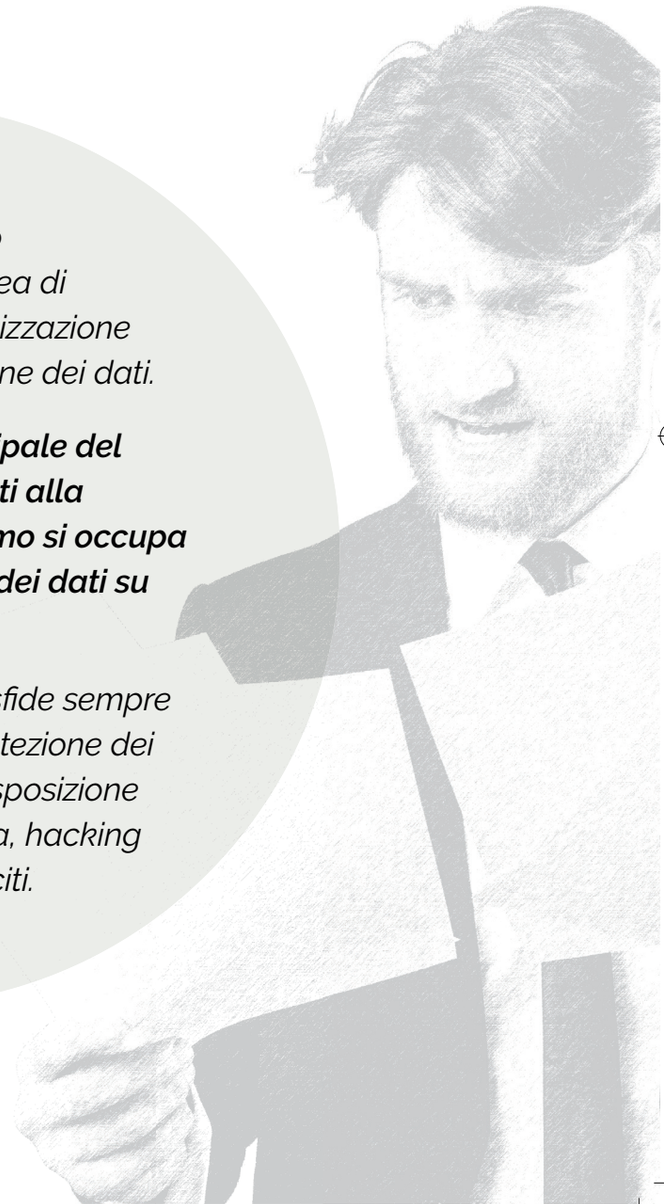
Raccolta e limitazione delle finalità
Il diritto di aspettarsi che le organizzazioni riducano al minimo la raccolta e l'utilizzo delle informazioni.

Notifica di violazione
Il diritto di essere informati in caso di violazione dei dati.

Il GDPR fa parte del piano della Commissione Europea di modernizzazione e armonizzazione delle norme sulla protezione dei dati.

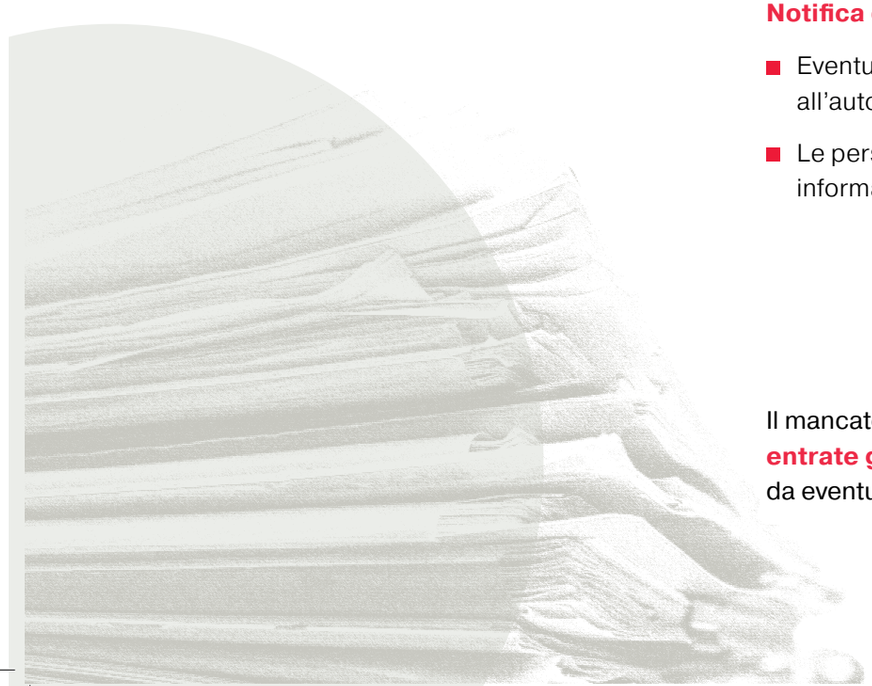
Sebbene l'obiettivo principale del GDPR sia rafforzare i diritti alla privacy online, quest'ultimo si occupa comunque della privacy dei dati su supporto cartaceo.

Si concentra inoltre sulle sfide sempre maggiori in materia di protezione dei dati e della vita privata, esposizione a violazioni della sicurezza, hacking e altri comportamenti illeciti.



Cos'è cambiato?

I punti seguenti individuano i settori specifici all'interno del GDPR che sono nuovi diritti per gli individui o diritti esistenti ai sensi della legge sulla protezione dei dati che sono stati rafforzati come parte del GDPR:



Portabilità dei dati e diritto all'oblio

- Le persone fisiche hanno ora il diritto di trasferire i loro dati personali da un'organizzazione all'altra.
- I dati personali devono essere forniti in un formato strutturato e leggibile da un dispositivo automatizzato.
- Un individuo può richiedere la cancellazione o la rimozione di dati personali

Notifica di violazione dei dati

- Eventuali violazioni devono essere segnalate all'autorità di vigilanza
- Le persone interessate devono inoltre essere informate

Inventario

- Le autorità locali non devono più essere informate del trattamento dei dati personali
- Le organizzazioni devono tenere un registro delle attività di trattamento sotto la propria responsabilità

Valutazioni d'impatto sulla protezione dei dati (DPIA) e sicurezza

- Le DPIA sono un modo per identificare rischi elevati per i diritti alla privacy delle persone.
- I requisiti e le raccomandazioni di sicurezza dovrebbero basarsi sulla valutazione del rischio

Controllo dei dati e responsabilità

- Le organizzazioni devono inoltre essere in grado di dimostrare il rispetto delle disposizioni del GDPR.

Il mancato rispetto delle norme del GDPR può comportare **multe fino a 20 milioni di Euro, o il 4% delle entrate globali delle società**, a seconda di quale sia il valore maggiore. Inoltre, il soggetto interessato da eventuali violazioni ha il diritto di citare in giudizio un'organizzazione dinanzi a un tribunale.

A chi si applica?

L'introduzione del GDPR nel maggio 2018 impatta sui seguenti ruoli:

Responsabili del trattamento
Determinano come e perché vengono trattati i dati personali.

Incaricati del trattamento
Persone che agiscono per conto del responsabile del trattamento.

È responsabilità di queste due figure assicurare che i loro clienti siano pienamente conformi a tutti gli aspetti del GDPR, per evitare di incorrere in ammende.

Il Responsabile del trattamento **deve nominare un Responsabile della Protezione dei Dati** e tenere traccia di tutte le attività di trattamento da lui svolte per conto dei clienti.

Il GDPR copre i dati personali e i dati sensibili in formato elettronico e fisico

Quando si costruisce una politica di conformità per la propria organizzazione, è fondamentale considerare a quali tipi di dati si applicherà il GDPR.

I dati che rientrano nell'ambito di applicazione del GDPR comprendono qualsiasi informazione relativa a una persona identificabile. Alcuni esempi di **dati personali** coperti da GDPR includono il nome completo, l'indirizzo e-mail e il numero di telefono.

Il GDPR applica inoltre protezioni supplementari a una **sottocategoria di dati personali, i cosiddetti dati personali sensibili**.

Il GDPR si occupa dei dati personali trattati da organizzazioni **sia in formato elettronico che fisico**, come i documenti cartacei.

Un quadro di riferimento per le imprese per il rispetto del GDPR

Le organizzazioni hanno tre aree principali che devono essere riviste per raggiungere la conformità con le disposizioni del GDPR. Affrontando queste tre componenti, le aziende possono costruire quadri chiari di una politica di sicurezza dei dati per ogni aspetto, che consentiranno la piena conformità con tutte le aree del GDPR.

Queste componenti sono:

Persone

La proprietà e la responsabilità del personale per tutti i dati da esso trattati all'interno dell'organizzazione è fondamentale. Un'organizzazione deve stabilire regole chiare per ogni dipendente per la corretta gestione di tutti i dati elettronici o cartacei detenuti all'interno dell'azienda. Seguendo queste regole si rispettano i requisiti del GDPR per quanto riguarda il trattamento di tutti i dati. Ad esempio, è possibile che si desideri introdurre regole chiare sull'uso di documenti cartacei contenenti informazioni sensibili e sul processo per la corretta distruzione del documento una volta utilizzato, in base al livello di sensibilità dei dati in esso contenuti.

Processi

Si riferisce ai processi all'interno dell'organizzazione. Ad esempio, per gestire l'uso di dati quali l'elaborazione o l'archiviazione di dati sui clienti. È fondamentale che le aziende rivedano tutti i loro attuali processi relativi ai dati. Una volta individuate le lacune e le debolezze delle procedure esistenti, l'impresa dovrà elaborare un piano quadro per rafforzare o sostituire tali settori, se necessario, al fine di ottemperare alle disposizioni del GDPR.

Tecnologia

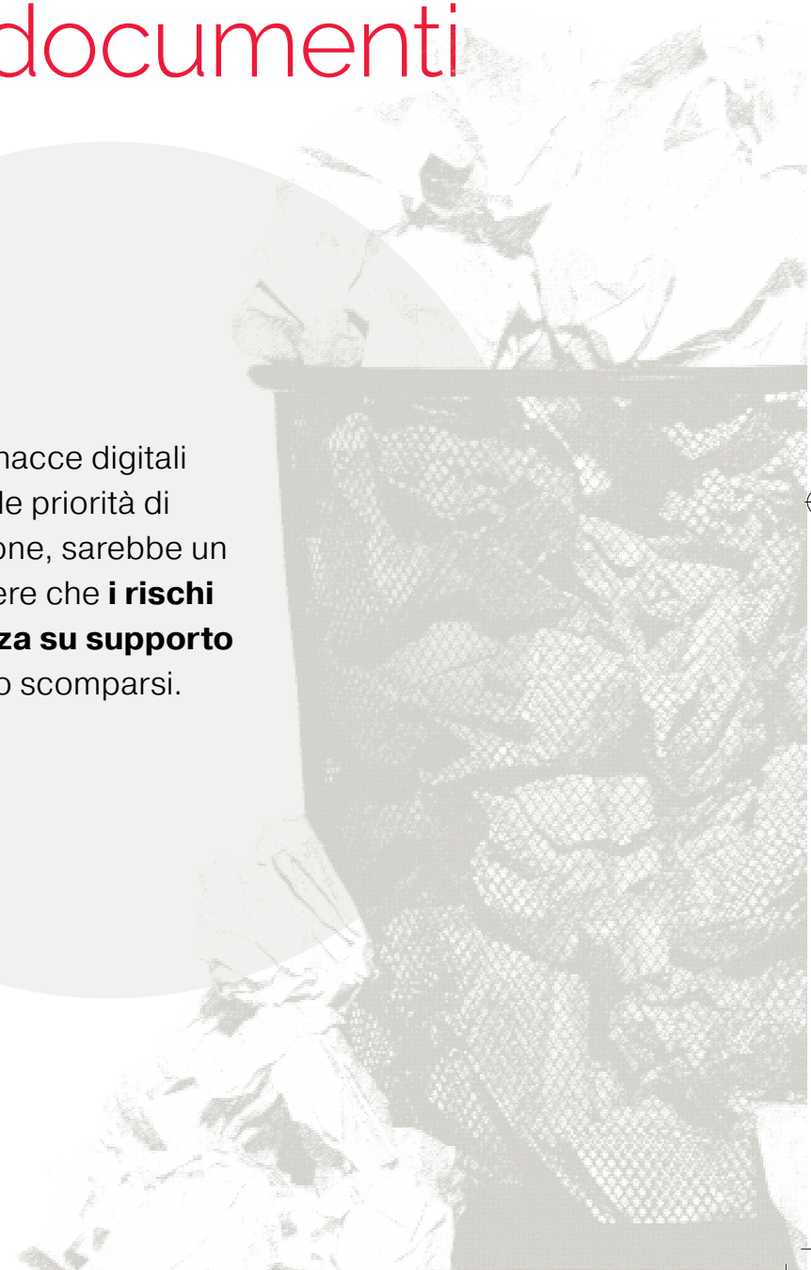
Anche le capacità e i requisiti IT attuali dovrebbero essere rivisti e adeguati di conseguenza. Spetta alle singole imprese garantire che i sistemi esistenti che non rispettano pienamente la normativa siano migliorati o sostituiti, per evitare di incorrere in potenziali sanzioni pecuniarie.

Perché la sicurezza dei documenti cartacei è importante?

Dopo aver discusso di ciò che il GDPR richiede alle imprese, è ora opportuno affrontare la questione della sicurezza dei documenti cartacei all'interno delle organizzazioni e del motivo per cui è una preoccupazione fondamentale per le imprese al fine della soddisfazione dei requisiti del GDPR.

Infatti, un rapporto PwC del 2014, in collaborazione con l'azienda di gestione degli archivi Iron Mountain[2] - che ha intervistato le aziende europee di medie dimensioni per capire come percepiscono e gestiscono il loro rischio legato alle informazioni - ha rilevato che due terzi delle aziende degli intervistati ha affermato che la gestione dei rischi associati alle registrazioni cartacee è una delle preoccupazioni principali.

Anche se le minacce digitali sono in cima alle priorità di un'organizzazione, sarebbe un errore presumere che **i rischi per la sicurezza su supporto cartaceo** siano scomparsi.

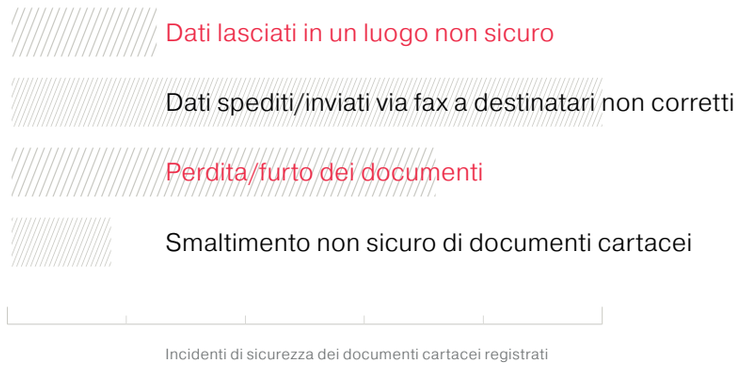


I documenti cartacei sono ancora all'origine di molte violazioni della sicurezza comune

Dei 598 incidenti in materia di sicurezza dei dati registrati tra luglio e settembre 2016 dall'autorità britannica di regolamentazione della protezione dei dati, l'Ufficio del commissario per l'informazione (ICO):

Il 14% è dovuto a smarrimento o furto di documenti cartacei. Un ulteriore 19% è dovuto alla spedizione o all'invio via fax al destinatario sbagliato. **Un altro 3%** è dovuto allo smaltimento insicuro della carta. Pertanto, nonostante un aumento esponenziale delle tecnologie digitali, **il 40% degli incidenti** è imputabile al settore cartaceo[3].

Il 40% **degli incidenti legati alla sicurezza dei dati nel Regno Unito è stato attribuito alla carta.**



La cooperazione tra gli utenti è fondamentale per la conformità con il GDPR

Se possiamo concludere che la sicurezza della carta rimane essenziale per la sicurezza delle informazioni, la domanda è: **che cosa possono fare le organizzazioni al riguardo?**

Rexel è specializzata nella fornitura di distruggi documenti per carta alle organizzazioni e, grazie alla possibilità di collaborare direttamente con organizzazioni come Kensington, leader mondiale nella sicurezza fisica per l'hardware IT quando condividiamo le opinioni dei clienti, siamo in grado di ottenere preziose informazioni sulle esigenze, i desideri e le sfide che le organizzazioni devono affrontare per proteggersi e ottemperare alle disposizioni del GDPR.

Queste informazioni preziose ci hanno fatto comprendere che ci sono due ostacoli principali per l'efficace distruzione dei documenti all'interno delle organizzazioni:

Mancanza di consapevolezza

Le imprese ignorano l'importanza della carta in un ambiente di lavoro sempre più digitale e pertanto non si prendono il tempo necessario per affrontare i problemi di sicurezza associati ai documenti cartacei. Anche quando esiste una politica interna, se la regolamentazione non è comunicata efficacemente a tutti i livelli dell'azienda, spesso porta a una mancanza di consapevolezza.

Facilità d'uso

La disponibilità di macchine distruggidocumenti adeguate è fondamentale per il successo di un'efficace politica di distruzione dei documenti.
Troppo spesso le organizzazioni o gli uffici si affidano a distruggidocumenti manuali inefficaci che non sono adatti a soddisfare le loro esigenze, non permettendo ai dipendenti di distruggere i documenti in modo efficace e produttivo.

Una volta individuate le barriere che ostacolano l'attuazione di un'efficace politica di distruzione dei documenti all'interno dell'organizzazione, il passo successivo riguarda l'individuazione di una soluzione adeguata per superare questi ostacoli.

Soluzione 1
per la conformità al GDPR

Mancanza di consapevolezza

In generale, i dipendenti svolgono attività che sono chiaramente evidenziate come prioritarie dai loro manager.

Con questo in mente, una politica chiara e decisa sulla distruzione dei documenti può risolvere molte inefficienze.

L'indagine PwC/Iron Mountain[2] del 2014 sulle società europee di medie dimensioni rileva che solo il 40% dispone di linee guida chiare per i dipendenti riguardo allo smaltimento interno e alla conservazione dei documenti fisici e solo il 27% implementa politiche aziendali per la sicurezza, la conservazione e la distruzione delle informazioni riservate.

Soluzione 2
per la conformità al GDPR

Facilità d'uso

Una seconda causa comune di non conformità dei dipendenti in materia di distruzione dei documenti riguarda la difficoltà e il consumo di tempo associati a questo compito.

Mentre alcuni lavoratori possono avere accesso alle macchine distruggi documenti, non tutti i lavoratori possono distruggere i documenti dovuti se l'attività richiede molto tempo o è difficile da gestire.

Non sorprende che nessuna organizzazione voglia investire in macchinari che i propri dipendenti potrebbero evitare di utilizzare a causa della scarsa produttività o delle barriere di facilità d'uso, quindi questi problemi dovrebbero essere risolti per garantire il massimo utilizzo.

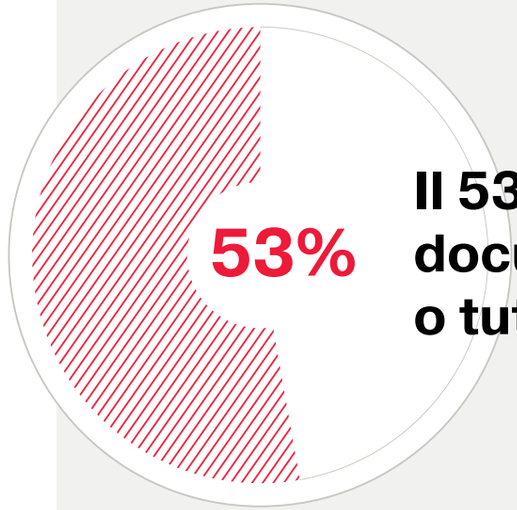
Aumenta la produttività dei dipendenti con la tecnologia di alimentazione automatica Auto Feed.

Conclusioni

Fate in modo di far rispettare i criteri di sicurezza dei documenti cartacei con i distruggi documenti Auto+ SmarTech.

I nostri distruggidocumenti Auto+ SmarTech dispongono di un sistema di auto-alimentazione della carta, consentono il monitoraggio e la manutenzione in più punti e sono la risposta diretta per incoraggiare il rispetto della sicurezza dei documenti cartacei da parte dei dipendenti. Una ricerca[4] mostra che il 53% dei dipendenti adotta un comportamento di distruzione a plichi di documenti, per cui il dipendente di solito accumula una pila di documenti diversi prima di giustificare l'utilizzo di una macchina distruggidocumenti.

Consentendo ai dipendenti di distruggere pile di carta, una ricerca indipendente ha scoperto che in effetti potrebbero impiegare il 98% in meno di tempo[5] nella distruzione ed essere quindi più inclini a distruggere i documenti più frequentemente.



Il 53% distrugge i documenti in plichi o tutto in una volta

14 min. 25 sec.
Manualmente

14 sec. con le macchine distruggi-documenti Rexel Auto+

Tempo necessario per distruggere 500 fogli

Piano d'azione **GDPR a 6 punti** per la vostra azienda

1. Nominare un responsabile della protezione dei dati

Questo addetto deve essere pienamente in linea con le responsabilità dell'organizzazione in materia di GDPR e avere una conoscenza approfondita di quali dati all'interno dell'organizzazione sono considerati "personali", dove sono conservati, chi vi ha accesso, come individuare le violazioni quando si verificano e a chi segnalarle. Il responsabile della protezione dei dati non deve necessariamente essere un dipendente, ma è possibile esternalizzare questa funzione.

2. Valutare i sistemi

Rivedere tutti i contratti, il supporto tecnologico, le procedure e gli strumenti relativi all'elaborazione, alla gestione, all'archiviazione e alla cancellazione dei dati per consentire di individuare eventuali punti deboli o lacune che richiedono modifiche.

3. Sviluppare una strategia

Elaborare una nuova strategia che garantisca il pieno rispetto del GDPR. Questa strategia può comprendere nuovi investimenti in tecnologia, la revisione delle procedure del personale e della responsabilità per l'elaborazione dei dati, la creazione di nuovi ruoli all'interno dell'organizzazione.

4. Attuare una nuova politica organizzativa

Il prossimo passo verso la conformità al GDPR è mettere in atto il vostro piano a tutti i livelli dell'organizzazione. Investire e introdurre le nuove tecnologie e i nuovi sistemi necessari sul posto di lavoro e pubblicare una guida informativa sulla gestione e l'elaborazione dei dati.

5. Coinvolgimento dei dipendenti

Inviate la vostra nuova politica di conformità dei dati a tutto il personale; fornite corsi di formazione, informazioni e linee guida ai dipendenti affinché siano informati e consapevoli dei cambiamenti in atto e della loro responsabilità nel garantire che l'azienda soddisfi i requisiti del GDPR.

6. Revisione e miglioramento

Dopo aver avviato il vostro piano di conformità al GDPR, questo deve essere continuamente rivisto e migliorato, anche dopo l'entrata in vigore delle normative. Identificare continuamente i miglioramenti necessari riuscirà a garantire con successo ed efficienza che la vostra organizzazione sia completamente conforme.

Fonti

1 envirowaste.it/blog/articoli/documenti di società terze-shred-private-documenti

2 Al di là delle buone intenzioni: La necessità di passare dall'intenzione all'azione per gestire il rischio informativo nel mercato di fascia media, rapporto PwC in collaborazione con Iron Mountain, giugno 2014

3 ico.org.uk/action-weve-taken/data-security-incident-trends

4 Valutazione dei trituratori ad alimentazione automatica. Preparato per ACCO Brands da Deep Blue Insight

5 Test indipendente a opera di Intertek Testing & Certification Ltd Giugno 2012

- Massimo risparmio con l'utilizzo di un Auto+ 500X con SmarTech rispetto a un trituratore ad alimentazione tradizionale a un livello di prezzo simile
- Le ricerche dimostrano che l'inserimento manuale di 500 fogli richiede in media 14 minuti e 25 secondi in un tradizionale trituratore ad alimentazione manuale, ma solo 14 secondi per caricare lo stesso numero di fogli in un Auto+ 500X con SmarTech

www.rexeleurope.com

Per ulteriori informazioni, contattare:
Esselte Srl
Via Milano, 35
20064 Gorgonzola (MI)
Telefono: +39 02 950991
Fax: +39 02 95300415
e-mail: esselte.italia@acco.com