

MISURE DI PROTEZIONE DEI DATI PERSONALI

POLICY DI ISTITUTO PER LA DISMISSIONE DI HARDWARE CONTENENTE DATI

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 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 indeterminazione 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 (Raee) 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

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.

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

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.

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;

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).

ACCESSO AL DEVICE

In caso di cessazione, trasferimento o cambio di assegnazione di un dipendente, i dispositivi informatici già in uso (quali computer, tablet, smartphone o altri device) devono, di regola, essere sottoposti a procedure di cancellazione sicura dei dati o di smagnetizzazione, prima di un eventuale riutilizzo. Qualora, anche per motivate ragioni organizzative o di budget, non sia possibile procedere immediatamente a tali operazioni, il Dirigente Scolastico può autorizzare l'accesso al dispositivo da parte di una persona fisica espressamente incaricata, interna o esterna all'Istituzione, adeguatamente istruita e vincolata alla riservatezza. L'accesso al dispositivo è in tal caso limitato alle sole informazioni strettamente necessarie per il perseguimento delle seguenti finalità:

- ripristino del sistema e riconfigurazione tecnica del dispositivo;
- recupero di informazioni di utilità istituzionale, quali, a titolo esemplificativo, materiali didattici, compiti in classe, documenti amministrativi o altri contenuti necessari alla continuità delle attività scolastiche.

Tali operazioni devono essere svolte nel rispetto dei principi di minimizzazione, proporzionalità e necessità, evitando la consultazione di dati personali non pertinenti o eccedenti rispetto alle finalità sopra indicate. Solo in presenza di un fondato e specifico sospetto di illecito, e nel rispetto dei presupposti e dei limiti individuati dalla normativa vigente e dalla giurisprudenza in materia di controlli difensivi del datore di lavoro, potrà essere autorizzato un accesso più esteso ai dati presenti sul dispositivo, esclusivamente al fine di accertare eventuali condotte illecite. Anche in tale ipotesi, il Dirigente incaricherà un soggetto specificamente designato, anche interno all'Istituzione, con il compito di

- limitare l'accesso ai soli dati pertinenti all'accertamento dell'illecito;
- epurare e non utilizzare ogni informazione superflua, non rilevante o attinente alla sfera personale del dipendente;
- garantire la tracciabilità delle operazioni effettuate e il rispetto delle misure di sicurezza previste.

In ogni caso, il trattamento dei dati personali eventualmente effettuato nell'ambito delle attività sopra descritte avviene nel rispetto della normativa in materia di protezione dei dati personali e della disciplina sui controlli a distanza dei lavoratori, assicurando adeguate garanzie a tutela dei diritti e delle libertà degli interessati.

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.

Per qualsiasi dubbio, anomalia riscontrata, rischio o violazione dei dati (anche sospetta) il lavoratore è tenuto a consultare immediatamente il dirigente scolastico o i suoi delegati.

Francesca Nardi
Dirigente scolastico