L'adozione di **NUOVI MODELLI DI LAVORO** aumenta il rischio di violazione dei dati per le aziende?

Fellowes Studio **"Metti al sicuro i dati" 2022.** Un report sulla **DISTRUZIONE DEI DOCUMENTI** in un mondo del lavoro ibrido.

Premessa

> “Molte delle organizzazioni che sono passate al modello di lavoro in remoto all’inizio del 2020 ritengono di non aver avuto il tempo sufficiente per condurre le appropriate valutazioni dei rischi prima di introdurre cambiamenti così profondi nelle pratiche di lavoro aziendali.”

“L’attenzione di tutti era rivolta a garantire la continuità dei servizi piuttosto che a valutare i rischi associati all’introduzione dei cambiamenti necessari. Anche i dipendenti non hanno avuto tempo di adattarsi al nuovo metodo di lavoro e, come emerso da molti studi, la diffusione del telelavoro durante la pandemia è stata accompagnata da un aumento di inadeguate pratiche di sicurezza dei dati.

Facendo un salto in avanti nel 2022, si noterà che i metodi di lavoro si sono evoluti rapidamente, con un numero record di dipendenti che continuano a lavorare in modalità ibrida anche dopo essere tornati in ufficio all’indomani della pandemia. Ma le aziende hanno introdotto e adattato i loro processi interni? E il nuovo modello di lavoro espone le aziende a maggiori rischi di violazione di dati?

- La risposta è affermativa per entrambe le domande. Il 50% degli intervistati ritiene che il lavoro ibrido abbia aumentato le violazioni di informazioni sensibili così come le violazioni al GDPR (Regolamento generale sulla protezione dei dati). Se da un lato, i documenti cartacei non sono stati una priorità nelle politiche aziendali di protezione dei dati, dall’altro la rapida transizione al lavoro ibrido ha portato a migliaia di documenti in più che passano tra casa e lavoro ogni settimana. Questo fa emergere un’importante questione sui documenti cartacei riservati e su come proteggerli in una realtà dove molti dipendenti non lavorano più solo negli uffici aziendali.

Per approfondire l’esperienza quarantennale di Fellowes nello sviluppo di soluzioni distruggidocumenti, abbiamo voluto esplorare come i dipendenti proteggono e distruggono i documenti cartacei nel modello di lavoro ibrido allargato e in che misura le organizzazioni si sono conformate ai requisiti del GDPR a quattro anni dalla sua entrata in vigore. Fin dagli inizi, Fellowes ha sviluppato soluzioni distruggidocumenti pensando alle esigenze di ogni ambiente di lavoro. Siamo impegnati a proteggere le aziende e gli individui in qualsiasi ambiente di lavoro, impedendo che i documenti cartacei sensibili finiscano in mani sbagliate.

In collaborazione con B2B International, abbiamo condotto un sondaggio tra 605 utenti di soluzioni distruggidocumenti operanti nel settore finanziario, nel settore pubblico e nel settore dell’assistenza sanitaria in Francia, Germania e Regno Unito.

Questa relazione esamina le tendenze e i comportamenti concernenti la sicurezza dei dati in un mondo del lavoro in costante evoluzione, con l’obiettivo di accompagnare le aziende in questa transizione. Infatti, distruggere i documenti in modo sicuro, in qualsiasi ambiente di lavoro, è fondamentale per limitare i rischi di sicurezza che incombono sulle organizzazioni”.

Steven Hickey

Cronologia

1982
DISTRUGGIDOCUMENTI COMMERCIALI:
Fellowes conclude un accordo di licenza con una società tedesca per la produzione di distruggidocumenti commerciali

1990
IL PRIMO DISTRUGGIDOCUMENTI PERSONALE:
È annunciata un’invenzione, il distruggidocumenti personale

2005
SAFESENSE™
La tecnologia Fellowes SafeSense™ rende i distruggidocumenti per uso domestico ancora più sicuri

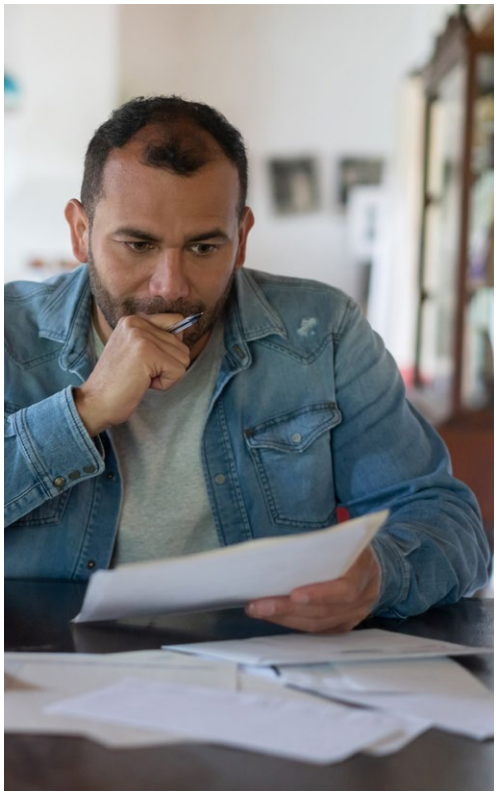
2008
DISTRUGGIDOCUMENTI 100% ANTI-INCEPPAMENTO
Nasce la linea di distruggidocumenti con tecnologia 100% anti-inceppamento di Fellowes

2014
DISTRUGGIDOCUMENTI AUTOMATICI AUTOMAX™:
Fellowes presenta i distruggidocumenti ad alimentazione automatica AutoMax™ che migliorano la produttività in ufficio

2020
SERIE LX:
Sono introdotti i più avanzati distruggidocumenti a microframmento di Fellowes progettati per qualsiasi ambiente di lavoro.

Il GDPR e la protezione dei dati in un ambiente di lavoro ibrido

Dalla nostra ricerca è emerso che **8 intervistati su 10** hanno adottato il telelavoro a tempo pieno o parziale. Il lavoro ibrido, cioè una combinazione di lavoro in ufficio e da remoto, ha sicuramente portato maggiore flessibilità e varietà nella scelta del luogo di lavoro, ma ha anche introdotto una sfida costante per le aziende, cioè garantire che i loro dipendenti comprendano le regole sulla riservatezza dei dati e applichino le buone pratiche di protezione dei dati ovunque lavorino.



Che i dipendenti siano in ufficio, a casa, in spazi di lavoro comuni o altrove, le aziende devono essere in grado di gestire i rischi di sicurezza. Il primo passo consiste nello studiare le aree che possono esporre l'azienda a nuovi rischi. Le aziende dovrebbero, ad esempio, attuare rigorose politiche sull'uso di computer, tablet e smartphone personali a fini lavorativi non potendo controllare la configurazione e l'utilizzo di tali dispositivi come farebbero in ufficio. Un'altra area di attenzione sono le reti Wi-Fi pubbliche e private e l'uso di password deboli o ripetute. Queste sono infatti due aree di vulnerabilità comunemente sfruttate dai criminali informatici ed è importante comunicare istruzioni chiare ai dipendenti per garantire la protezione dei dati aziendali.

E non è una sorpresa per noi che i documenti cartacei siano uno dei rischi di sicurezza più sottovalutati dalle aziende. In un mondo del lavoro prevalentemente digitale, talvolta le aziende dimenticano di includere i dati cartacei nelle loro politiche di sicurezza. Ma è importante notare che la maggior parte delle aziende (68%) che hanno partecipato al nostro sondaggio dichiarano di gestire ogni giorno un grande volume di informazioni cartacee sensibili. Il **70%** degli intervistati afferma di portare a casa documenti di lavoro stampati, di stampare documenti di lavoro a casa o di fare entrambe le cose. Di questa percentuale, la metà

Qualche dubbio sui dettagli del GDPR? Cosa devi sapere...

Il Regolamento generale sulla protezione dei dati (GDPR), entrato in vigore nel maggio 2018, ha introdotto un quadro completo di requisiti in materia di protezione dei dati che si applicano al trattamento dei dati personali dei cittadini europei. Qualsiasi organizzazione che gestisce informazioni personali deve infatti rispettare rigorosi requisiti in materia di raccolta, finalità e protezione dei dati.

I dati personali devono essere trattati in modo sicuro attraverso l'implementazione di adeguate misure tecniche e organizzative che ne garantiscano la protezione contro il trattamento illecito o non autorizzato e contro la perdita accidentale, la distruzione o il danno.

Cosa sono i dati personali?

I dati personali sono qualsiasi informazione correlata a un individuo che permetta di identificarlo. Alcuni esempi sono nomi, indirizzi, codici fiscali, dati dei profili di social media, registrazioni di telecamere a circuito chiuso o fotografie. I dati personali possono essere in formato digitale o cartaceo.

Quali sono le conseguenze delle violazioni al GDPR?

Una violazione dei dati personali può risultare in sanzioni pari al 4% del fatturato globale dell'azienda o 20 milioni di euro nonché danneggiare la reputazione dell'azienda.

I 6 principi della protezione dei dati

Ogni strategia per la protezione dei dati deve includere i seguenti principi:

- **I dati sono trattati in modo lecito, equo e trasparente**
- **I dati sono raccolti per finalità specifiche, esplicite e legittime e non possono essere trattati per finalità diverse dalle originali in un secondo momento**
- **I dati sono adeguati, pertinenti e limitati a quanto strettamente necessario**
- **I dati sono accurati e aggiornati Qualsiasi inesattezza deve essere gestita, eliminata e corretta**
- **I dati sono mantenuti solo per il periodo di tempo strettamente necessario**
- **I dati sono trattati in modo sicuro**

Maggiori informazioni sul Regolamento generale sulla protezione dei dati - Fellowes®

afferma di gettare tali documenti nel cestino della spazzatura o nel contenitore del riciclaggio senza prima distruggerli. Inoltre, il **46%** degli intervistati ha affermato di aver visto colleghi lasciare documenti di lavoro riservati incustoditi. Queste risposte dovrebbero creare grande preoccupazione nelle aziende. Anche se in generale le aziende europee hanno introdotto rigorose politiche sulle procedure di distruzione di documenti sensibili, spesso i dipendenti non seguono queste regole fuori dall'ufficio. Che si tratti di un ufficio aziendale o domestico, i documenti cartacei sensibili devono essere chiusi a chiave quando non sono utilizzati ed essere distrutti in modo sicuro quando non sono più necessari per il fine originale.

Il nostro studio ha inoltre rivelato che, pur essendo passati 4 anni dall'entrata in vigore, solo il **60%** degli intervistati dichiara di conoscere il GDPR e solo **1 azienda su 4** ha adattato le proprie politiche per includere i modelli di lavoro da casa o il telelavoro in generale. Le autorità di regolamentazione quali l'ICO (Information Commissioner's Office) sono state più flessibili durante la pandemia, riconoscendo le forti pressioni esercitate sulle aziende. Ma ora che gran parte delle restrizioni sono state revocate in Europa, l'ICO non avrà ragione di fare concessioni. Per questo, le aziende che prevedono di adottare il modello di lavoro ibrido in modo permanente devono agire subito. Le politiche aziendali devono essere riviste e aggiornate per riflettere i nuovi modelli di lavoro e contemplare i potenziali rischi di violazione dei dati.

Una volta aggiornate le politiche, le aziende devono dotarsi di un robusto piano di implementazione e comunicazione. Il nostro studio ha evidenziato gravi discrepanze all'interno delle organizzazioni. Se la maggioranza (83%) degli intervistati in ruoli senior sembra conoscere il GDPR e rispettare attivamente le politiche e le regole aziendali sulla protezione dei dati, solo il **57%** degli intervistati in ruoli junior sembra conoscere il GDPR e rischia quindi di non seguire le raccomandazioni, indipendentemente dal luogo di lavoro.

La comunicazione e il controllo di documenti e informazioni sensibili sembra essere più facile nel contesto di ufficio insieme ai colleghi. Ma è certo che il lavoro ibrido è una nuova realtà che le aziende dovrebbero adottare per sostenere i loro dipendenti. Allo stesso tempo, è fondamentale che i processi e i regolamenti interni vengano adattati per riflettere questi cambiamenti. Perdere documenti cartacei sensibili può avere conseguenze molto gravi. Per questo, è fondamentale coinvolgere tutti i dipendenti dell'azienda in programmi di formazione sul regolamento GDPR. Infatti, anche una piccola disattenzione nel trattamento dei dati può risultare in una violazione della legge. Nella prossima sezione, presentiamo alcuni consigli su come implementare le modifiche in tutta l'azienda.

Cosa possono fare le aziende per aiutare i loro dipendenti a rispettare le politiche sulla privacy e la protezione dei dati?

Aggiornare le politiche

Considerare la politica del "Bring your own device" (BYOD), in base alla quale i dipendenti possono utilizzare i loro dispositivi personali quando lavorano da casa.

Sottolineare che le reti Wi-Fi pubbliche e private sono una minaccia e spiegare al personale come utilizzarle in modo sicuro.

Rivedere e adattare le politiche aziendali sulle procedure di stampa, conservazione e smaltimento dei documenti cartacei e integrare una sezione sulla conservazione e lo smaltimento dei documenti cartacei quando si lavora da casa.

Rivedere le politiche sulla sicurezza delle password. Il National Cyber Security Centre (NCSC) raccomanda l'utilizzo di frasi di accesso a tre parole (o passphrase) piuttosto che di password. È inoltre opportuno utilizzare l'autenticazione a più fattori.

La politica aziendale deve specificare che, prima di procedere allo smaltimento, alla vendita o alla donazione di computer o dischi rigidi vecchi, è necessario che tutti i dati vengano cancellati in modo permanente dal disco rigido.

Organizzare formazione

Non dare per scontato che tutti conoscano il GDPR. Formare tutti i dipendenti ai requisiti del GDPR, al trattamento dei dati personali e ai 6 principi della protezione dei dati. La formazione deve essere impartita anche ai neoassunti e prevedere corsi di aggiornamento periodici sulla sicurezza dei dati.

Fornire una lista di controllo ai dipendenti che operano nelle aree più esposte al rischio di violazione dei dati. Incaricarli di condurre un **controllo sulla salute della sicurezza dei dati.**

Assicurarsi che i programmi di formazione affrontino la gestione dei documenti cartacei sensibili. Specificare quali documenti e record possono essere conservati per determinati periodi di tempo e quali devono invece essere distrutti quando non sono più necessari.

Includere un modulo di formazione sulla sicurezza dei dati quando si lavora da casa, dove si spiegano in dettaglio le nuove aggiunte alle politiche esistenti.

Considerare un portale di formazione online per monitorare lo stato di formazione di ogni dipendente e definire le relative scadenze.

Dotarsi di attrezzature

Per evitare problemi con il modello di lavoro BYOD, consigliamo alle aziende di investire in computer laptop piuttosto che da tavolo, per facilitare il trasporto dei dispositivi tra casa e ufficio.

Investire in sistemi anti-virus e firewall all'avanguardia.

Assicurarsi che il personale abbia accesso a un distruggidocumenti nell'ufficio aziendale. Anche i dipendenti in telelavoro devono avere un piccolo distruggidocumenti personale.

Per i dati personali o strettamente riservati (quali indirizzi, fatture, bilanci, ecc.) optare per un distruggidocumenti a microframmento (P-5) poiché la distruzione in frammenti rende impossibile la lettura o il recupero delle informazioni ed è quindi più sicura.

Creare un ambiente di lavoro sicuro e produttivo per i dipendenti scegliendo una soluzione distruggidocumenti che includa funzioni di prevenzione degli inceppamenti e funzionalità di sicurezza.

Fare comunicazione

La comunicazione è cruciale a tutti i livelli dell'azienda. Occorre colmare le lacune di conoscenza nei ruoli junior.

Includere la sicurezza dei dati nella futura riunione generale di ufficio, ma anche nelle riunioni mensili dei team e nei colloqui individuali con i dipendenti.

Affiggere poster promemoria in azienda e pubblicare ugualmente tutti gli aggiornamenti delle politiche nella newsletter e sulla rete Intranet aziendali.

Divulgare a tutti i livelli dell'azienda le migliori pratiche così come le informazioni su eventuali minacce di phishing o attacchi informatici affinché tutti possano farvi attenzione.

Includere la sicurezza dei dati nelle revisioni trimestrali dell'attività.

Cosa possono fare i dipendenti per prevenire le violazioni dei dati?

Riconoscere i dati sensibili e come proteggerli

Qualsiasi documento contenente dati personali o record aziendali deve essere distrutto in modo sicuro, nel rispetto degli obblighi legali sulla conservazione dei dati.

Ricorda che il periodo di conservazione obbligatorio di contratti, accordi commerciali e documenti simili varia in ogni Paese. Raggiunto il termine di conservazione, occorre distruggere i documenti sia per liberare spazio di archiviazione che per proteggere la riservatezza.

In genere, le ricevute, i certificati di deposito e gli estratti bancari possono essere distrutti dopo essere stati confrontati con la contabilità.

I documenti delle Risorse Umane devono essere verificati regolarmente e distrutti alla data di scadenza legale. Ai sensi del GDPR, i dipartimenti RU devono essere in grado di giustificare la conservazione dei dati di dipendenti ed ex-dipendenti e ogni eventuale conservazione dei dati oltre il periodo di legge.

Conservare o eliminare i documenti cartacei in modo sicuro

Pensa prima di stampare. Chiediti: è davvero necessario stampare questo documento? Potrebbe finire accidentalmente in mani sbagliate?

Consigliamo di distruggere i documenti di volta in volta. Se questo non è possibile, distruggi tutti i documenti cartacei sensibili prima di gettarli nella spazzatura o riciclarli, possibilmente evitando il trasporto tra casa e ufficio o viceversa.

Non lasciare in giro incustoditi documenti cartacei sensibili a casa o in ufficio. A fine giornata libera la scrivania e chiudi a chiave i documenti cartacei e tutti i supporti informatici rimovibili prima di lasciare la postazione di lavoro.

Rivedere regolarmente i dati conservati e, se possibile, renderli anonimi quando non sono più necessari.

Mantenersi aggiornati sulle politiche e completare i corsi di formazione

Mantieniti aggiornato sui moduli di formazione disponibili e assicurati di avervi accesso. Imposta promemoria trimestrali nel tuo calendario per non perdere le sessioni di aggiornamento.

Incoraggia i colleghi e i membri del team a partecipare ai moduli di formazione e ricorda le regole e le linee guida se noti comportamenti non conformi (ad es. lasciare documenti sensibili sulla scrivania, usare dispositivi personali, ecc.)

Studia i 6 principi della protezione dei dati.

Per qualsiasi dubbio o domanda, rivolgiti al tuo manager o al responsabile della protezione dei dati.

I risultati più importanti del nostro studio

8 intervistati su 10

hanno adottato modalità di lavoro domestico.

Il 70% degli intervistati

ha stampato e portato a casa documenti di lavoro, oppure li ha stampati a casa, o entrambi.

Il 47%

di questi **non distruggono documenti di lavoro** dopo l'uso >>> **Questo ne mette a rischio la sicurezza durante il transito!**

Il 46%

hanno visto altre persone **lasciare incustoditi documenti di lavoro confidenziali**

C'è una grande **mancanza di consapevolezza del GDPR tra i ruoli junior e non manageriali**

Solo il 57%

dichiara di conoscere bene il regolamento.

Dopo 4 anni

Solo il 60%

di tutti gli intervistati afferma di essere a conoscenza del GDPR.

Quattro su dieci (41%)

afferma di non aver ancora ricevuto un aggiornamento formale della

policy GDPR per il lavoro

Guida alle migliori pratiche di distruzione dei documenti:

La distruzione sicura dei documenti è essenziale per evitare che informazioni confidenziali finiscano in mani sbagliate e per ridurre l'esposizione al rischio di perdita di dati. Viviamo un'epoca in cui sempre più persone lavorano in modo ibrido tra l'abitazione e l'ufficio, eppure la conformità al GDPR è più importante che mai, vista la mole di rischi per la sicurezza che questo stile di lavoro comporta.

L'uso di un distruggidocumenti per liberarsi in sicurezza di documenti confidenziali dovrebbe far parte della routine quotidiana di lavoro, ovunque ci troviamo.

- Non diamo per scontato che tutti sappiano cos'è il GDPR. Educhiamo i dipendenti sulle regole del GDPR, sulla gestione dei dati personali e sui sei principi della protezione dei dati. Questo dovrebbe far parte del training iniziale di ogni nuovo assunto e dovrebbe essere ripetuto periodicamente e ad ogni aggiornamento della legislazione.
- Chiudiamo al sicuro i documenti confidenziali quando non vengono usati, senza mai lasciarli in giro senza sorveglianza sia a casa che al lavoro.
- Distruggiamo tutti i documenti cartacei sensibili prima di riciclarli o gettarli via, se possibile senza correre il rischio di trasportarli da casa all'ufficio o viceversa.
- Rendiamo facilmente disponibile per tutti gli impiegati un distruggidocumenti sicuro a casa e in ufficio.

Trova il distruggidocumenti giusto per il tuo ambiente di lavoro.
Visita www.fellowes.com o fai click qui

Sondaggio Metti al sicuro i dati 2022
Metodologia

Nell'aprile 2022, B2B International ha condotto un sondaggio tra 605 utenti di soluzioni distruggidocumenti nel Regno Unito, in Francia e in Germania. La ricerca si è concentrata su utenti di diversi livelli di anzianità di piccole e medie imprese del settore finanziario (206), pubblico (206) medico/assistenza sanitaria (193).
Per poter confrontare le pratiche di lavoro concernenti la sicurezza dei dati in un ambiente di lavoro ibrido, era importante intervistare in equa proporzione: dipendenti che lavorano sia in ufficio che in remoto; dipendenti che lavorano principalmente in ufficio; dipendenti che lavorano solo in ufficio; dipendenti che lavorano principalmente a casa; dipendenti che lavorano solo a casa.

Per ulteriori dettagli sulla metodologia di campionamento, contattare **jdettler-bates@fellowes.com**

Fellowes

www.fellowes.com

© Fellowes Ltd 2022