DISTRUZIONE DATI SENSIBILI

Distruzione Documenti e Archivi

Distruzione Supporti Magnetici

Distruzione presso la nostra azienda

VIA G. GIOLITTI, 20 z.i. | COPERTINO LE
INFO LINE 0832 930816
info@distruzionedatisensibili.it
www.distruzionedatisensibili.it
Distruzione Dati Sensibili - Arca

LL-C Certification

A.U.A.
Autorizzazione Unica Ambientale n. 4/2015

DISTRUZIONE SICURA DATI RISERVATI E SENSIBILI

CODICE D'USO

Arca

DISTRUZIONE DATI SENSIBILI

DATI PERSONALI COME DISTRUGGERLI

Il trattamento dei dati personali è un argomento di notevole importanza, che spesso viene sottovalutato. Ogni giorno veniamo a contatto con documenti che contengono informazioni personali, trascurando il fatto che i dati contenuti in suddetti documenti, siano essi in forma cartacea o informatica, siano protetti da specifiche norme per la tutela della Privacy.
Purtroppo, nella maggior parte dei casi, non vengono attuate nemmeno le più elementari precauzioni in difesa dei dati personali.
Solitamente la comune documentazione presente nei nostri uffici, viene smaltita e gestita con la raccolta dei rifiuti indifferenziati o ancor peggio con la raccolta differenziata della carta, lasciando per lunghi periodi di tempo questi documenti alla portata di chiunque.
Per quanto riguarda invece i supporti ottici e magnetici, spesso vengono donati ad altri organi oppure smaltiti nei centri di raccolta dei rifiuti, senza una corretta eliminazione dei dati presenti negli hard disk, mettendo a rischio i dati contenuti che, anche se cancellati, possono essere facilmente recuperati.

CODICE DELLA PRIVACY
D. Lgs. 196/2003:

IL CODICE DELLA PRIVACY, D. Lgs. 196/2003 obbliga alla distruzione dei dati sensibili una volta cessato il loro trattamento. Il responsabile del trattamento dei dati deve vigilare affinchè ciò avvenga, adottando misure di protezione dei dati e ne è responsabile penalmente e civilmente con sanzioni fino a 2 anni di arresto e € 50.000 di multa per mancata adozione di misure minime.

IL FURTO D'IDENTITA' avviene quando le informazioni personali di una persona o un'azienda vengono carpite ed utilizzate da un terzo soggetto. La frode d'identità avviene quando dei criminali utilizzano tali informazioni in maniera fraudolenta per ottenere credito, merci o altri servizi utilizzando per questo il nome della persona o dell'azienda.
IN CHE MODO AVVIENE IL FURTO D'IDENTITÀ?
Ogni giorno abbiamo a che fare con migliaia di informazioni: nomi ed indirizzi, dettagli di carte di credito, listini prezzi dei clienti, piani di marketing, dati finanziari, etc.
I ladri di identità potrebbero frugare nel vostro cestino della spazzatura per rubare queste informazioni.
Il furto di identità mette a rischio le aziende e le organizzazioni, che spesso mettono anche in pericolo clienti e impiegati se non distruggono in modo sicuro i dati sensibili.
Tutti gli stati hanno una legislazione di protezione dei dati per assicurare che le aziende adottino idonee politiche di smaltimento dei documenti.
Sono da distruggere dopo il cessato utilizzo tutti documenti contenenti dati personali e riservati, come dati dei clienti, dettagli delle buste paga dei dipendenti, dati di vendita, informazioni finanziarie, curricula e dati del personale, documenti legali, qualsiasi documento contenente firme, estratti conto bancari, scontrini delle carte di credito, fatture e bollette, copie della patente ed altri documenti di identità, ricevute, vecchie carte di credito e tessere.

D. Lgs. 196/2003: COSA PRESCRIVE IL CODICE DELLA PRIVACY

Art. 1. Diritto alla protezione dei dati personali

"Chiunque ha diritto alla protezione dei dati personali che lo riguardano".

Art. 4. Definizioni

Ai fini del presente codice si intende per:

a) "TRATTAMENTO", qualunque operazione o complesso di operazioni, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) "DATO PERSONALE", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificato o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) "DATI IDENTIFICATIVI", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "DATI SENSIBILI", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) "DATI GIUDIZIARI", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
   c) esatti e, se necessario, aggiornati;
   d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Art. 12. Codici di deontologia e di buona condotta

1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.
2. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice.
3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.
4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

Art. 13. Informativa

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
   a) le finalità e le modalità del trattamento cui sono destinati i dati;
   b) la natura obbligatoria o facoltativa del conferimento dei dati;
   c) le conseguenze di un eventuale rifiuto di rispondere;
   d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
   e) i diritti di cui all'articolo 7;
   f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili.
   Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 16. Cessazione del trattamento

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

a) distrutti;
b) ceduti ad altro titolare, purchè destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

2. La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

DIN 66399
NORMATIVA SULLA DISTRUZIONE CERTIFICATA

Con il progredire della tecnologia e delle teniche di archiviazione, i dati sensibili sono sempre più al centro dell'attenzione tanto da richiedere più volte l'intervento del legislatore per una corretta regolamentazione del settore, sia esso a livello nazionale che europeo.
DIN è il Deutsches Institut für Normung, Istituto tedesco per la standardizzazione dei formati.
La nuova normativa **DIN 66399**, è l'ultimo protocollo a livello internazionale per classificare e regolare le giuste linee guida per la protezione della privacy delle aziende e dei cittadini che trattano dati sensibili.
L'aggiornamento cambia gli attuali sistemi di sicurezza e fornisce criteri per classificare la distruzione dei diversi materiali, oltre ai documenti cartacei, inclusi CD/DVD, floppy, carte magnetiche, descrivendo con accuratezza le procedure e i requisiti necessari per una distruzione certificata sicura ed affidabile.

Nella sua completezza la normativa prende in considerazione la distruzione ed il successivo smaltimento di varie tipologie di materiali, definendone i vari livelli di distruzione. Ovviamente il grado di tutela dei dati aumenta a seconda dei dati trattati.

La normativa DIN 66399 è dunque molto particolareggiata ed estremamente attenta a classificare e prevedere ogni genere di situazione nella quale i documenti, siano essi cartacei che elettronici ma anche supporti informatici, si possono presentare.
La normativa stabilisce quindi anche il livello di sicurezza da applicare per ogni tipo di supporto, relazionato alla propria classe di protezione.
Vediamo nel dettaglio le classi di protezione, livelli di sicurezza e i tipi supporto.

La normativa DIN 66399 analizza il tipo di dati trattati dividendoli in tre classi fondamentali, permettendo di stabilire per ogni tipo supporto un preciso standard. Ogni classe necessita di uno specifico grado di protezione.

DIN 66399
CLASSI DI PROTEZIONE E RELATIVI RISCHI

- **PROTEZIONE 1 - Requisito di sicurezza normale per dati Interni:**
  La pubblicazione o diffusione non autorizzata avrebbe un impatto negativo limitato sulla società. Deve essere garantita la protezione dei Dati, altrimenti ci sarebbe un rischio per la posizione e la situazione finanziaria delle persone colpite.

- **PROTEZIONE 2 - Requisito di sicurezza elevato per dati Riservati:**
  La diffusione non autorizzata avrebbe un effetto notevole sulla società e potrebbe violare obblighi di legge o la legge stessa. La protezione dei dati personali deve soddisfare severi requisiti, ci sarebbe altrimenti un notevole rischio per la pposizione sociale e la situazione finanziaria delle persone colpite.

- **PROTEZIONE 3 - Requisito di sicurezza molto alto, dati riservati e segreti:**
  La diffusione non autorizzata avrebbe conseguenze gravi per terminali della società, con violazione degli obblighi di riservatezza commerciale, contratti o leggi. È essenziale che la riservatezza dei dati personali sia mantenuta, altrimenti ci sarebbe un rischio per la salute, la sicurezza o la libertà personale degli interessati.

LIVELLI DI SICUREZZA STABILITI DALLA NORMA

Di recente, la norma tecnica che esplicita i livelli di sicurezza per la distruzione dei documenti identificata come DIN 32757 è stata sostituita dalla nuova **DIN 66399**. L'aggiornamento cambia gli attuali sistemi di sicurezza e fornisce criteri per classificare anche la distruzione di materiali diversi dalla carta inclusi CD/DVD, floppy, schede a chip, carte magnetiche.

Ecco la tabella del nuovo sistema DIN per i distruggidocumenti:

- **LIVELLO DI SICUREZZA P-1:** per i dati comuni, riduce il volume della carta straccia (distruzione in strisce inferiori a 12 mm o particelle max 2 cm^2);
- **LIVELLO DI SICUREZZA P-2:** per i dati interni, i frammenti rimangono leggibili (distruzione in strisce inferiori a 6 mm o particelle max 0,8 cm^2);
- **LIVELLO DI SICUREZZA P-3:** per i dati riservati, difficile il riassemblaggio e la lettura (distruzione in strisce non superiori a 2 mm o particelle max 320 mm^2);
- **LIVELLO DI SICUREZZA P-4:** per dati riservati e sensibili, estremamente difficile il riassemblaggio (distruzione in particelle 4×40 mm o particelle max 160 mm^2);
- **LIVELLO DI SICUREZZA P-5:** per dati strettamente riservati, impossibile il riassemblaggio (distruzione in particelle 2×15 mm o particelle max 30 mm^2);
- **LIVELLO DI SICUREZZA P-6:** per dati segretissimi, sicurezza elevata per documenti di estrema sensibilità (distruzione in particelle 0,8×12 mm o particelle max 10 mm^2);
- **LIVELLO DI SICUREZZA P-7:** per dati segretissimi, il maggiore livello di sicurezza possibile (distruzione in particelle 0,8×5 mm o particelle max 5 mm^2).

DIN 66399
TIPI DI SUPPORTO

I supporti vengono divisi in 6 categorie contraddistinte da una specifica nomenclatura all'interno di ognuna, vengono elencati i supporti previsti.

P

Informazioni in dimensioni originali: ad es. carta, pellicole radiografiche, forme da stampa

O

Supporti dati ottici: ad es. CD/DVD

T

Supporti dati magnetici: ad es. dischetti, carte d'identificazione con bande magnetiche

E

Supporti dati elettronici: ad es. chiavette USB, smart card ad es. unità a stato solido, memorie flash di smartphone e tablet PC, Schede di memoria di fotocamere digitali

F

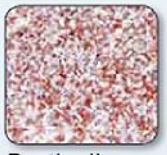
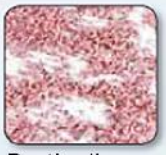
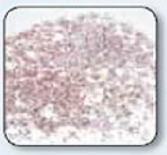
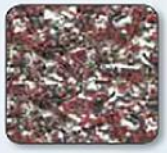
Informazioni in forma ridotta: ad es. pellicole, lucidi

H

Dischi rigidi con supporto dati magnetico: hard disk

PROTEZIONE DOCUMENTI
DIN 66399

LIVELLO FRAMMENTAZIONE PER TIPO DI SUPPORTO

P-1	**P-2**	**P-3**	**P-4**	**P-5**	**P-6**	**P-7**
						
Strisce max 12 mm	Strisce max 6 mm	Particelle max 320 mm²	Particelle max 160 mm²	Particelle max 30 mm²	Particelle max 10 mm²	Particelle max 5 mm²
O-1	**O-2**	**O-3**	**O-4**	**O-5**	**O-6**	**O-7**
						
Particelle max 2000 mm²	Particelle max 800 mm²	Particelle max 160 mm²	Particelle max 30 mm²	Particelle max 10 mm²	Particelle max 5 mm²	Particelle max 0,2 mm²
T-1	**T-2**	**T-3**	**T-4**	**T-5**	**T-6**	**T-7**
						
Meccanicamente inutilizzabile	Particelle max 2000 mm²	Particelle max 320 mm²	Particelle max 160 mm²	Particelle max 30 mm²	Particelle max 10 mm²	Particelle max 2,5 mm²
E-1	**E-2**	**E-3**	**E-4**	**E-5**	**E-6**	**E-7**
						
Meccanicamente/ elettronicamente inutilizzabile	Diviso	Particelle max 160 mm²	Particelle max 30 mm²	Particelle max 10 mm²	Particelle max 1mm²	Particelle max 0,5 mm²
F-1	**F-2**	**F-3**	**F-4**	**F-5**	**F-6**	**F-7**
						
Particelle max 160 mm²	Particelle max 30 mm²	Particelle max 10 mm²	Particelle max 2,5 mm²	Particelle max 1 mm²	Particelle max 0,5 mm²	Particelle max 0,2 mm²
H-1	**H-2**	**H-3**	**H-4**	**H-5**	**H-6**	**H-7**
						
Meccanicamente/ elettronicamente inutilizzabile	Danneggiato	Deformato	Diviso e spezzato più volte. Particelle max 2000 mm²	Diviso e spezzato più volte. Particelle max 320 mm²	Diviso e spezzato più volte. Particelle max 10 mm²	Diviso e spezzato più volte. Particelle max 5 mm²

CLASSI DI PROTEZIONE
LIVELLI DI SICUREZZA


Con la normativa **DIN 66399** in fase di distruzione i **7 LIVELLI DI SICUREZZA** applicati alle **3 CLASSI DI PROTEZIONE**

CLASSE DI PROTEZIONE 1
LIVELLO DI SICUREZZA 1
LIVELLO DI SICUREZZA 2
LIVELLO DI SICUREZZA 3

CLASSE DI PROTEZIONE 2
LIVELLO DI SICUREZZA 3
LIVELLO DI SICUREZZA 4
LIVELLO DI SICUREZZA 5

CLASSE DI PROTEZIONE 3
LIVELLO DI SICUREZZA 5
LIVELLO DI SICUREZZA 6
LIVELLO DI SICUREZZA 7

Nello schema sottostante, vengono incrociate le tre categorie di protezione con i livelli di sicurezza per tipo di supporto:

PROTEZIONE DOCUMENTI
DIN 66399

CLASSE DI PROTEZIONE 1	LIVELLO DI SICUREZZA 1	P-1	O-1	T-1	E-1	F-1	H-1
	LIVELLO DI SICUREZZA 2	P-2	O-2	P-2	E-2	F-2	H-2
	LIVELLO DI SICUREZZA 3	P-3	O-3	P-3	E-3	F-3	H-3
CLASSE DI PROTEZIONE 2	LIVELLO DI SICUREZZA 4	P-4	O-4	P-4	E-4	F-4	H-4
	LIVELLO DI SICUREZZA 5	P-5	O-5	P-5	E-5	F-5	H-5
CLASSE DI PROTEZIONE 3	LIVELLO DI SICUREZZA 6	P-6	O-6	P-6	E-6	F-6	H-6
	LIVELLO DI SICUREZZA 7	P-7	O-7	P-7	E-7	F-7	H-7

LINEE GUIDA SULLE MODALITÀ DI DISTRUZIONE

CONTRATTO CLIENTE/DITTA APPALTATRICE

Il processo commerciale tra il cliente e il fornitore del servizio viene regolato da un contratto scritto, dove il cliente ha l'onere di scegliere un'azienda appaltatrice che fornisca sufficienti garanzie in quanto a mezzi tecnici utilizzati, mezzi organizzativi e misure di sicurezza utilizzate per la raccolta e la distruzione dei materiali.
Deve altresì assicurarsi che tutte le prescrizioni della norma vengano rispettate e riportare le modalità e i livelli di distruzione concordati.

COME AVVIENE IL PROCESSO DI DISTRUZIONE DEI DATI RISERVATI E SENSIBILI?

Tutto il processo di distruzione avviene nel pieno rispetto delle normative vigenti, garantendo un servizio di qualità rispettando la Privacy del cliente e dell'interessato i cui dati vengono trattati.
Il servizio può essre effettuata a chiamata del cliente, oppure su richiesta, possone essere forniti dei contenitori di sicurezza dove riporre i dati sensibili in attesa di distruzione.
È il cliente stesso a raccogliere il materiale sensibile.

TRASPORTO DOCUMENTI INTEGRI (DISTRUZIONE FUORI SEDE)

Appena il materiale contenente dati sensibili è pronto, la ditta appaltattrice invierà il suo personale, qualificato e formato per applicare la normativa **DIN 66399**, a ritirare i documenti per trasportarli presso il proprio sito dove avvierà il processo di distruzione.
La distruzione avviene all'interno di un impianto industriale dotato delle più moderne tecnologie, in un ambiente completamente protetto.
Il sito dell'azienda, all'interno del quale i documenti saranno triturati, dispone di un sistema di allarme antintrusione, conforme alle norme, dotato di centrale per il monitoraggio.
L'impianto è altresì dotato di un circuito di video controllo, con apparecchi di registrazione, installato per monitorare le aree di scarico, custodia e distruzione dei documenti.

VEICOLO CON IMPIANTO MOBILE (DISTRUZIONE DOMICILIARE)

Su richiesta, tale processo di distruzione può avvenire nella sede del cliente, con automezzo dotato di macchinario mobile. In questo caso il veicolo deve operare all'interno della stessa sede del cliente dove sosterà fino alla fine del processo di distruzione.
Il veicolo, non sarà mai lasciato incustodito quando a bordo vi è del materiale integro.

SMALTIMENTO FINALE DEL PRODOTTO

Il prodotto finale, costituito da frammenti di materiale, come carta e parti elettroniche sarà stoccato ed avviato al riciclo, nel rispetto delle normative ambientali.

GARANZIE PER IL CLIENTE

L'azienda addetta a tale servizio opererà nel pieno rispetto della Privacy delle normative ambientali, disponendo delle certificazioni e delle autorizzazioni necessarie.
Alla fine del processo di distruzione dei documenti sensibili, sarà rilasciato un Certificato di Distruzione che soddisfi i requisiti di sistema del cliente.

DISTRUZIONE DATI SENSIBILI

Arca

distruzionedatisensibili.it