IDC Executive Brief

Sponsorizzato da: **Brother**

Autore:

Jacqui Hendriks

Marzo 2018

Garantire la riservatezza dei dati: una crescente sfida per la gestione della stampa e dei documenti

Numerose sono le aziende che non riusciranno ad adempiere alla nuova normativa inerente la riservatezza e la sicurezza dei dati perché hanno trascurato le potenziali vulnerabilità associate alla stampa. Un ambiente di stampa non protetto è sinonimo di un ambiente IT non sicuro.

Questo IDC Executive Brief introduce la nuova legislazione sulla riservatezza dei dati, le iniziative necessarie per soddisfare i requisiti di conformità e gli interventi necessari per rendere i processi di gestione della stampa e dei documenti conformi.

Protezione dei dati dei clienti

Spinto dall'innovazione tecnologica, il modo in cui le aziende di tutte le dimensioni ricevono, elaborano, utilizzano e forniscono informazioni è cambiato radicalmente. Le imprese ricevono volumi esponenziali di informazioni in formati elettronici e cartacei. Secondo una ricerca IDC, entro il 2025 la quantità di dati creati, acquisiti e replicati, crescerà fino a 163 zettabyte (ZB) o 163 trilioni di gigabyte (GB), dieci volte i 16,12 ZB di dati generati nel 2016[1]. Eppure, la legislazione per la protezione dei dati non riesce a tenere il passo con questi andamenti variabili sul lavoro.

La capacità di estrarre informazioni da questi dati può aiutare sia ad attirare sia a mantenere i clienti, ottimizzando l'esperienza del cliente[2]. Tuttavia, alla luce dell'inefficace gestione delle informazioni, spesso le aziende hanno difficoltà a trovare queste informazioni[3]. In particolare, se le informazioni non sono gestite in modo adeguato, si corre il rischio che dati sensibili finiscano nelle mani sbagliate. Ciò può sfociare in violazioni significative, mettendo a repentaglio i dati personali della società e dei clienti.

Punti di vulnerabilità comprendono:

- Uso improprio di dispositivi e documenti di stampa
- Conservazione di dati su memorie interne di dispositivi e memorie in dispositivi
- Violazioni potenziali da porte di rete dei dispositivi
- Mancata presa in consegna di documenti

La legislazione per la protezione dei dati è stata recentemente aggiornata al fine di riflettere i comportamenti e i valori di oggi, tra cui l'impiego di social media e altri servizi online. La Direttiva UE per la protezione dei dati del 1995 (95/46/CE) risale a prima dell'esistenza di numerosi attuali modelli d'impresa online e anticipa di gran lunga l'avvento di servizi cloud e social media. La

nuova normativa imporrà sanzioni pesanti per le aziende che non s'impegnano in uno sforzo concertato per attenuare i rischi.

Attualmente, la massima attenzione è rivolta al GDPR, Regolamento generale sulla protezione dei dati 2016/679 dell'Unione Europea (UE); tuttavia, esiste un lungo elenco di normative europee in fase di elaborazione in materia di riservatezza UE, ad esempio[4]:

Attualmente, la massima attenzione è rivolta al GDPR, Regolamento generale sulla protezione dei dati 2016/679 dell'Unione Europea (UE); tuttavia, esiste un lungo elenco di normative europee in fase di elaborazione in materia di riservatezza UE.

- **Direttiva 2016/680** — Questa direttiva è vista come la gemella del GDPR e si concentra sull'elaborazione dei dati personali al fine di prevenire, indagare, rilevare o perseguire reati penali oppure mettere in atto sanzioni penali. In precedenza, questa era una direttiva che, a partire dal 6 maggio 2018, sarà trasposta in legge nazionale in tutti i 28 stati membri UE.
- **Direttiva per la sicurezza delle reti e dei sistemi informativi (NIS)** — È stata promulgata dalla UE per introdurre un approccio coerente contro gli attacchi cibernetici a servizi essenziali come energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, approvvigionamento idrico, infrastrutture digitali e servizi digitali.
- **Regolamento ePrivacy** — Insieme al GDPR, la Direttiva ePrivacy (ePD) costituisce il quadro giuridico per la riservatezza digitale dei cittadini UE e interessa le comunicazioni tramite reti pubbliche. L'ePD risale al 2002 ma è attualmente oggetto di revisione per essere aggiornata al fine di tenere il passo con il progresso tecnologico.
- **Direttiva sul codice di prenotazione (PNR)** — Questa direttiva è associata alla prassi comune di raccogliere dettagli sul passeggero prima dell'imbarco su un volo. Gli stati membri UE devono trasporre la direttiva in leggi nazionali entro il 24 maggio 2018. I dati personali raccolti in conformità con la Direttiva PNR devono essere conservati per sei mesi, dopodiché saranno anonimizzati e quindi conservati per un ulteriore periodo di quattro anni e mezzo.

Mentre alcune delle nuove normative sono relativamente generiche e altre altamente specifiche per il settore, tutte influiranno sul modo in cui le aziende gestiscono i documenti stampati e i workflow dei documenti in futuro.

Riservatezza e sicurezza dei dati

Il GDPR 2016/679 definisce la violazione dei dati come "distruzione, perdita, alterazione, diffusione non autorizzata di, o accesso, accidentali o illegittimi, a dati personali trasmessi, conservati o elaborati in altro modo." Il GDPR costituisce un cambiamento fondamentale nelle leggi UE che regolamentano i dati personali e la riservatezza dei cittadini UE. Anche le aziende internazionali con sede al di fuori della UE, tra cui quelle nel Regno Unito in seguito alla Brexit, ne saranno interessate per la gestione dei dati dei cittadini UE.

Il GDPR ha due obiettivi primari: aggiornare la normativa sulla protezione dei dati e armonizzare le norme per la protezione dei dati UE in un unico ordinamento giuridico, e si basa sui seguenti presupposti:

- Le aziende non possiedono i dati delle persone. La legislazione più recente sostiene il diritto dei cittadini di sapere se i propri dati sono manipolati correttamente e di essere informati se i dati sono persi, rubati o trattati impropriamente, per cui tale violazione comporta un elevato rischio (notifica obbligatoria di violazione).
- Le aziende devono rispettare il "diritto di essere dimenticati" dei cittadini. Per raggiungere questo obiettivo, le aziende devono sapere dove sono i dati riguardanti un argomento specifico, in quale applicazione o dispositivo. Inoltre, è previsto che tutte le informazioni siano indicate in maniera standardizzata in tutte le memorie dati di tutti i sistemi/piattaforme/apparecchiature.

Molti dei requisiti del GDPR, così come quelli di altre normative imminenti, sono potenzialmente più severi rispetto alla legge che sostituisce. Le ammende per inadempienza sono severe, "efficaci, proporzionali e dissuasive" come cita il teso del GDPR, sebbene l'obiettivo alla base sia rendere chiaro e semplice il percorso verso la conformità per tutte le parti coinvolte. La chiara dimostrazione dell'intento e degli sforzi profusi verso l'adempienza influenzeranno positivamente qualora l'autorità locale debba avviare un'indagine su una violazione di sicurezza.

L'inadempienza può avere un impatto negativo grave sulla reputazione di un'azienda. Di fatto, il rischio reputazionale di non-conformità è una delle preoccupazioni chiave associate al GDPR[5].

Nel tentativo di affrontare i requisiti di conformità, le aziende hanno quattro priorità d'investimento principali[6]:

- Identificare le applicazioni che usano dati relativi al regolamento specifico di conformità
- Mappare e scoprire i dati, valutando e classificando i dati
- Istituire processi di documentazione
- Rivedere e ottimizzare la gestione di identità e accesso

Il GDPR punta i riflettori sulla sicurezza della stampa e dei documenti e sulla riservatezza dei dati. Richiede che siano soddisfatte determinate condizioni per tutto il workflow in formato elettronico e stampato. Deve essere in atto un percorso di audit, l'accesso e l'elaborazione devono essere autorizzati, mentre le informazioni devono essere protette, compresi eventuali dati conservati su dispositivi di stampa. Processi correttamente documentati, registri e percorsi di audit adeguati aiutano a mitigare le violazioni della sicurezza; tuttavia, nel caso in cui si verifichi una violazione, le società devono dimostrare concretamente di aver messo in atto misure adeguate erano state messe in atto per evitarla.

Gli stessi fornitori di soluzioni per la gestione della stampa e dei documenti devono conformarsi alla normativa sulla riservatezza dei dati e sono perciò nella posizione ideale per sostenere i loro clienti. Sebbene, alla fine, la responsabilità di adempiere alla normativa ricada sulla singola azienda.

Il GDPR punta i riflettori sulla sicurezza della stampa e dei documenti e sulla riservatezza dei dati. Richiede che siano soddisfatte determinate condizioni per tutto il workflow in formato elettronico e stampato. Processi correttamente documentati e verbali, registri e percorsi di audit adeguati aiutano a mitigare le violazioni della sicurezza; tuttavia, nel caso in cui si verifichi una violazione, dimostra concretamente che delle misure adeguate erano state messe in atto per evitarla.

Ad oggi, le aziende sembrano non avere i requisiti necessari per adempiere alla normativa, o spesso sono inconsapevoli della normativa, del suo impatto e delle relative scadenze[7]:

- Stranamente, nonostante le sanzioni entrino in vigore nel 2018, all'inizio del 2017 il 40% degli acquirenti di prodotti stampati non sapeva che cosa fosse il GDPR e un ulteriore 19% sapeva che cosa fosse ma non era a conoscenza delle scadenze. Le aziende consapevoli di avere un approccio rilassato, erano generalmente convinte che alla fine sarebbero riuscite a soddisfare i criteri di conformità.
- Ancora più sorprendente è che gli acquirenti di prodotti stampati consapevoli di cosa il GDPR fosse, il 51% non ne comprendeva le significative implicazioni per la stampa.

Assicurare che i propri processi di gestione della stampa e dei documenti siano conformi con la normativa

Tra quegli acquirenti di prodotti stampati, consapevoli dell'esistenza del GDPR, il 51% non comprendeva le implicazioni significative per la stampa.

La sicurezza organizzativa è una priorità assoluta per tutte le aziende, dai liberi professionisti alle grandi multinazionali. I tre principali punti dolenti da affrontare relativi alla sicurezza sono[7]:

1. Pianificare la continuità di servizio e il ripristino in caso di disastro
2. Restare al passo aggiornandosi contro attacchi sempre più sofisticati
3. Soddisfare le normative obbligatorie in materia di conformità

Nonostante i crescenti casi di perdita di dati aziendali e personali, quando si tratta di sicurezza per la stampa, poca attenzione è rivolta a ciò che deve essere fatto per conformarsi alla normativa[7]:

- L'investimento nella sicurezza per la stampa è minimo; più della metà delle aziende spende meno del 3% del proprio budget IT sulla sicurezza della stampa
- In termini di piani futuri, due terzi non intendono incrementare questa spesa nei successivi 12 mesi e soltanto un terzo delle aziende prende in considerazione la sicurezza per la stampa nelle richieste di proposte riguardanti l'IT

Soluzioni che migliorano l'efficienza della gestione della stampa e dei documenti presso le aziende e allo stesso tempo aiutano ad affrontare la sfida della conformità in materia di riservatezza dei dati già esistono:

- Le aziende sono molto interessate a funzionalità di stampa sicura, come ad esempio la tecnica "pull printing" e soluzioni di autenticazione e autorizzazione per l'utente finale, integrate nelle stampanti polifunzionali (MFP)[3]. In questo modo, le aziende possono limitare l'accesso dei dipendenti a informazioni specifiche, sulla base del ruolo e delle responsabilità del dipendente. Ciò rappresenta una misura di conformità attendibile volta a ridurre i rischi.
- La crescente domanda di digitalizzazione delle informazioni per l'integrazione in flussi di lavoro elettronici si è tradotta in un maggiore

utilizzo degli scanner. Un'indagine europea IDC sul cartaceo del 2017 ha rivelato che la scansione per l'invio via e-mail, la scansione in cartelle di rete e la scansione su sistemi esistenti (ad es. ERP, CRM) sono oggi tutti elementi di grande interesse per le aziende. Inoltre, aumenta la domanda di MFP intelligenti che offrono la funzione di scansione e accesso diretto ai dati conservati[3].

I fornitori di stampa e imaging non stanno trascurando la gestione efficace e sicura per la stampa e i documenti e già offrono una vasta scelta di soluzioni che aiutano le aziende a ottimizzare il modo in cui gestiscono il processo di conformità senza dover dirottare risorse da attività che generano profitti:

I fornitori di stampa e imaging non stanno trascurando la gestione efficace e sicura per la stampa e i documenti, e già offrono una vasta scelta di soluzioni che aiutano le aziende a ottimizzare il modo in cui gestiscono il processo di conformità.

- **Soluzioni per la gestione e il monitoraggio della stampa —** Queste si sono rivelate strumenti efficaci per tenere traccia e segnalare l'impiego dei dispositivi da usare nella valutazione dell'ambiente di stampa in negoziazioni di contratti/acquisti. Per questo motivo, più della metà delle aziende (il 53%) ha messo in atto queste soluzioni[8]. Queste soluzioni offrono anche un valore aggiunto, in quanto permettono di creare un percorso di audit, volto a individuare che cosa viene stampato/elaborato, dove e da chi. Questa capacità di mantenere un percorso di audit è un elemento essenziale per la mitigazione delle violazioni di sicurezza.
- **Accesso e autenticazione sicuri —** Il 46% delle aziende richiede ai propri dipendenti di autenticarsi su un dispositivo di stampa[8] prima dell'uso, accedendo tramite codice PIN oppure scheda di comunicazione near-field (NFC). Questa funzionalità è spesso obbligatoria soltanto per i dipartimenti che elaborano principalmente materiale sensibile, come le risorse umane, i reparti finanziari o di alta finanza.
- **Accesso sicuro alla stampa con directory attiva —** Questo espediente offre persino maggiore sicurezza, bloccando funzioni fisiche del dispositivo e, quindi, consentendo maggiore flessibilità, come l'impostazione di un limite temporale per la raccolta di job di stampa. I documenti non elaborati sul dispositivo possono costituire un potenziale rischio se intercettati in modo non conforme.
- **Sicurezza del dispositivo di stampa—** Le aziende temono sempre più che le informazioni aziendali riservate, conservate su dispositivi periferici di rete, possano inavvertitamente diventare di dominio pubblico[8]. Alcuni produttori di stampanti garantiscono che gli utenti non possono conservare informazioni nel dispositivo, bensì possono attingere alla possibilità di recuperare i documenti da un server centrale sicuro oppure da un dispositivo di archiviazione cloud protetto. Le aziende, pertanto, hanno la certezza che i documenti non possono essere recuperati da un dispositivo, qualora tale dispositivo sia compromesso fisicamente in qualche modo.
- **Scansione sicura —** Le misure di sicurezza non si limitano esclusivamente ai prodotti stampati. Anche i documenti scansionati possono essere protetti come un file PDF con un codice PIN di accesso

oppure impiegando un protocollo di trasferimento sicuro dei file (SFTP) per creare un flusso di dati protetto. Il 20% delle aziende ha individuato dei timori in materia di sicurezza relativi all'accesso autorizzato dei dipendenti a documenti scansionati [9].

- **Comunicazioni sicure di dati —** I dispositivi impiegati per la stampa, la scansione o altre attività di gestione dei documenti devono essere protetti configurando funzioni di sicurezza riconosciute dal settore come Internet Protocol Security (IPsec) e Transport Layer Security (TLS). Queste funzioni assicurano che le comunicazioni da e verso il dispositivo siano autenticate, affidabili e riservate.
- **Minacce di rete —** Le aziende devono garantire che il dispositivo di stampa non sia un punto vulnerabile, applicando lo stesso livello di sicurezza previsto per altre apparecchiature IT, come laptop e tablet.

Piuttosto che vedere la strada verso la conformità come un pesante fardello, le aziende dovrebbero interpretarla come un'opportunità per implementare processi più efficienti.

Workflow più snelli non solo le aiutano a soddisfare la normativa ma, in linea di massima, permettono di elaborare le informazioni in modo più efficiente su base quotidiana. Inoltre, l'implementazione di processi più efficienti volti ad adempiere alla conformità può risultare anche in risparmi di costo.

L'implementazione di processi più efficienti volti ad adempiere alla conformità può risultare anche in risparmi di costo.

Linee guida per garantire l'adempienza alla normativa riguardante la gestione della stampa e dei documenti

La seguente lista fornisce 10 azioni che le aziende dovrebbero considerare come parte integrante delle iniziative per rendere il business sicuro ed essere conformi alle normative sulla riservatezza dei dati:

- ☑ Sottoporre ad audit le attuali politiche aziendali riguardanti la sicurezza e la riservatezza e allinearle ai requisiti essenziali in materia di sicurezza e riservatezza dei dati, garantendo che l'infrastruttura della stampa sia parte integrante dell'audit.
- ☑ Individuare il personale con abilità pertinenti e potenziali lacune.
- ☑ Chiedere al proprio fornitore di dispositivi di stampa a quali risorse il dipartimento IT può attingere per garantire la conformità.
- ☑ Proteggere la rete a cui sono collegate le stampanti.
- ☑ Salvaguardare tutti i tipi di informazioni sensibili che sono inviate o elaborate dalla stampante/scanner.
- ☑ Assicurare che tutte le stampanti non siano suscettibili a malware o altri attacchi cibernetici.
- ☑ Garantire che le informazioni potenzialmente riservate non siano conservate su dispositivi periferici come le stampanti.
- ☑ Adottare uno strumento di gestione della flotta per il monitoraggio e la gestione continua centralizzata dei dispositivi di stampa e scansione.
- ☑ Adottare l'autenticazione utente (compresa la tecnica "pull printing") e l'autorizzazione sul dispositivo per garantire il recupero sicuro di documenti riservati.
- ☑ Sviluppare un piano continuo per monitorare, scalare, rimediare e mettere in atto politiche per la sicurezza e la riservatezza, nel presente e nel futuro.

Fonti:

1. *Data Age 2025: The Evolution of Data to Life-Critical, Don't Focus on Big Data; Focus on the Data That's Big*, IDC White Paper, aprile 2017
2. *What are the Top Priorities of LOBs and Industries in Western Europe?* IDC #EMEA43168117, ottobre 2017
3. *Content Management Opportunity: Integrated Solutions vs Outsourcing*, IDC #EMEA43165417, ottobre 2017
4. *An Overview of Incoming EU Privacy and Data Security Legislation*, IDC #EMEA42911917, agosto 2017
5. Sondaggio IDC sul GDPR EMEA, 2017
6. *IDC PlanScape: EU General Data Protection Regulation Compliance*, IDC #US42574817, giugno 2017
7. *Low Investment in Print Security and Increasing Compliance Challenges Leave European Companies at Risk*, IDC #EMEA42819617, giugno 2017
8. *Still Significant Opportunity to Address Print Infrastructure /Management Challenges*, IDC #EMEA43059617, settembre 2017
9. *Workplace Dynamics Drive Print and Document Management,* IDC #EMEA41529116, giugno 2016

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, Regno Unito
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Informazioni su IDC

IDC (International Data Corporation) è il primo gruppo mondiale specializzato in ricerche di mercato, servizi di consulenza e organizzazione di eventi nei settori dell'Information Technology, delle telecomunicazioni e della tecnologia consumer. IDC aiuta i professionisti IT, i dirigenti aziendali e la community degli investitori a prendere decisioni basate su elementi concreti in merito agli acquisti nel settore della tecnologia e alle strategie di business. Oltre 1.100 analisti di IDC in 110 paesi di tutto il mondo mettono a disposizione la loro esperienza e capacità a livello globale, regionale e locale circa le opportunità e le tendenze della tecnologia e dell'industria. Da 50 anni, IDC fornisce analisi strategiche per aiutare i propri clienti a raggiungere i loro principali obiettivi di business. IDC fa parte del gruppo IDG, società leader a livello mondiale nel settore dell'editoria, della ricerca e degli eventi in ambito tecnologico.