DISTRUZIONE DOCUMENTI

SICURA, CERTIFICATA, NELLA TUA AZIENDA

Studi & Ricerche

Perché la tua azienda è obbligata a distruggere documenti, archivi hard disk e supporti digitali che contengono dati riservati.

Cosa dice il GDPR e cosa rischi in caso di smarrimento (*data breach*).

Indice dei contenuti

CONTENUTI

INTRODUZIONE

In tutte le aziende, grandi o piccole, arriva il momento in cui liberarsi di un archivio pieno di vecchi faldoni, smaltire qualche computer ormai vecchio o assegnare il telefono aziendale ad una nuova persona. Cosa hanno in comune tutte queste situazioni? **Faldoni, hard disk e smartphone sono pieni di dati sensibili di dipendenti, consumatori, collaboratori e clienti e anche zeppi di informazioni strategiche per l'azienda.**

Cosa succede se il supporto non è distrutto correttamente e i dati vengono smarriti? Cosa prevede il GDPR in questo caso? **Vediamo tre domande che un'azienda dovrebbe porsi in relazione ai dati riservati contenuti in documenti di carta e digitali. Per essere conforme al GDPR ed evitare altri guai!**

La prima domanda: c'è una legge che mi obbliga a distruggere i dati riservati che conservo nei miei archivi di carta e nei miei computer. La risposta è Sì.

La seconda: come faccio a liberarmi di questi dati senza rischiare conseguenze? La risposta è: adottando misure di sicurezza adeguate durante il processo di distruzione e/o smaltimento di archivi, hard disk e altri supporti. Quindi, no, non puoi affidarti alla ditta delle pulizie, a uno svuota – cantine o centri di recupero.

La terza: se smarrisco (volontariamente o meno) i dati personali e questi sono recuperati integri da terzi (data breach) devo aspettarmi delle sanzioni? La risposta è Sì, le sanzioni sono pesanti e anche la reputazione rischia di andare in pezzi.

Queste domande possono sembrare superflue nella già complicata vita burocratica delle aziende italiane, ma dopo aver letto le conseguenze di un eventuale smarrimento o diffusione anche accidentale di dati riservati, siamo certi che avrai cambiato idea.

PERCHÉ DEVI DISTRUGGERE I DATI RISERVATI IN MODO SICURO E CERTIFICATO

Prima di tutto, cerchiamo di capire insieme cosa sono i dati personali. Secondo la definizione del GDPR e del Garante della Privacy sono:

01 **i dati che permettono l'identificazione diretta:** come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. – e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

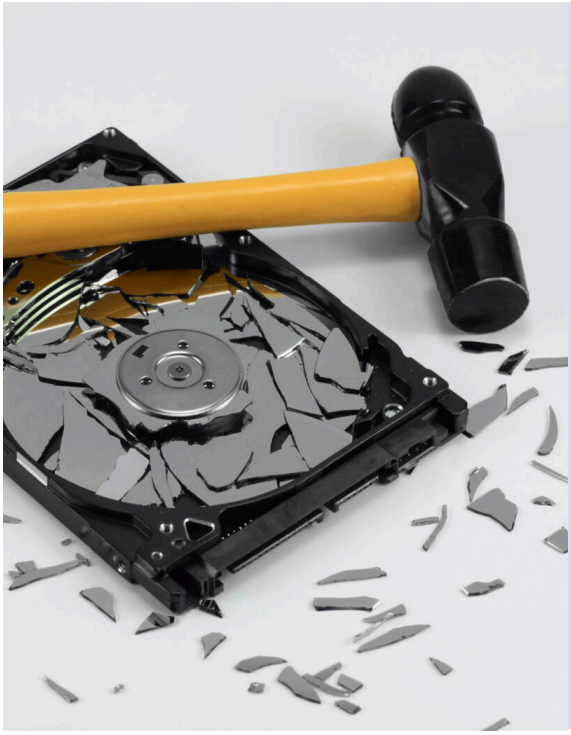
02 **i dati rientranti in particolari categorie:** si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;

03 **i dati relativi a condanne penali e reati:** si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale

COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?

Sempre secondo le definizione del Regolamento GDPR, **un** *data breach* **è una 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.**

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.



DATA BREACH

Una 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.

Alcuni esempi di violazione dei dati forniti dal Garante per la Privacy

1. **l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;**
2. **il furto o la perdita di dispositivi informatici contenenti dati personali;**
3. **la deliberata alterazione di dati personali;**
4. **l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;**
5. **la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;**
6. **la divulgazione non autorizzata dei dati personali.**
7. **documentazione cartacea integra inserita in contenitori aperti privi di serratura posizionati anche all'interno di perimetri aziendali.**

Un data breach può avvenire in qualsiasi momento della vita di un'organizzazione. Il momento della distruzione di un archivio cartaceo o dello smaltimento di un supporto digitale però è particolarmente pericoloso.

Quando hard disk, smartphone o faldoni di archivio lasciano l'azienda, quello è il momento in cui una perdita di dati o violazione diventa più probabile ed è per questo motivo che vengono richieste ed imposte idonee misure al fine di mitigare o eliminare il possibile smarrimento.

LE FONTI DI LEGGE CHE OBBLIGANO LE AZIENDE A DISTRUGGERE I DATI RISERVATI IN MODO SICURO

Siamo arrivati al punto in cui cerchiamo di capire cosa obbliga un'azienda a evitare lo svuota-cantine, imprese di pulizia, centri di recupero e affidarsi a un'azienda specializzata nella distruzione di dati riservati.

Il riferimento principale in materia è il Regolamento Europeo del 2016 (GDPR) approvato in Italia nel 2018. Ecco gli articoli principali che ci permettono di capire in modo semplice ma completo perché è necessario distruggere i dati riservati in modo sicuro, irrecuperabile e certificato.
Come vedremo in seguito i capisaldi del Regolamento che riguardano la distruzione e cancellazione sono:

1. **cos'è il Trattamento;**
2. **diritto alla cancellazione;**
3. **chi è il Titolare che responsabilità ha in merito alla distruzione;**
4. **chi è responsabile e che responsabilità ha?;**
5. **le misure idonee di sicurezza da adottare;**
6. **le certificazioni sulla distruzione che dimostrano il corretto trattamento.**

COS'È UN TRATTAMENTO DEI DATI PERSONALI?

L'Art. 4, paragrafo 2 definisce cosa rientra nel "trattamento" :

...qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione";

Ogni trattamento ha una percentuale di rischio più o meno elevata. La distruzione di un archivio cartaceo o di un hard disk, per esempio, è un'attività che espone a possibili violazioni dei dati.

In base al rischio devono quindi essere adottati criteri di sicurezza adeguati. Come vedremo più avanti il GDPR impone al titolare obblighi di nomina scritta e valutazione delle competenze e della capacità tecniche dei responsabili interni o esterni.

Senza questo non si è conformi alla normativa.

DIRITTO ALLA CENCELLAZIONE E ALL'OBLIO

Art 17, comma 1, lettera a): diritto alla cancellazione e all'oblio

L'interessato ha il 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;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento.

Anche prima della scadenza naturale l'interessato può chiedere la cancellazione definitiva dei dati riservati.

Essendo la cancellazione/distruzione un trattamento dei dati a tutti gli effetti di legge, dev'essere svolta nel rispetto del principio di accountability.

Di conseguenza è un'attività sotto la responsabilità del Titolare del trattamento, il quale, per evitare danni e sanzioni, dovrà inevitabilmente rivolgersi ad un provider esterno che deve fornire adeguate garanzie del corretto trattamento.

Sotto questo punto di vista sarà inevitabile rivolgersi ad un fornitore certificato e che accetti ad essere designato quale responsabile esterno ex art. 28 GDPR, meglio ancora se in grado di certificare l'avvenuta cancellazione/distruzione. Questo passaggio è inevitabile tenuto conto degli obblighi di prova stabiliti dalla legge e, normalmente, anche dai contratti dei più importanti players.

Art. 13, comma 2, lettera a):

[...] nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato [...]

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

Chi ci fornisce dei dati deve sapere in anticipo per quanti anni saranno conservati. Il periodo può essere fissato per legge (per esempio i 10 anni per le fatture) oppure può essere fissato dall'azienda ma deve chiarire perché.

Anche in questo caso, oltre questo periodo la distruzione sicura è obbligatoria.

In questo punto si definisce la catena delle responsabilità.

Dato che il Titolare richiede il consenso e che deve scegliere accuratamente responsabili del trattamento, in caso di *data breach* o violazioni verrà chiamato a risponderne *in primis* per poi rifarsi eventualmente su altri soggetti qualora ritenuti responsabili.

Come si può desumere è una cosa seria e gravosa.
Visti il trattamento e la loro conservazione, vediamo ora chi è il titolare del trattamento e che responsabilità ha.

CHI È IL TITOLARE DEL TRATTAMENTO E CHE RESPONSABILITÀ HA?

Art 4, paragrafo 7:

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali;

Art.5, paragrafo 1, lettera e):

I dati sono [...] conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati [...]

La conseguenza di questi articoli è che il titolare del trattamento deve provvedere alla cancellazione/distruzione dei dati raccolti tramite consenso informato una volta raggiunto lo scopo del trattamento stesso.

Non può conservarli per periodi ulteriori se non in casi eccezionali di pubblico interesse.

Oltre questo periodo la cancellazione/distruzione è di regola obbligatoria e deve essere fatta evitando un *data breach* di dati personali.

IL PRINCIPIO DELLA RESPONSABILITÀ: È SEMPRE COLPA TUA FINO A PROVA CONTRARIA

Art 5, paragrafo 2:

Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Come abbiamo visto, rispetto al precedente Codice della Privacy, il GDPR ha previsto il principio di *accountability*. Il titolare del trattamento dei dati deve essere in grado di dimostrare in maniera circostanziata alle autorità competenti, da un lato, e ai proprietari dei dati, dall'altro, di aver fatto tutto il possibile per proteggere i dati

Sacco per la raccolta sicura e tracciabile dei documenti cartacei con dati riservati

CHI È IL TITOLARE DEL TRATTAMENTO E CHE RESPONSABILITÀ HA?

Articolo 24: Responsabilità del trattamento

"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".

Aspetto importante è la dimostrazione a terzi di due cose: dell'adozione di misure di sicurezza che vedremo in seguito e della conformità del trattamento.

Quest'ultimo punto impone al titolare la responsabilità di dimostrare non solo formalmente ma soprattutto sostanzialmente l'adozione di un processo di distruzione conforme e sicuro in tutte le fasi.

Una maggiore credibilità e soprattutto una validazione esterna ed indipendente può essere fornita, come vedremo, da schemi certificativi specifici (vedi paragrafo sulle certificazioni).

Tra le responsabilità rientra anche la nomina del responsabile del trattamento seguendo specifiche indicazioni soprattutto di sicurezza come riportato più avanti.

L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento. Vediamo adesso gli oneri del responsabile del trattamento.

CHI È IL RESPONSABILE DEL TRATTAMENTO E CHE RESPONSABILITÀ HA?

Art 4, paragrafo 8 responsabile del trattamento:

[la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Art 28, Responsabile del trattamento (C81):

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

In questo punto viene evidenziato il profilo di sicurezza del responsabile del trattamento. Da cosa è costituito? **Fondamentalmente dalla sua capacità di sanitizzare il dato con sistemi idonei e specifici e non generici.**

Ad esempio sul mercato esistono varie tipologie di trituratori corredati da varie tipologie di lame che determinano la dimensione del triturato. Più sono sottili queste lame contrapposte più è alto il livello di sicurezza e dimensione del coriandolo.

Nello scenario attuale molte realtà dicono di distruggere documenti ma sono pochissimi che effettivamente hanno sistemi di distruzione che garantiscono ciò.

1. **come può un titolare del trattamento verificare questo?**
2. **ha le competenze per effettuare tale indagine?**

Dato che è sua responsabilità non solo verificare formalmente la dichiarazione del responsabile ma soprattutto verificarne la capacità di attuare misure di sicurezza, cosa lo aiuterà? **Le certificazioni specifiche come la UNI CEI21964, UNIEN 15713 e ADISA 8.0** di cui parleremo dopo.

CHI È IL RESPONSABILE DEL TRATTAMENTO E CHE RESPONSABILITÀ HA?

Art 28 Responsabile del trattamento (C81):

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche...

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

Art. 32: Misure di sicurezza

... il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio...

Documenti distrutti in modo irrecuperabile da Distruzione Documenti Srl

PERCHÉ NON POSSO AFFIDARMI A UN'AZIENDA DI MACERO O A UN'IMPRESA DI PULIZIE?

Capita spesso che l'attività di distruzione venga demandata a terzi che **non hanno certificazioni specifiche, mezzi e risorse per sanitizzare il dato in modo conforme al GDPR.** Questo accade quasi sempre quando ci si rivolge a imprese di pulizie o traslochi, centri di recupero e macero.

Immaginiamo un Titolare del trattamento del dato che sta effettuando uno spostamento di uffici e vengano fuori documenti da distruggere.

Chiede alla società di traslochi di distruggerli senza verificare le misure di sicurezza richieste dal trattamento e senza sapere dove saranno portati i documenti.

Tale procedimento, per essere conformi ed evitare salate sanzioni, deve essere **formalizzato per iscritto in modo tale che tutti i responsabili ed eventuali sub responsabili siano informati e osservino le indicazioni del titolare.** Tale attività di nomina è la prima cosa verificata dall'autorità garante ed ispettiva.

I trattamenti da parte di un responsabile sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli:

- **la materia disciplinata e la durata del trattamento;**
- **la natura e la finalità del trattamento;**
- **il tipo di dati personali;**
- **le categorie di interessati;**
- **gli obblighi e i diritti del titolare del trattamento.**

CHI È IL RESPONSABILE DEL TRATTAMENTO E CHE RESPONSABILITÀ HA?

Art 28, par 4, Responsabile del trattamento:

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3...

Molto spesso accade che il materiale da distruggere venga preso come rifiuto omettendo l'atto di nomina del responsabile. Per esempio, un'impresa di pulizia che ritira il materiale da distruggere e poi lo affida a un centro di recupero, senza informare il Titolare del trattamento.

Se da un'ottica ambientale potrebbe essere corretto, sotto l'aspetto GDPR non lo è. Perché? Il processo di distruzione è un trattamento dei dati e non di rifiuti e come tale necessita di una nomina come già specificato a pagina 7.

Far ritirare un archivio aziendale solo con il **FIR** (formulario di identificazione dei rifiuti) trasferisce la responsabilità del rifiuto al centro di recupero ma lascia la responsabilità dei dati sempre e comunque al Titolare del trattamento.

Se il centro di recupero decide di processare i supporti tra un mese o 6 mesi lasciandoli in banchina, non elimina la responsabilità del Titolare del trattamento.

Questo perché una violazione può avvenire anche in un arco temporale indeterminato ed indefinito finché i dati non sono distrutti correttamente. Per più tempo, le informazioni sono lasciate intatte, più aumenta il rischio di una violazione.

LE CERTIFICAZIONI CHE AIUTANO IL RESPONSABILE DEL TRATTAMENTO A RIDURRE I RISCHI

Art 28, par 5: Responsabile del trattamento

L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

La presenza di certificazioni come la 9000, la 14001 etc. è semplicemente legata ai sistemi di gestione di qualità aziendale ed ambientale, certificazioni che non sono specifiche per il trattamento dei dati, quindi non garantiscono conformità al GDPR.

Vedremo nelle prossime pagine quali sono le certificazioni specifiche che possono essere usate per dimostrare di aver adottato tutte le misure richieste dal GDPR e la conformità al trattamento.

SE IL MATERIALE NON È DISTRUTTO COME SI DEVE, SEI SEMPRE TU IL RESPONSABILE

Cosa significa per te? Nonostante vengano rilasciati certificati di distruzione il materiale scartato essendo ancora integro contiene tutti i dati per i quali ci sia aspetta dopo il trattamento distruttivo la totale inintelligibilità.

Il possesso di un certificato di distruzione non è sempre sufficiente. In caso di rinvenimento o accesso a terzi non autorizzati, sei sempre ritenuto responsabile dall'autorità garante per non aver vigilato correttamente sull'operato del service provider e delle misure di sicurezza messe in atto.

Differenza tra il materiale conferito in cartiera da Distruzione Documenti Srl e quello di una normale azienda di pulizia uffici, di smaltimento o macero carta. Da notare la differente dimensione del ritaglio e come le informazioni riservate siano ancora visibili per il materiale non distrutto in modo conforme al GDPR.

I CODICI DI CONDOTTA E LE CERTIFICAZIONI CHE RIGUARDANO LA DISTRUZIONE DEI DATI RISERVATI: ISO/IEC 21964-3 E UNI EN 15713:2023

Articolo 40: Codici di condotta

(C98, C99, C167-C168) 1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

La distruzione sicura e certificata è diventata così stringente che ha portato alla **nascita di alcune certificazioni di qualità del processo di distruzione come la norma italiana ISO/IEC 21964-3 e la norma europea UNI EN15713:2023.**

Entrambe le norme mirano a regolamentare non la singola fase ma l'intero processo di distruzione effettuato sia conto proprio o per conto di altri.

Le norme in merito alla distruzione dei dati vengono intese come un processo dove ogni fase deve essere esaminata e progettata per essere sicura come **punto di raccolta, il trasporto, la distruzione in base a 7 livelli dimensionali e 3 di sicurezza nonché l'avvio al recupero o smaltimento di quanto distrutto.**

La certificazione 21964 di Distruzione Documenti Srl

Se decidi di esternalizzare tale servizio, un service provider certificato ISO/IEC 21964-3, UNI EN15713:2023 e ADISA 8.0 ti permetterà di dimostrare la tua *accountability* e dovuta diligenza alle autorità garanti o ispettive.

Purtroppo, da una ricerca commissionata da Distruzione Documenti Srl, emerge come **il 95% dei centri di recupero contattati effettua solo operazioni di compattazione dei documenti scartati con avvio al macero lasciando integri i documenti.**

Quindi, spesso un'azienda è convinta di aver distrutto irrimediabilmente le informazioni presenti in faldoni e documenti mentre finiscono in trituratori non adatti lasciano i dati riservati perfettamente leggibili.

95%

Dei centri di recupero in Italia effettua solo operazioni di compattazione dei documenti scartati con avvio al macero lasciando integri i documenti.

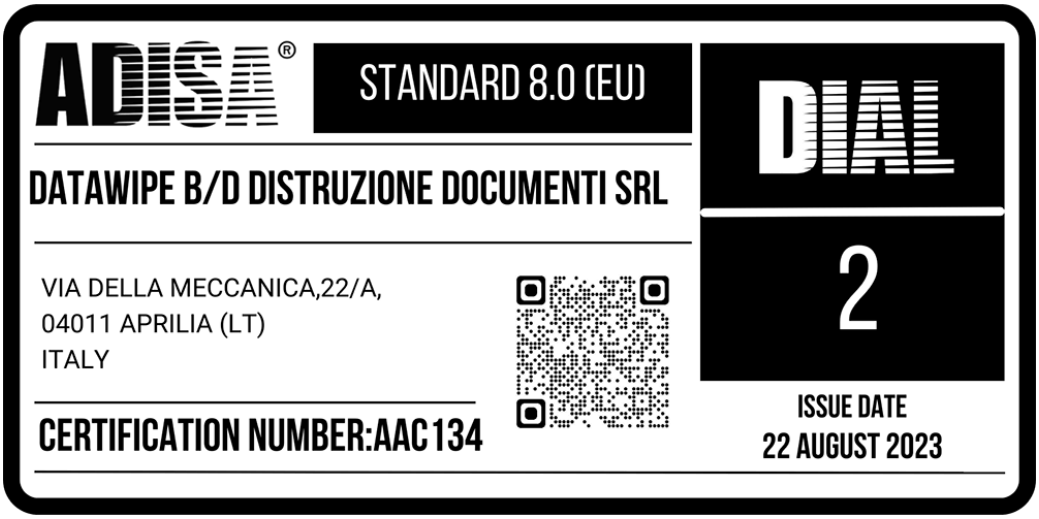
LE CERTIFICAZIONI SPECIFICHE CHE RIGUARDANO LA DISTRUZIONE DEI DATI DIGITALI: **ADISA 8.0**

Lo standard ADISA 8.0 è uno schema incentrato sul processo di eliminazione sicura delle informazioni e il recupero delle risorse IT dismesse ed è stato formalmente approvato dall'Ufficio del Commissario per l'Informazione del Regno Unito (ICO) (il omologo del Garante della Privacy Italiano) al fine di aiutare i Titolari del trattamento del dato e i responsabili esterni ad essere conformi alla normativa vigente GDPR.

Lo schema certificativo si articola in 4 sezioni:

1. **credenziali di business;**
2. **conformità normativa al GDPR;**
3. **risk management;**
4. **gestione ambientale.**

La specificità di ADISA 8.0 si basa sulla qualità dell'audit e sulla *data verification* degli applicativi software e hardware utilizzati nell'erogazione di servizi certificati di cancellazione, demagnetizzazione, distruzione e disintegrazione di supporti informatici di memorizzazione.



La certificazione ADISA 8.0 di Distruzione Documenti Srl

NOTIFICA DELLE VIOLAZIONI

Articolo 33: Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. 2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Come indicato al punto precedente, se i documenti sono ritirati come rifiuti, nel caso di una violazione la società che non opera come responsabile non sarà tenuta ad informare entro le 72 ore il Titolare del trattamento. Quest'ultimo, a sua volta, non potrà informare l'autorità di controllo competente rischiando sanzioni fino a 20 milioni di euro.

Qui si comprende il reale valore della nomina scritta di un responsabile e perché molti provider cercano di eluderla affermando che non serve. Per tutelarsi bisogna necessariamente seguire le indicazioni del regolamento, anche se scomode.

Le società specializzate come Distruzione Documenti Srl si assumono la nomina di responsabile del trattamento fornendo, nel caso, una contrattualistica specifica.

SANZIONI PREVISTE DAL GDPR IN CASO DI DATA BREACH: FINO A 20 MILIONI DI EURO

Nel caso in cui le organizzazioni (pubbliche amministrazioni, imprese) non rispettino gli obblighi previsti dal GDPR in materia di Data Breach, il **Regolamento prevede sanzioni pecuniarie fino a 10.000.000 euro o al 2% del fatturato mondiale annuo dell'esercizio precedente,** se superiore (primo scaglione), ovvero fino a 20.000.000 euro o al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore (secondo scaglione).

Secondo il Garante, le violazioni più gravi sono quelle che *"possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali. Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale".*

In particolare, **il Garante ha più volte sanzionato i Titolari del trattamento che, essendosi affidati ad un provider "di fortuna",** hanno visto i loro documenti e i loro hard disk abbandonati nei luoghi più disparati.

LE SANZIONI DEL GARANTE PER LA PRIVACY NEL CORSO DEGLI ANNI: UN MONITO PER TUTTI

Nel corso degli anni il Garante italiano per la Privacy ha più volte sanzionato aziende ed enti pubblici per aver violato la precedente Legge sulla Privacy e poi il GDPR.

Le sanzioni hanno colpito diversi soggetti e per diversi motivi: qui ne riportiamo alcune a titolo di esempio e rimandiamo al sito del Garante per l'approfondimento: **www.garanteprivacy.it**

PROVVEDIMENTO N. 535 DEL 28 NOVEMBRE 2013: SANZIONATO IL RDT DEL CENTRO IMPIEGO DI SAVONA

SINTESI DEL FATTO
Il RDT ha collocato un cassone di stoccaggio dell'archivio da eliminare in in un'area all'interno del Centro, di proprietà privata, interdetta al pubblico e delimitata da sbarre e cancelli", considerando che "il materiale depositato nel cassone attenesse esclusivamente a documentazione obsoleta e del tutto marginale".

Motivazione
Diversamente da quanto ritenuto, le menzionate cautele poste a protezione del cassone di stoccaggio non sono evidentemente sufficienti a qualificare un archivio controllato ove custodire dati sensibili (nel caso di specie anche dati inerenti lo stato di salute degli interessati) nel rispetto delle prescritte misure minime di sicurezza.

Sanzione
Sanzione pecuniaria per la violazione dell'art. 162, comma 2 bis del Codice, nella misura di euro 10.000,00 (diecimila).

PROVVEDIMENTO DEL 28 SETTEMBRE 2023 [9946386] USL TOSCANA CENTRO

SINTESI DEL FATTO

L'Autorità ha ricevuto una segnalazione in cui è stata lamentata una violazione della disciplina in materia di protezione dei dati personali in relazione alla presenza, nei locali dell'ex Sanatorio Guido Banti, sito a Pratolino e afferente all'Azienda Usl Toscana centro (di seguito Azienda), di documentazione sanitaria (es. ricette, cartelle cliniche e radiografie) in stato di abbandono e accessibile a chiunque.

Motivazione

Si rileva che la predetta documentazione sanitaria è stata conservata con modalità difformi rispetto a quelle indicate nella normativa di settore sopra richiamata e nello stesso regolamento aziendale adottato in materia e, quindi, in violazione degli artt. 5, par. 1, lett. a), e) e f) e 32 del Regolamento, dell'art. 75 del Codice con riferimento alla specifica disciplina di settore (d.lgs. 22/01/2004, n. 42).

Sanzione

Condanna la Usl Toscana centro a pagare la somma di euro € 50.000,00 entro 30 giorni

PROVVEDIMENTO DEL 22 FEBBRAIO 2024 [9999973] COMUNE DI CIVITA CASTELLANA

SINTESI DEL FATTO

La S.A.T.E. S.p.a. è una società mista pubblico-privata affidataria del servizio di raccolta e smaltimento dei rifiuti. In tale contesto, esaminata la tipologia del servizio affidato e le finalità dei trattamenti dei dati effettuati dai due soggetti coinvolti, appare evidente la diversa, distinta ed autonoma titolarità dei trattamenti in capo al Comune di Civita Castellana e alla S.A.T.E. S.p.a." Nel caso in oggetto il Garante ha esaminato la "Messa a disposizione "Su WhatsApp e poi su Facebook [... di] una foto del documento interno con cui il Comune di Civita Castellana ha notiziato la società SATE S.p.a., gestore del servizio di raccolta dei rifiuti, delle abitazioni in cui risiedono soggetti per i quali deve essere attivata una particolare forma di raccolta legata all'emergenza epidemiologica da Covid-19", per un totale di nove interessati coinvolti".

Motivazione

Il responsabile effettua il trattamento (in questo caso S.A.T.E. S.p.a.) attenendosi alle condizioni stabilite ai sensi del comma 4 bis e alle istruzioni impartite dal titolare, il quale, anche **tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni**. In questo caso, il Garante ha registrato "l'illiceità del trattamento effettuato dal Comune di Civita Castellana per la violazione degli artt. 5, par. 2, 24 e 28 del Regolamento".

Sanzione

Condanna il Comune di Civita Castellana a a pagare la somma di euro € 3.000 entro 30 giorni

QUANDO I DATI ESCONO DALL'AZIENDA SONO ESPOSTI A POTENZIALI E PERICOLOSI DATA BREACH

Dai *data breach* e dalle conseguenti sanzioni e responsabilità ci si può tutelare distruggendo documenti, archivi e supporti informatici con delle procedure sicure e irrimediabili prima che lascino l'azienda, direttamente in sede.

Per esempio, triturando un archivio, smagnetizzando un hard disk distruggendo gli smartphone che contengono i dati riservati direttamente sul posto e sotto il diretto controllo del Responsabile del Trattamento.

Oppure **assicurandosi che l'azienda che raccoglie questi supporti li trasporti in modo sicuro in uno stabilimento di distruzione che rispetti precisi standard di sicurezza.**

Per completare le procedure di sicurezza, è bene assicurarsi che l'azienda di distruzione si assuma l'incarico di Responsabile e si accolli eventuali responsabilità dello smarrimento.

Noi di Distruzione Documenti assicuriamo la distruzione sicura, certificata e direttamente in azienda di ogni supporto con informazioni riservate.

! *Assicurarsi sempre che l'azienda di distruzione si assuma l'incarico di Responsabile e si accolli eventuali responsabilità dello smarrimento.*

LA CANCELLAZIONE DEI DATI È UN OBBLIGO DI LEGGE, NON UNA SCELTA. COME ASSICURARSI UNA DISTRUZIONE SICURA E CERTIFICATA

Ecco un riepilogo sintetico per assicurarsi che i dati contenuti in documenti di carta e digitali siano distrutti in modo sicuro e certificato.

01 Affidarsi solo a un'azienda certificata. Non affidare i dati riservati alle imprese di pulizia o aziende che offrono il semplice macero

02 Distruggere gli archivi cartacei direttamente in sede e sotto il controllo del Titolare del Trattamento

03 Se non è possibile distruggere in sede, assicurarsi che l'azienda trasporti i documenti (cartacei o digitali) nella sede di distruzione assumendosi la carica di responsabile del trattamento e legale di eventuali *data breach*. Verificare se sono presenti polizze assicurative professionali E&O e non le semplici RCT RTO per indennizzi dovuti a data breach.

04 Controllare che la distruzione degli archivi di carta sia irrimediabile e definitiva e che le informazioni non possano essere recuperate. Questo è assicurato solo da aziende con certificazione UNI 21964 e UNI EN 15713

05 Se i dispositivi digitali non devono essere riutilizzati, renderli inutilizzabili con una smagnetizzazione e poi distruggerli fisicamente con un trituratore industriale

06 Se i dispositivi devono essere riutilizzati, la semplice formattazione non basta. Per cancellare definitivamente i file servono procedure di Wiping (sovrascrittura) ultra-professionali.

07 Farsi rilasciare un certificato di avvenuta distruzione con indicazione dei documenti e archivi digitali distrutti. In caso di eventuali azioni legali l'azienda potrà dimostrare di avere messo in atto le misure di sicurezza adeguare richieste dal GDPR.

CENTRO STUDI & RICHERCHE

Distruzione Documenti è la prima azienda italiana ad offrire un servizio di distruzione sicura e certificata di documenti, archivi aziendali e supporti digitali che contengono informazioni riservate.

Il servizio è destinato a professionisti, piccole, medie e grandi imprese, enti pubblici nazionali e locali e a soggetti che possiedono informazioni classificate.

Questo e-book è stato realizzato dal Centro Studi & Ricerche di Distruzione Documenti Srl

---

Aggiornato a luglio 2024

CONTATTI

Distruzione Documenti Srl
Sede legale:
Via Alessandro Farnese 26,
00192, Roma (RM)

www.distruzionedocumenti.com
info@distruzionedocumenti.com

Sede operativa:
Via della Meccanica 22/A
04011 - Aprilia (LT)
Tel: 06.88809638

Sede operativa:
Via degli Affari 234
24045 – Fara Gera D'Adda (BG)
Tel. 0363.1753003

Sede operativa:
Strada VIII 101- Interporto
95121 - Catania (CT)
Tel. 095.2291067