PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4619 di Mercoledì 22 gennaio 2020

Una strategia organica per la distruzione di documenti con dati personali

Linea guida per lo sviluppo di un concetto di cancellazione con definizione dei periodi di cancellazione per dati personali: DIN 66398: 2016.

Chi scrive ha partecipato alla elaborazione della norma en 15713, che dà indicazioni sulle modalità cui possono essere distrutti vari supporti. Che poi tali supporti contengono dati personali, oppure no, è fatto incidentale. L'entrata in vigore del nuovo regolamento europeo sulla protezione dei dati ha indotto la Germania a sviluppare una serie di norme, da parte dell'ente normativo nazionale Deutsche Industrie Normen, che fanno specifico riferimento a questo tema. La prima norma DIN 66398 fa riferimento alle linee guida i principi da adottare, per decidere quali dati debbano essere cancellati con quali modalità, mentre la seconda serie normativa DIN 66399 fa riferimento agli aspetti tecnici della cancellazione, quale che sia il supporto, su cui tali dati sono memorizzati.

Esaminiamo di seguito queste norme, che, in assenza di normative italiane ed europee, costituiscono regola d'arte per questo fondamentale adempimento, imposto regolamento generale europeo e dal decreto legislativo 101 barra 2018, che ha recepito in Italia alcuni aspetti specifici di tale regolamento.

DIN 66398: 2016 - Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information

Esiste un obbligo legale e generale di eliminare i dati personali se non sono più necessari per il processo aziendale e non sono in conflitto con i requisiti di conservazione previsti dalla legge. Finora questo è fatto raramente dalle aziende. La norma DIN 66398 costituisce un prezioso riferimento per il titolare, che desidera rispettare puntualmente i dettati in materia di cancellazione dei dati personali.
In Germania, cinque società specializzate si sono unite per dare vita alla norma in questione. Il progetto è stato finanziato dal ministero federale dell'economia della tecnologia. Sono lieto di poter mettere a disposizione dei lettori una versione di questa norma, leggermente differente dalla versione finale ma disponibile gratuitamente.

Vedremo in un paragrafo successivo l'illustrazione della serie normativa DIN 66399, che esamina gli aspetti tecnici.

La norma DIN 66398 definisce un modello per l'impostazione e l'attuazione delle regole afferenti alla cancellazione dei dati personali. La norma descrive le procedure in base alle quali vengono definite le regole di cancellazione. Essa raccomanda inoltre una procedura per documentare i criteri adottati e le

modalità di attuazione, delle decisioni assunte.

Tutti i dati gestiti dal titolare vengano divisi in categorie e per ogni categoria viene definita una regola di cancellazione. Questa regola di cancellazione governata da due parametri:

- il periodo di custodia,
- le modalità di cancellazione.

È evidente che in un mondo ideale, i dati, soprattutto su supporto informatico, dovrebbero essere eliminati automaticamente, come ad esempio avviene negli impianti di videosorveglianza, laddove il registratore digitale delle immagini provvede in automatico alla cancellazione dei dati archiviati, al termine del periodo di conservazione determinato dal titolare. È bene comunque sottolineare il fatto che questa norma offre delle linee guida, ma la responsabilità finale in merito ai tempi e modi della cancellazione resta in carico al titolare. In particolare, la norma illustra i seguenti passi, che possono essere adottati dal titolare per attuare questo processo:

- Determinazione dei tipi di dati esistenti nei database dell'azienda
- Riepilogo dei tipi di dati nelle classi di eliminazione
- Definizione delle regole di cancellazione per i tipi di dati
- Definizione di regole di attuazione concrete
- Definizione della persona responsabile dell'attuazione
- Documentazione delle misure adottate e da adottare e manutenzione della documentazione

Questa norma è tanto più importante, in quanto una indagine, condotta in Germania, ha mostrato che circa la metà degli intervistati non ha un chiaro concetto dei principi di conservazione dei dati e di modalità di cancellazione. In particolare molte aziende non sanno: quali dati eliminare quando, dove i dati si trovano, come sono stati distribuiti.

Il diritto all'oblio

L'articolo 17 del regolamento europeo (diritto alla cancellazione, diritto all'oblio) offre una sorta di linea guida per evidenziare la necessità di cancellazione dei dati; in particolare:

- I dati personali non sono più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati (vedi sopra).

- L'interessato revoca il proprio consenso su cui si basa il trattamento e non esiste altra base giuridica per il trattamento.
- L'interessato si oppone al trattamento e non vi sono motivi legittimi per il trattamento.
- I dati personali sono stati trattati illegalmente.
- La cancellazione dei dati personali è necessaria per adempiere a un obbligo legale, ai sensi del diritto dell'Unione o nazionale, a cui è soggetto il responsabile del trattamento.

Tuttavia, l'obbligo di cancellazione non si applica se i dati personali sono (ancora) richiesti per:

- esercitare il diritto alla libertà di espressione e di informazione

- adempiere a un obbligo legale richiesto dal diritto dell'Unione o degli Stati membri a cui è soggetto il responsabile del trattamento, o svolgere un compito di interesse pubblico o nell'esercizio di un'autorità pubblica delegata al responsabile del trattamento
- motivi di interesse pubblico nel campo della sanità pubblica
- fini di archiviazione di interesse pubblico, a fini di ricerca scientifica o storica o a fini statistici,
- far valere, esercitare o difendere azioni legali.

Sono numerosi gli obblighi legali e contrattuali, che comportano l'obbligo per le società di conservare i dati personali per un determinato periodo di tempo. Dopo questo periodo, si applica l'obbligo di cancellazione di cui sopra.

Allo stesso modo, si applica l'articolo 18 del GDPR (Diritto di limitazione del trattamento). Successivamente, a determinate condizioni, l'interessato ha il diritto di richiedere al responsabile del trattamento di limitare il trattamento.

Non per nulla l'articolo 30, che fa riferimento al registro dei trattamenti, prevede esplicitamente che tale registro contenga una indicazione delle scadenze per la cancellazione delle diverse categorie di dati.

Linee guida per lo sviluppo di una procedura di cancellazione

La norma DIN 66398 fornisce raccomandazioni per contenuto, struttura e responsabilità in un concetto di cancellazione dei dati personali. Inoltre descrive le procedure per determinare i periodi di cancellazione e le regole di cancellazione per vari tipi di dati.

Quando si applica la norma allo sviluppo di un concetto di eliminazione, questi termini svolgono un ruolo:

termine	**definizione**
tipo di dati	Tutti i dati trattati per uno scopo comune
tempo di cancellazione	Periodo di tempo dopo il quale i dati dovrebbero (di solito) essere eliminati, tenendo conto dei periodi di conservazione contrattuali e legali
Periodo di inizio	Determinare quando inizia il periodo di cancellazione
classi di estinzione	Riepilogo dei tipi di dati dopo il periodo di eliminazione e l'ora di inizio
regola di cancellazione	Regola per ogni classe di cancellazione
regola di distruzione	Specifica la regola di distruzione in base alla tecnologia utilizzata
responsabilità	Sono definiti per l'implementazione della cancellazione, nonché per la creazione e il mantenimento del principio di cancellazione

Vediamo adesso gli aspetti tecnici della cancellazione, che sono illustrati nella serie normativa DIN 66399 ovvero la nuova normativa a livello europeo sulla classificazione e distruzione dei documenti contenenti dati sensibili. Tale cena normative articolata in tre norme:

DIN 66399-1-Office machines - Destruction of data carriers - Part 1: Principles and definitions

DIN 66399-2- Office machines - Destruction of data carriers - Part 2: Requirements for equipment for destruction of data carriers

DIN SPEC 66399--Office machines - Destruction of data carriers - Part 3: Process for destruction of data carriers

Con il progredire della tecnologia e delle tecniche di archiviazione avanzate, i dati sono entrati sempre più al centro dell'attenzione tanto da richiedere più volte l'intervento da parte del legislatore per regolare il settore, sia esso a livello nazionale che europeo. La nuova normativa DIN 66399, è l'ultimo protocollo a livello internazionale per classificare e dettare rigide linee guida per la protezione dei dati personali di ogni cittadino e dei titolari, che trattano dati particolari. Molto evoluta rispetto alla precedente normativa DIN 32757, la DIN 66399 non regolamenta soltanto i classici supporti cartacei, ma amplia il raggio d'azione anche a tutti i supporti elettronici e digitali, descrivendo accuratamente procedure e requisiti necessari per una distruzione certificata sicura ed affidabile.

Prima ancora di descrivere le procedure da adottare per la distruzione dei documenti, la normativa DIN 66399 analizza il tipo di dati trattati dividendoli in tre classi fondamentali di riferimento, in modo da poter stabilire per ogni supporto un preciso standard. Ogni classe necessita di uno specifico grado di protezione:

Classe di protezione 1: Normale necessità di protezione per dati personali	La divulgazione o trasmissione non autorizzata di dati comporterebbe limitate conseguenze negative per l'azienda. Deve essere garantita la protezione dei dati personali. Diversamente, sussiste il rischio che vengano compromesse la posizione e le condizioni economiche del soggetto interessato.
Classe di protezione 2: Elevata necessità di protezione per dati particolari	La divulgazione non autorizzata comporterebbe enormi conseguenze per l'azienda e potrebbe violare obblighi contrattuali o leggi. La protezione di dati personali deve soddisfare stringenti requisiti. Diversamente sussiste il rischio che vengano seriamente compromesse la posizione e le condizioni economiche dell'interessato.
Classe di protezione 3: Necessità di protezione elevata per dati particolari critici, e soggetti a segretezza.	La divulgazione non autorizzata comporterebbe serie conseguenze, che potrebbero compromettere l'esistenza stessa dell'azienda e violare segreti professionali, contratti o leggi. La protezione dei dati personali deve essere assolutamente garantita. Diversamente possono essere messe a rischio l'incolumità e la vita dell'interessato, nonché la sua libertà personale.

La serie normativa quindi esamina sei tipologie di supporti dei dati, previsti dalla normativa DIN 66399, come ad esempio supporti cartacei, supporti informatici, supporti ottici via dicendo.

Successivamente la serie normativa passa ad esaminare 7 livelli di sicurezza della normativa DIN 66399

La normativa prevede per la fase di distruzione, 7 livelli di sicurezza applicati alle 3 classi di protezione, illustrati in precedenza. In particolare, maggiore è il livello e più piccoli saranno i frammenti, al termine della fase di distruzione certificata:

	Livelli di sicurezza
Classe di protezione 1	1, 2, 3
Classe di protezione 2	3, 4, 5
Classe di protezione 3	5, 6, 7

Livello di sicurezza 1:
Documenti di carattere generale che devono essere invalidati o resi illeggibili.

Livello di sicurezza 2:
Documenti interni che devono essere invalidati o resi illeggibili.

Livello di sicurezza 3:
Supporti dati con dati sensibili, riservati e personali che richiedono una maggiore protezione.

Livello di sicurezza 4:
Supporti dati con dati particolarmente sensibili e riservati, nonché dati personali che richiedono una maggiore protezione.

Livello di sicurezza 5:
Supporti dati con informazioni segrete di rilevanza per l'esistenza di una persona, azienda o istituzione.

Livello di sicurezza 6:
Supporti dati con documenti segreti da trattare con straordinarie precauzioni e misure di sicurezza

Livello di sicurezza 7:
Supporti dati segreti per cui è necessario adottare le misure di prevenzione di massima sicurezza.

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.
Nello schema seguente, vengono incrociate le tre categorie menzionate sopra per una panoramica completa:

Ecco la tabella del nuovo sistema DIN per i distruggidocumenti:

classificazione	carta, pellicola, etc.	supporti media CD/ DVD
P-1 riduce il volume della carta straccia	particelle ? 2cm² o ? 12mm strisce	particelle ? 2cm²
P-2 ad uso personale, i frammenti rimangono leggibili	particelle ? 0,8cm² o ? 6mm strisce	particelle ? 0,8cm²
P-3 documenti riservati, difficile l'assemblaggio e la	particelle ?320mm² o ? 2mm strisce	particelle ? 160mm²

lettura		
P-4 documenti riservati, estremamente difficile l'assemblaggio	particelle ? 160mm² e larghezza particella 6 mm max. (es.4x38mm)	particelle ? 30mm²
P-5 documenti strettamente riservati, impossibile l'assemblaggio	particelle ? 30mm² e larghezza particella 2mm max. (es. 2x15mm)	particelle ? 10mm²
P-6 sicurezza elevata per documenti di estrema sensibilità	particelle ? 10mm² e larghezza particella 1 mm max. (es.0.8x12 mm)	particelle ? 5mm²
P-7 il maggiore livello di sicurezza possibile	particelle ? 5mm² e larghezza particella 1mm max. (es. 0.8x5mm)	particelle ? 0.2mm²

Adalberto Biasiotti

Allegato- testo non soggetto a copyright - " Linea guida per lo sviluppo di un concetto di cancellazione con definizione dei periodi di cancellazione per dati personali"