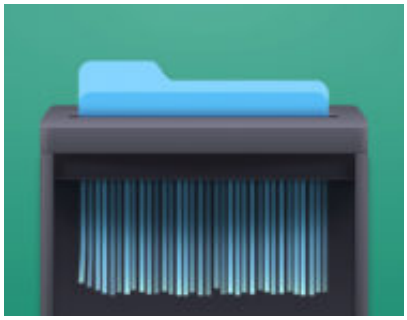
L’importanza dell’eliminazione sicura dei dati secondo il GDPR

Author : Stefano Gorla

Date : 15 Marzo 2019



La sicurezza dei dati è diventata ormai un aspetto imprescindibile dell’attività di un’organizzazione. La sicurezza dei dati deve intendersi come un **processo generale** che considera la gestione dei dati in tutti i suoi flussi e i suoi percorsi. La Data protection e la Security by design devono essere parte integrante delle organizzazioni. I dati devono essere gestiti in ottica sistemica: dalla culla alla tomba.

Molte organizzazioni si concentrano nella gestione interna dei dati ma perdono di vista sia la gestione esterna sia il fine vita degli stessi, con eventuali gravi conseguenze in termini di potenziali Data Breach.

I modelli di gestione della sicurezza dei dati riportano punti di controllo proprio su tali aspetti, infatti:

- **CSF CORE NIST**

PR.IP-6: I dati sono distrutti in conformità con le policy;

- **NIST SP 800-53 Rev. 4**

MP-6 MEDIA SANITIZATION;

- **ISO 27001:2014**

A.8.2.3 Trattamento degli asset

A.8.3.2 Dismissione dei supporti

A.11.2.7 Dismissione sicura o riutilizzo delle apparecchiature;

- **COBIT5**

BAI09.03 Manage the asset life cycle.

La gestione a fine vita dei dati non deve considerarsi solo per i dati di natura informatica ma anche per tutti i dati cartacei che sono custoditi, gestiti, archiviati presso le organizzazioni.

Non ultimo, la gestione dei dati ed il loro fine vita vengono ribaditi dal Regolamento 2016/679.

L'entrata in vigore del Regolamento Generale sulla Protezione dei Dati (GDPR) definisce nel dettaglio i compiti che il Titolare del Trattamento dei dati (Data Controller) dovrà ottemperare al fine di garantire al meglio la conformità dell'intero processo di acquisizione, trattamento, conservazione ed eliminazione dei dati personali dei clienti.

L'eliminazione sicura dei dati è un'attività già da molti anni consolidata nel resto del mondo e che, ad oggi, si rende necessaria al fine di evitare - e quindi prevenire - una qualsiasi "violazione del dato".

Nel GDPR, infatti, **per "dato" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; mentre per "violazione del dato" si intende la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

L'eliminazione dei dati può avvenire sia tramite la distruzione fisica dei supporti sia tramite la cancellazione dei dati contenuti nei supporti; l'importante è che l'attività sia svolta da un provider certificato e che vi sia un report che attesti il lavoro svolto.

L'obbligo del titolare del trattamento dei dati a cancellare i dati dell'interessato è chiaramente espresso nell'articolo 17 del GDPR, "Diritto alla cancellazione (Diritto all'oblio)" che recita così:

1. *L'interessato ha diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:*
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
2. *Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di*

cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Terminato il tempo utile di ritenzione, il titolare del trattamento è obbligato a cancellare i dati senza alcun tipo di procrastinazione temporale. Il tempo di conservazione dei dati dovrebbe essere limitato al minimo necessario e il titolare del trattamento dovrebbe stabilire un termine per la cancellazione di ogni dato. Inoltre, la cancellazione deve essere effettuata utilizzando tecnologie che garantiscano la conformità al regolamento e la sicurezza dell'intero processo, come la distruzione certificata dei documenti cartacei o la cancellazione (wiping) certificata dei dati digitali.

La distruzione e/o cancellazione dei dati dai supporti (attività contenute nel trattamento dei dati) deve essere svolta sotto il diretto controllo del Titolare del Trattamento dei Dati come descritto nell'articolo 24, "Responsabilità del titolare del trattamento":

1. *Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*

È compito del titolare del trattamento scegliere il giusto provider per l'eliminazione dei dati. Infatti, nel caso in cui vi sia una violazione a seguito di un trattamento svolto in maniera difforme al regolamento, la **responsabilità** ricadrebbe, oltre che sul provider, anche sul titolare del trattamento per aver messo a rischio i dati dei propri clienti scegliendo un servizio di distruzione/cancellazione non certificato e non conforme al regolamento.

È, quindi, estremamente importante selezionare un provider che assicuri una distruzione/cancellazione dei dati completamente certificata, che si avvalga di personale professionale, qualificato e specificatamente formato, che utilizzi strumenti e mezzi conformi, che rispetti elevati standard di qualità e che garantisca la sicurezza delle informazioni in ogni fase del servizio che svolge.

A volte scegliere un provider certificato non è l'opzione più conveniente in quanto un servizio di eccellenza è sicuramente più gravoso ma assicura più sicurezza, maggiori garanzie e una completa conformità alle normative.

Inoltre, ogni attività di distruzione o di cancellazione dei dati deve essere certificata da un documento, come esposto nel Decreto Legislativo n° 51 del 18 maggio 2018 sulla protezione dei dati personali in ambito penale, entrato in vigore subito dopo il GDPR.

L'articolo 21, "Registrazione", recita così:

1. *Le operazioni di raccolta, modifica, consultazione, comunicazione, trasferimento, interconnessione e cancellazione di dati, eseguite in sistemi di trattamento automatizzati, sono registrate in appositi file di log, da conservare per la durata stabilita*

con il decreto di cui all'articolo 5, comma 2.

2. *Le registrazioni delle operazioni di cui al comma 1 debbono consentire di conoscere i motivi, la data e l'ora di tali operazioni e, se possibile, di identificare la persona che ha eseguito le operazioni e i destinatari.*

Soprattutto in ambito digitale, ogni cancellazione dei dati deve essere registrata in appositi file di log che contengano data e ora, nome di chi effettua la cancellazione e tutte le informazioni dei dispositivi cancellati.

Sul **mercato italiano** sono presenti aziende che effettuano la distruzione dei supporti cartacei e digitali direttamente presso il cliente e che vendono software che eliminano i dati digitali in maniera certificata, rilasciando un report al termine del lavoro.

Le aziende che svolgono i servizi di **distruzione certificata** si recano presso il cliente con l'unità mobile di triturazione e, come prima operazione, inseriscono tutta la documentazione in sacchi anti-taglio che vengono chiusi con sigilli di sicurezza codificati. Successivamente, i sacchi vengono trasportati sull'unità mobile e, dopo aver scansionato ogni sigillo, tutta la documentazione viene inserita all'interno del trituratore situato a bordo del mezzo per la sua distruzione. La distruzione avviene in poco tempo assicurando la completa inintelligibilità dei dati e delle informazioni contenute, che non potranno essere recuperate in nessun modo. I trituratori a bordo delle unità mobili possono arrivare ad effettuare una distruzione pari al livello 7 della norma DIN 66399. Tutte le operazioni sono svolte sotto la supervisione diretta del cliente, che può assistere anche alla distruzione. Al termine delle attività di distruzione, il triturato viene avviato al recupero in modo da garantire la salvaguardia ambientale.

Per quanto riguarda l'attività di **eliminazione dei dati digitali**, nel caso in cui debba essere svolta per grandi aziende, vengono utilizzate soluzioni che permettono di collegare più di un dispositivo o hard disk all'apparecchio e operare una cancellazione simultanea rilasciando, al termine, un certificato di cancellazione. Per le piccole aziende o per i professionisti sono in commercio, invece, delle chiavette USB che, inserite nel PC, permettono di cancellare in modo semplice e veloce qualsiasi dato presente rilasciando, al termine, un report che permette di dimostrare l'avvenuta cancellazione dei file in linea con le leggi italiane ed europee sulla Privacy e la sicurezza dei dati. Nessun tipo di informazione potrà essere recuperata, neanche tramite analisi forense.

Chi è nominato Titolare del trattamento dovrebbe rivolgersi a questo tipo di aziende e utilizzare questi prodotti al fine di tutelare i dati dei propri clienti.

Il Regolamento Generale sulla Protezione dei Dati, quindi, ha risvegliato la sensibilità delle aziende sull'importanza di trattare i dati personali in maniera corretta in tutte le sue sfaccettature, dalla loro creazione alla loro eliminazione, che deve essere svolta seguendo determinati standard di sicurezza.

Articolo a cura di **Stefano Gorla** e **Giorgia Tursini**