



Distruggidocumenti Rexel

Perché una politica di sicurezza cartacea è parte integrante della conformità al regolamento detto GDPR (General Data Protection Regulation)?

Liberatoria

Nulla di quanto contenuto nel presente documento deve essere interpretato come un consiglio legale.

Le organizzazioni devono consultare un consulente legale in merito alla conformità al Regolamento Generale per la Protezione dei Dati o qualsiasi altra legge o regolamentazione applicabile.

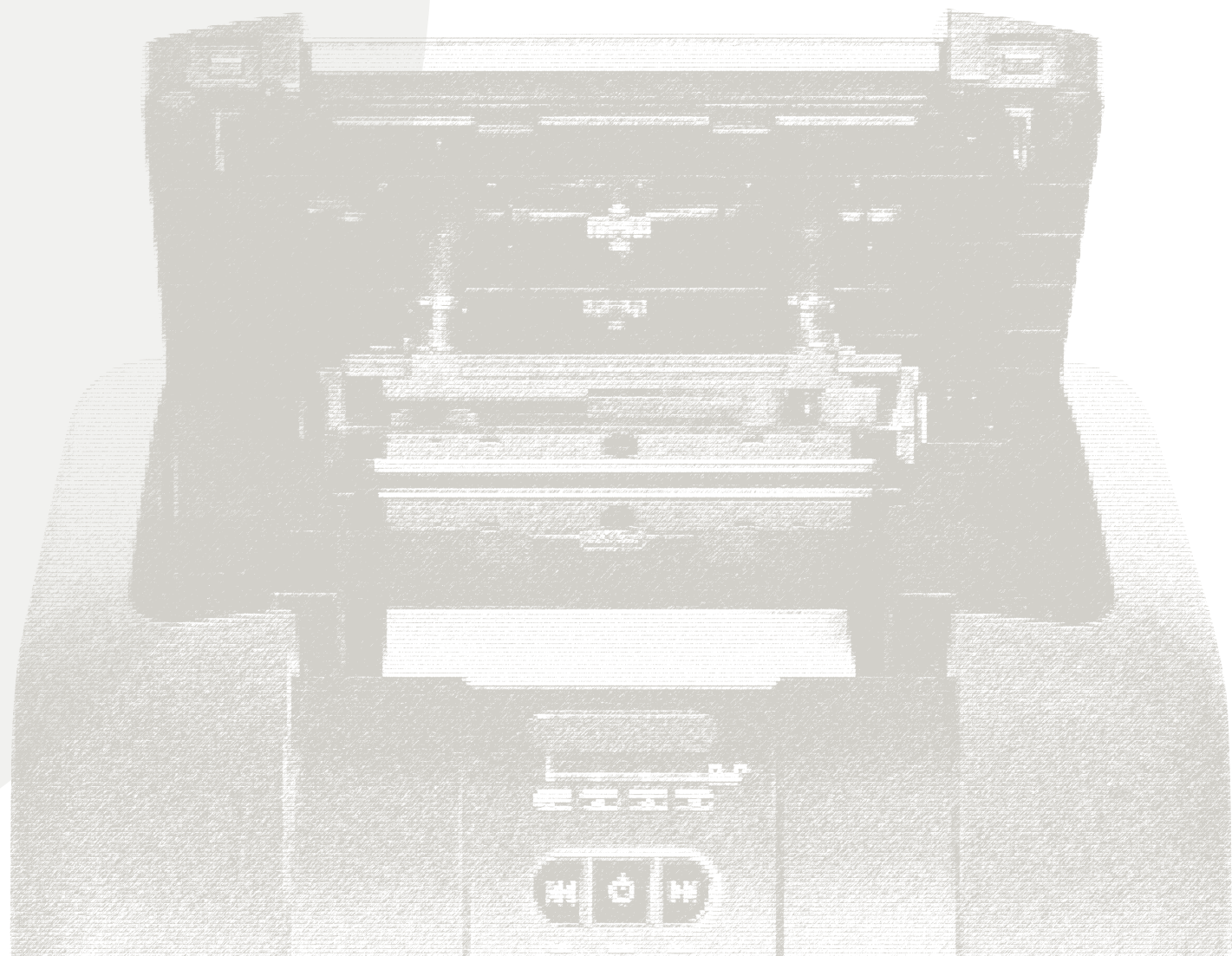
In merito a **questo documento**

Questa informativa fornisce **una panoramica di ciò che il GDPR vuole raggiungere**, i problemi che può presentare alle organizzazioni.

Lo scopo del presente documento è fornire un'introduzione al Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea e informare circa le modalità con cui influenzerà diverse aziende, in modo da sviluppare una politica di sicurezza dei documenti cartacei della propria azienda in anticipo rispetto a tali normative che entreranno in vigore nel maggio 2018.

Quindi che cos'è il GDPR? Questo regolamento richiede alle organizzazioni di applicare solide pratiche di sicurezza per i dati elettronici e cartacei e, in caso di violazione della protezione dei dati, di informare i soggetti interessati o potenzialmente interessati. La portata del GDPR include a livello globale tutte le organizzazioni che controllano o elaborano dati di identificazione personale in merito a persone nell'UE, indipendentemente dall'area geografica d'intervento di tali organizzazioni. Le direttive del GDPR si applicano ai dati personali elettronici e cartacei e richiedono che tutte le organizzazioni debbano soddisfare i requisiti del GDPR se trattano dati di identificazione personale all'interno dell'UE.

Sebbene la sicurezza elettronica dei dati rappresenti giustamente la preoccupazione principale di molte organizzazioni, molte altre non riescono ad affrontare adeguatamente la sicurezza dei dati cartacei. Infatti, quasi due terzi degli uffici ammette di non distruggere informazioni riservate¹. Una tale situazione può portare le organizzazioni a violare il GDPR e sottoporre le persone interessate a rischio di frode e furti di identità. Con questo scopo, Rexel, marchio leader di distruggidocumenti, incoraggia le organizzazioni a riesaminare le proprie politiche e pratiche di sicurezza relative ai dati cartacei e elettronici.



IL REGOLAMENTO GENERALE DI PROTEZIONE DEI DATI

Una panoramica

Il GDPR cerca di proteggere i diritti della privacy delle persone in Europa, siano essi cittadini dell'UE o meno. Questi diritti di privacy comprendono, ma non sono limitati a:

Trasparenza

Il diritto di ricevere informazioni chiare sulle modalità con cui le organizzazioni elaborano le informazioni personali.

Consenso

Il diritto di controllare le modalità con cui le organizzazioni utilizzano le informazioni personali.

Sicurezza

Il diritto di avere informazioni sulle modalità con cui le organizzazioni proteggono adeguatamente le informazioni personali.

Limitazione di finalità e raccolta

Il diritto di pretendere che le organizzazioni riducano al minimo la raccolta e gli utilizzi.

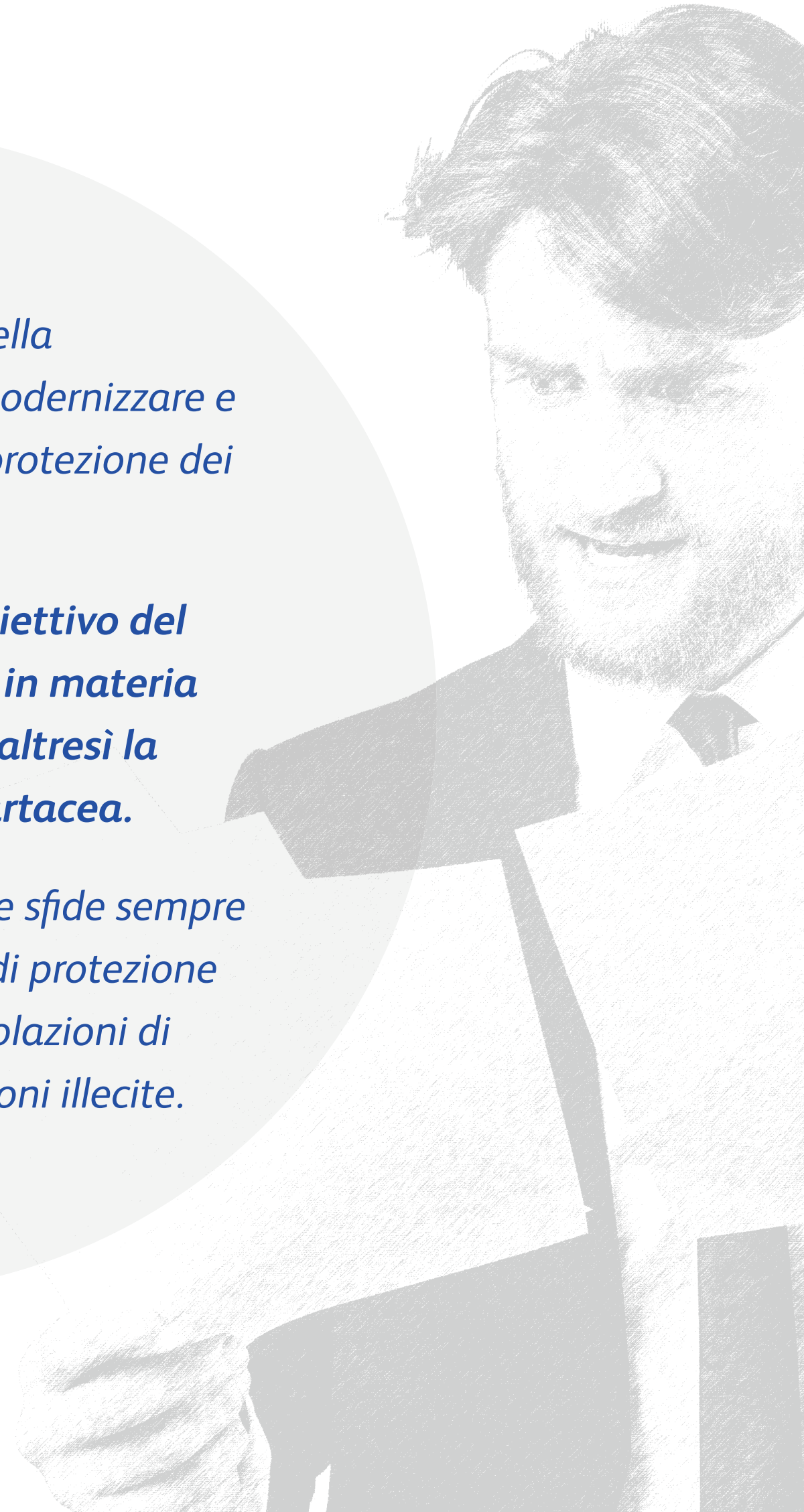
Notifica di violazione

Il diritto di essere informati in caso di violazione della sicurezza dei dati.

Il GDPR fa parte del piano della Commissione Europea per modernizzare e armonizzare le norme sulla protezione dei dati.

Nonostante il principale obiettivo del GDPR sia rafforzare i diritti in materia di privacy on-line, affronta altresì la privacy dei dati in forma cartacea.

Si concentra sull'affrontare le sfide sempre più impegnative in materia di protezione dei dati e privacy, rischi di violazioni di sicurezza, hacking e altre azioni illecite.



Cosa cambia?

I seguenti punti **individuano aree specifiche all'interno del GDPR che rappresentano nuovi** diritti per individui o diritti esistenti ai sensi della legge sulla protezione dei dati (Data Protection Act o DPA) rafforzati nell'ambito del GDPR:

Trasferimento dei dati e il diritto ad essere dimenticato

- Gli individui 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 una macchina.
- Una persona può richiedere la cancellazione o la rimozione dei dati personali.

Notifica di violazione dei dati

- Ogni violazione deve essere segnalata all'autorità di vigilanza.
- Devono essere informati anche gli individui interessati dalla violazione.

Inventario

- Le autorità locali non devono più essere informate in merito alla elaborazione dei dati personali.
- Le organizzazioni devono mantenere una documentazione delle attività di elaborazione sotto la propria responsabilità.

Valutazione dell'impatto sulla protezione dei dati e sicurezza

- Le valutazioni d'impatto sulla protezione dei dati sono un mezzo per identificare alti rischi per i diritti della privacy degli individui.
- I requisiti di sicurezza e le raccomandazioni dovrebbero basarsi su una valutazione del rischio.

Gestione dei dati e responsabilità

- Le organizzazioni devono inoltre essere in grado di dimostrare la conformità con il GDPR.

La mancata osservanza del GDPR può far incorrere in **multe fino a 20 milioni di euro o fino al 4% dei fatturati globali aziendali**. Inoltre, un soggetto interessato ha il diritto di denunciare un'organizzazione in un tribunale.

IL REGOLAMENTO GENERALE DI PROTEZIONE DEI DATI

A chi si applica?

L'introduzione del GDPR, nel maggio 2018, riguarderà i seguenti ruoli:

Titolari del trattamento: coloro che dichiarano come e perché vengono elaborati i dati personali.

Processori di dati: persone che agiscono per conto del titolare del trattamento.

La responsabilità di queste due figure è garantire che i loro clienti siano pienamente conformi a tutti gli aspetti del GDPR per evitare di incorrere in sanzioni.

Un Titolare del trattamento o Processore di dati **deve nominare un Funzionario della protezione dei dati** e tenere registri di tutte le attività di elaborazione che svolgono per conto dei clienti.



Il GDPR tratta dei dati personali e dei dati personali sensibili in formato elettronico e fisico

È importante esaminare a quali tipi di dati si applica il GDPR prima di redigere una politica di conformità per l'organizzazione.

I dati che rientrano nel campo di applicazione del GDPR includono tutte le informazioni su una persona che può essere identificata. Alcuni esempi di dati personali trattati dal GDPR includono nome completo, indirizzo e-mail e numero di telefono.

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

Il GDPR verte su dati personali gestiti dalle organizzazioni **sia in formato elettronico che fisico**, ad esempio documenti cartacei.

Un sistema di riferimento aziendale per la conformità al GDPR

Le organizzazioni hanno tre aree principali che devono essere riesaminate al fine di raggiungere la conformità al GDPR. Affrontando queste tre componenti, le aziende potranno costituire sistemi di riferimento chiari per una politica sulla sicurezza dei dati sotto ogni punto di vista, al fine di aiutare la conformità con tutti gli aspetti del GDPR.

Queste componenti sono:

Persone

La proprietà e la responsabilità del personale per tutti i dati trattati all'interno di ogni organizzazione sono fondamentali. L'organizzazione deve stabilire per ciascun dipendente regole chiare relative alla corretta gestione di tutti i dati elettronici o cartacei presenti all'interno dell'azienda. Tali norme devono mettere in pratica i requisiti del GDPR riguardanti la gestione di tutti i dati. Ad esempio, sarebbe ideale introdurre regole chiare sull'utilizzo di documenti cartacei contenenti informazioni riservate e sulla procedura per la corretta distruzione dei documenti una volta utilizzati, a seconda del livello di sensibilità dei dati in essi contenuti.

Processi

Questo riguarda i processi all'interno dell'organizzazione. Quali ad esempio l'elaborazione o l'archiviazione dei dati dei clienti. È fondamentale che le aziende riesaminino tutti i loro processi attuali relativi alle informazioni. Una volta individuate lacune e carenze delle procedure esistenti, è necessario sviluppare un piano quadro aziendale volto ad assicurare che queste aree siano rafforzate o sostituite, ove necessario, per conformarsi al GDPR.

Tecnologia

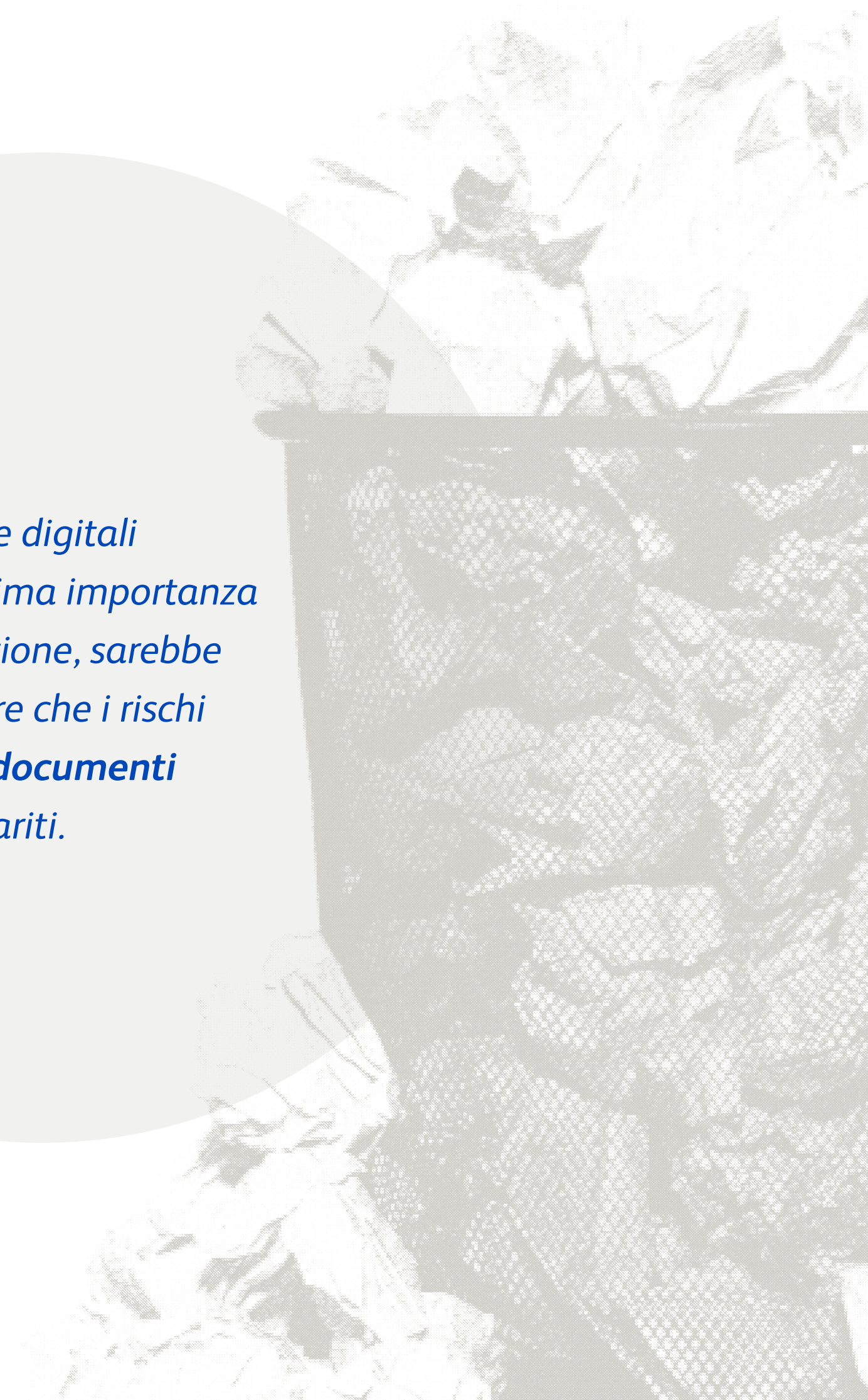
Inoltre le attuali capacità e requisiti IT dovrebbero essere rivisti e adeguati di conseguenza entro maggio 2018. È compito di ogni azienda assicurarsi che tutti i sistemi esistenti non pienamente conformi ai regolamenti siano migliorati o sostituiti, per evitare eventuali multe dopo l'entrata in vigore del GDPR.

Perché è importante la sicurezza dei documenti cartacei?

Dopo aver analizzato ciò che il GDPR richiede alle aziende, è ora opportuno affrontare la questione della sicurezza dei documenti cartacei nelle organizzazioni e perché si tratta di una questione fondamentale per le aziende che si apprestano a soddisfare i requisiti del GDPR.

Infatti, un rapporto di PwC del 2014, in collaborazione con la società per la gestione delle documentazioni Iron Mountain², in merito a come le società europee della fascia media di mercato percepiscono e gestiscono il loro rischio informativo, ha rivelato che due terzi degli intervistati ha affermato che la gestione dei rischi associati ai documenti cartacei era una preoccupazione importante.

*Mentre le minacce digitali rivestono la massima importanza per un'organizzazione, sarebbe un errore ipotizzare che i rischi di sicurezza **per i documenti cartacei** siano spariti.*

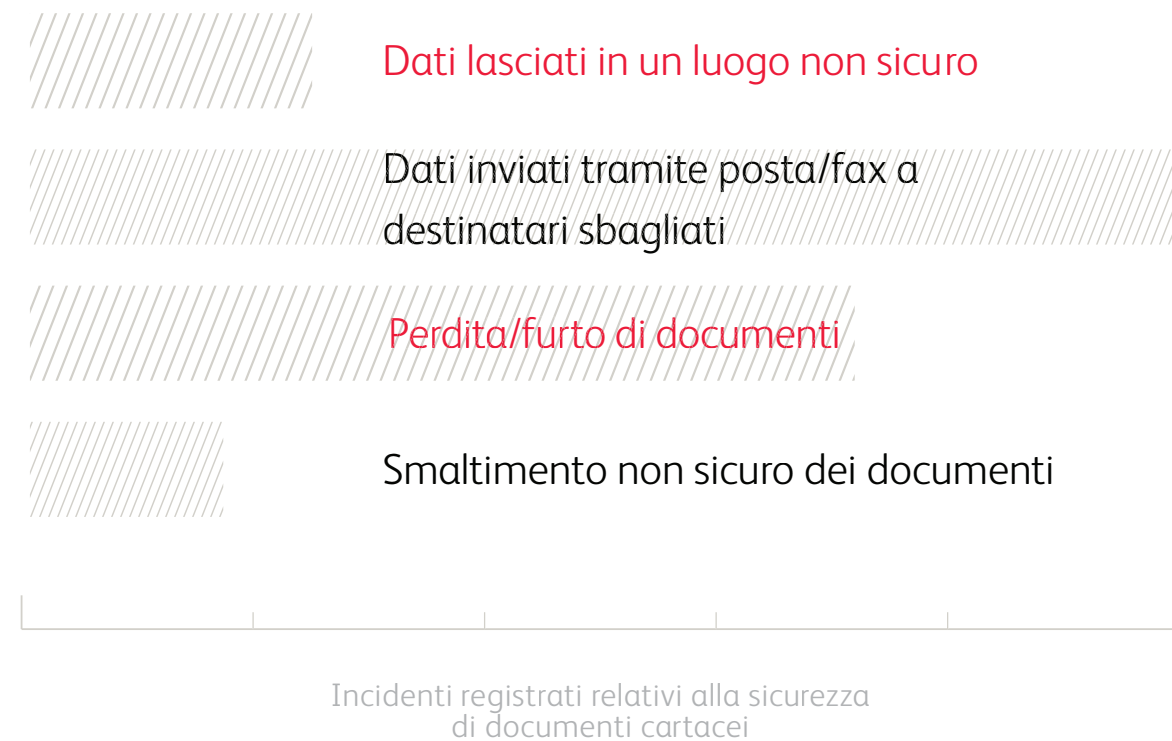


Le documentazioni cartacee sono ancora oggetto di molte **comuni violazioni della sicurezza**

Dei 598 incidenti relativi alla sicurezza dei dati, registrati tra luglio e settembre 2016 dall'Ispettore Generale per la protezione dei dati del Regno Unito, l'ICO (Information Commissioner's Office) riporta che:

Il 14% era dovuto alla perdita o al furto di documenti cartacei, **un ulteriore 19%** erano documenti inviati per posta o fax al destinatario sbagliato **e il 4%** era dovuto a dati lasciati in un luogo non sicuro. **Un altro 3%** era dovuto all'eliminazione non sicura della carta. Quindi, nonostante un aumento esponenziale delle tecnologie digitali, **il 40% degli incidenti** è attribuibile ai documenti di carta³.

Nel Regno Unito, il **40%** degli incidenti relativi alla sicurezza dei dati è stato attribuito a documenti cartacei



La cooperazione degli utenti è fondamentale per rispettare il GDPR

Se si può concludere che la sicurezza dei documenti cartacei rimane fondamentale per la sicurezza delle informazioni, allora la domanda che sorge è:
Cosa possono fare le organizzazioni a tale riguardo?

Rexel è specializzata nella fornitura di distruggidocumenti alle organizzazioni e, la possibilità di collaborare direttamente con organizzazioni quali Kensington, leader mondiale nella sicurezza fisica per l'hardware IT, con cui scambiamo informazioni sulla conoscenza del cliente, ci ha permesso di acquisire preziose informazioni sulle esigenze, i desideri e le problematiche che devono affrontare organizzazioni che cercano di proteggere se stesse e di rispettare il GDPR.

Queste informazioni ci hanno portato a credere che ci siano due barriere principali in merito alla distruzione efficace dei documenti nelle organizzazioni:

Mancanza di consapevolezza

Le imprese ignorano l'importanza della carta in un mondo del lavoro sempre più digitale e pertanto non dedicano il tempo necessario ad affrontare le questioni di sicurezza associate ai documenti cartacei. Anche quando esiste una politica, se le regole non sono comunicate in modo efficace a tutti i livelli aziendali, ciò spesso genera una mancanza di consapevolezza.

Facilità d'uso

La disponibilità di distruggidocumenti adatti 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 in grado di soddisfare le loro necessità, impedendo ai dipendenti di distruggere i documenti in modo efficace e produttivo.

Una volta individuate le barriere all'attuazione di un'efficace politica di distruzione all'interno dell'organizzazione, il passo successivo consiste nel determinare una soluzione adeguata per superare queste barriere.

Prima cooperazione utenti per la conformità al GDPR

Mancanza di consapevolezza

I dipendenti generalmente svolgono attività chiaramente evidenziate come prioritarie dai loro manager.

A questo proposito, una politica chiara e rigorosa di distruzione dei documenti potrebbe risolvere molte inefficienze.

L'indagine del 2014 di PwC/Iron Mountain sulle società europee della fascia media di mercato² osserva che solo il 40% dispone di chiari orientamenti per dipendenti in materia di smaltimento interno e archiviazione di documenti fisici e solo il 27% dispone di politiche aziendali per la sicurezza, l'archiviazione e lo smaltimento delle informazioni riservate.



SOLO
27%

**Le società hanno
politiche per lo
smaltimento di
dati**

Seconda cooperazione utenti per la conformità al GDPR

Facilità d'uso

Una seconda causa comune di non conformità dei dipendenti in merito alla distruzione dei documenti è la difficoltà e il tempo richiesto da tale compito.

Sebbene i dipendenti possano avere accesso ai distruggi-documenti, non tutti possono distruggere i dovuti documenti se l'attività richiede molto tempo o è di difficile gestione.

Non sorprende che nessuna organizzazione desideri investire in distruggidocumenti che i dipendenti probabilmente trascurano di utilizzare a causa di una scarsa produttività o difficile utilizzo, quindi queste barriere dovrebbero essere superate per garantire il massimo utilizzo.



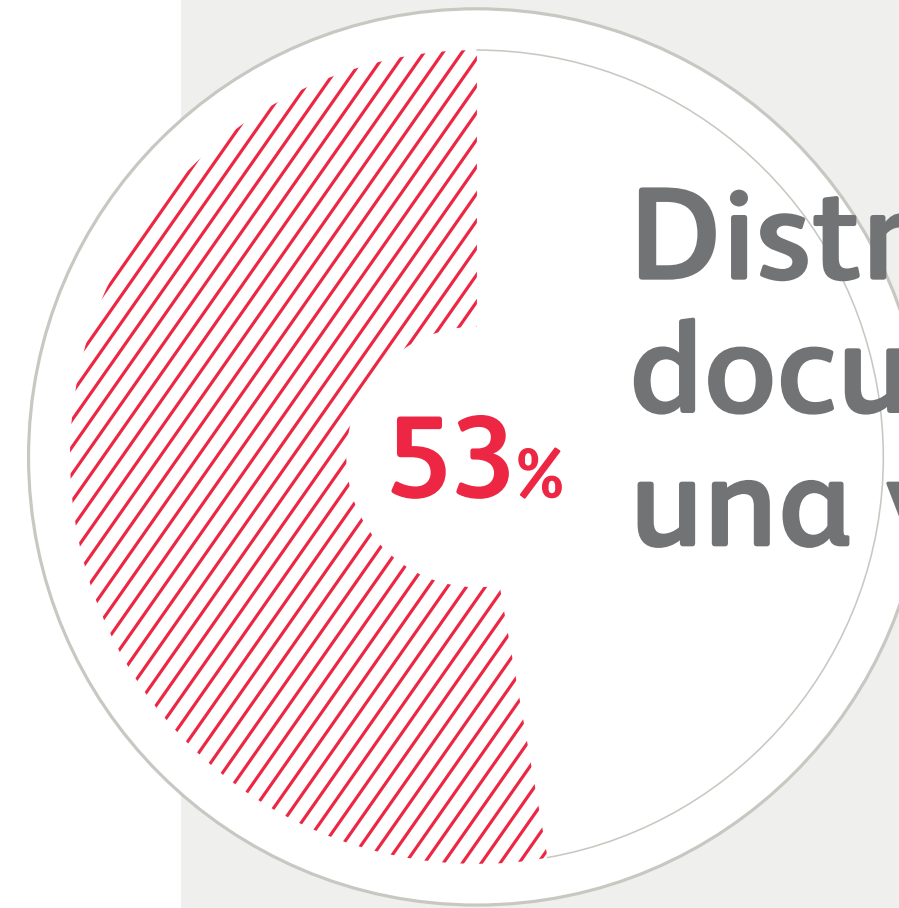
**Aumenta la produttività
dei dipendenti con
la tecnologia di
alimentazione automatica**

Conclusione:

I distruggidocumenti ad alimentazione automatica sono una soluzione immediata alla necessità aziendale di incoraggiare la conformità dei dipendenti alle norme per la sicurezza cartacea.

La nostra ricerca⁴ dimostra che il 53 % dei dipendenti crea una pila di documenti prima di ritenere che sia necessario utilizzare il distruggidocumenti.


Creando pile di documenti cartacei, secondo una ricerca indipendente, i dipendenti potrebbero spendere **il 98% di tempo in meno per la distruzione**⁵ ed essere più inclini a distruggere più frequentemente.



Distruzione di pile di documenti o tutto in una volta sola

14 minuti e
25 secondi
manualmente

14 secondi
con distruggi-
documenti Rexel
Auto+



Tempo
richiesto per
distruggere
500 fogli

The stopwatch illustration shows a red needle pointing to a very small amount of time on the right side of the dial, representing the 14 seconds for the automatic shredder. The left side of the dial is mostly empty, representing the 14 minutes and 25 seconds for manual shredding.

6 punti chiave da considerare per il GDPR



1. Prendere in considerazione la nomina di un Funzionario per la protezione dei dati

Questo funzionario deve essere pienamente all'altezza della responsabilità organizzativa in materia di GDPR e deve avere una approfondita comprensione di quali dati all'interno dell'organizzazione sono considerati "personali", dove sono tenuti, chi vi ha accesso, come individuare le violazioni quando si verificano e a chi segnalarle. **Il Funzionario della protezione dei dati non deve essere un dipendente, è possibile esternalizzare questa funzione.**



2. Valutazione dei sistemi

Rivedere tutti i contratti, il supporto tecnologico, le procedure e gli strumenti che riguardano l'elaborazione, la gestione, l'archiviazione e l'eliminazione dei dati per individuare eventuali debolezze o lacune che richiedono modifiche.



3. Sviluppo di una strategia

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



4. Attuazione di una nuova politica organizzativa

Il prossimo passo verso la conformità al GDPR è attuare il proprio piano a tutti i livelli dell'organizzazione. Investire e introdurre nuove tecnologie e sistemi necessari sul posto di lavoro e pubblicare una guida informativa per la gestione dei dati e delle procedure.



5. Impegno dei dipendenti

Far conoscere la nuova politica di conformità in materia di informazioni a tutto il personale; fornire formazione, informazioni e guide ai dipendenti in modo che siano istruiti e consapevoli dei cambiamenti e della loro responsabilità nel garantire che l'azienda soddisfi i requisiti del GDPR.



6. Revisioni e miglioramenti

Dopo aver lanciato il piano di conformità al GDPR, ora è il momento di rivederlo e migliorarlo prima che i regolamenti entrino in vigore. Individuare i miglioramenti necessari ben prima della data di efficacia del GDPR di modo che, una volta giunto maggio 2018, l'organizzazione si adatterà efficacemente e con successo ai cambiamenti e sarà completamente conforme.

FONTI

- 1 envirowaste.co.uk/blog/articles/third-companies-shred-private-documents
- 2 Oltre le buone intenzioni: La necessità di passare dall'intenzione all'azione per gestire il rischio delle informazioni nella fascia media di mercato, rapporto di PwC in collaborazione con Iron Mountain, giugno 2014.
- 3 ico.org.uk/action-weve-taken/data-security-incident-trends
- 4 Valutazione dei distruggidocumenti ad alimentazione automatica. Preparata per ACCO Brands da Deep Blue Insight
- 5 Test indipendenti da Intertek Testing & Certification Ltd giugno 2012.
Massimo risparmio quando si utilizza Auto+ 500X rispetto ad un distruggidocumenti ad alimentazione tradizionale in una fascia di prezzo simile.
La ricerca indica che occorre una media di 14 minuti e 25 secondi per inserire manualmente 500 fogli di carta in un distruggidocumenti tradizionale ad alimentazione manuale, ma solo 14 secondi per caricare lo stesso numero di fogli in un distruggidocumenti Auto+ 500X.