POLICY
DISMISSIONE HARDWARE CONTENENTE DATI

COD. C.12
VERS. 01 DEL 05.2022

CONTIENE:

1. **POLICY**

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE

PREMESSA

Il GDPR (Regolamento Generale sulla Protezione dei Dati) ha come suo obiettivo principale quello di disciplinare il corretto trattamento di dati. Ebbene, il trattamento si identifica con tutta quella serie di attività che possono essere eseguite su un dato personale. Abbiamo quindi la raccolta, l'archiviazione, la condivisione e, perché no, anche la cancellazione.
Tutta la vita del dato personale deve sottostare alle norme del GDPR, per questo, anche quando decidiamo di dismettere un computer o un tablet dobbiamo ricordarci che ciò potrebbe portare ad almeno due ordini di criticità a cui fare attenzione: 1) il riutilizzo del device da parte di terzi; 2) la corretta cancellazione dei dati in caso di smaltimento. Quanto alla fattispecie di cui al numero 1, non è cosa rara che una PA ceda o riceva computer da terzi anche a titolo gratuito. In queste situazioni è necessario evitare che soggetti non autorizzati accedano a dati personali trattati dal precedente titolare. La fattispecie n.2 porta con sé il problema dell'incertezza di chi potrebbe o meno entrare in possesso di un hardware abbandonato, con conseguente indeterminatezza dei destinatari dei dati personali ivi presenti.
Ebbene, con il provvedimento dell'Autorità Garante per la protezione dei dati personali del 13 ottobre 2008 DOCWEB 1571514 dal titolo "*Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*" sono state indicate regole importanti sulla corretta dismissione dei device come computer, hard disk, tablet, dispositivi di archiviazione esterni (disco esterno), chiavette USB ed altro, distinguendo in modo netto dalla condotta richiesta in caso di riuso delle apparecchiature o in caso di smaltimento delle stesse.

USO CORRETTO DEGLI HARDWARE

In base a quanto ricorda il Garante nel citato provvedimento, in caso di reimpiego e riciclaggio computer, tablet, chiavette USB ed altri device elettronici, le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità.

Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l'altro, in:

MISURE TECNICHE DA ADOTTARE PREVENTIVAMENTE

1. Cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura.

2. Memorizzazione dei dati sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (CD-ROM, DVD-R) in forma automaticamente cifrata al momento della loro scrittura.

MISURE TECNICHE DA ADOTTARE AL MOMENTO DELLA CANCELLAZIONE SICURA DEI DATI

1. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali *wiping program* o *file shredder*) che provvedono, una volta che l'utente abbia eliminato dei file dal PC in uso (o da altri device), a scrivere ripetutamente nelle aree vuote del disco sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati. Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all'importanza delle informazioni di cui si vuole impedire l'indebita acquisizione) **varia da sette a trentacinque**.

2. Formattazione "a basso livello" dei dispositivi di tipo hard disk (*low-level formatting–LLF*), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;

3. Demagnetizzazione (*degaussing*) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

SMALTIMENTO DEGLI HARDWARE

In questo caso il Garante Privacy, nell'esaminare le migliori modalità di smaltimento di rifiuti elettrici ed elettronici, suggerisce diverse soluzioni che vanno dalla distruzione fisica degli hardware alla smagnetizzazione con conseguente inutilizzabilità degli stessi. A prescindere dagli strumenti e dalle tecniche utilizzate, la finalità che si deve perseguire è quella di assicurare una reale ed effettiva cancellazione dei dati oppure la loro non intelligibilità. A tal riguardo, è chiaro che molte delle attività sopra elencate risultano piuttosto tecniche, motivo per cui, salvo presenza di personale particolarmente specializzato, per lo smaltimenti dei device e degli hardware in generale è caldamente consigliabile affidarsi all'ausilio di soggetti terzi i quali, si ricorda, dovranno necessariamente essere nominati quali Responsabili esterni del trattamento.