OGGETTO: Termini di conservazione e modalità di cancellazione dei dati personali da parte di Regione Umbria

Procedendo nell'adeguamento della Vostra struttura al disposto del D.Lgs. 30 giugno 2003 n. 196, intendiamo affrontare nel presente scritto il problema riguardante la disciplina relativa alla conservazione dei dati personali in formato elettronico e cartaceo, sempre dal punto di vista della disciplina in materia di protezione di tali dati, prendendo in considerazione in particolar modo le modalità concrete di cancellazione degli stessi nel caso di cessazione del trattamento. Questo allo scopo di fornirvi una panoramica quanto più ampia del problema, e permettervi dunque di affrontarlo con maggiore consapevolezza.

1. Una breve premessa: il contesto giuridico di riferimento.

Il D.Lgs. 196/2003 (come è noto, la normativa che detta le regole in materia di trattamento dei dati personali, la c.d. privacy) non disciplina nel dettaglio i termini di conservazione della documentazione che contiene le informazioni relative all'individuo in possesso del titolare (sia essa cartacea o elettronica, intendendo per tale la gestione informatica dei dati personali contenuti nei diversi tipi di "file" – di testo, immagini, e-mail, … –), né le modalità di distruzione della stessa.

1.1. *I tempi di conservazione.*

Norma generale di riferimento è quella dell'art. 11, comma 1 lett. *e*), secondo cui il titolare è tenuto a conservare i dati personali dell'interessato unicamente per il periodo necessario al perseguimento degli scopi per cui furono raccolti e trattati: raggiunti tali scopi, non è più consentito conservarli, e quindi devono essere distrutti. Distruzione che tra l'altro risulta essere una delle diciassette operazioni previste quale "trattamento" dall'art. 4, comma 1, lett. *a*) del D.Lgs. 196/2003, e che quindi deve essere posta in essere rispettando, nel suo complesso, la disciplina in materia di trattamento di dati personali.

Al di là di tale disposizione generale occorre comunque specificare che, nel caso in cui esistano normative speciali di settore che impongano la conservazione dei dati per un periodo di tempo superiore a quello strettamente necessario al perseguimento degli scopi del trattamento (ad esempio, i dieci anni previsti per gli obblighi fiscali), queste prevalgono sulla regola dell'art. 11 del D.Lgs. 196/2003. In assenza di normative di settore applicabili alla specifica situazione di utilizzo di informazioni relative all'individuo, il parametro per capire il momento in cui non può più essere ritenuto legittimo conservare i dati personali dell'interessato torna ad essere il raggiungimento dello scopo del trattamento: e questo nonostante la "scomodità" di tale regola e la sua frequente inosservanza (nonostante le severe sanzioni previste dal D.Lgs. 196).

1.2. *I modi di distruzione.*

Per ciò che riguarda poi i modi di distruzione della documentazione, in un primo momento il legislatore non ha imposto alcuna prescrizione apposita, e dunque di conseguenza la scelta circa la modalità concreta con cui effettuarla era assolutamente discrezionale per il titolare. Ma il fine dell'obbligo di distruzione stabilito nell'art. 11 era comunque preciso: evitare che, una volta cessato l'interesse del titolare (e quindi la sua attenzione e cura) alla conservazione dei dati personali (magari in seguito al raggiungimento dello scopo del trattamento), soggetti esterni potessero venire a conoscenza delle informazioni relative agli individui che fossero originariamente nel possesso di questo. In tale situazione il riferimento normativo utilizzabile per comprendere quale disciplina applicare era l'Allegato B del D.Lgs. 196/2003, in materia di misure di sicurezza nel trattamento dei dati personali, ed in particolare i suoi artt. 21 e 22.

1.3 *Il D.Lgs. 151/2005 e il Provvedimento del Garante 13 ottobre 2008*.

Successivamente una novità nel settore, anche se non direttamente collegata all'argomento in esame, è stata l'emanazione del D.Lgs. 25 luglio 2005, n. 151, attuativo di una serie di direttive (2002/95/CE, 2002/96/CE e 2003/108/CE) relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti: non ultimo perché ha portato il Garante per la protezione dei dati personali ad emanare uno specifico provvedimento proprio in materia di rifiuti di apparecchiature elettriche ed elettroniche (i cd. RAEE) e misure di sicurezza dei dati personali.

Infatti il 13 ottobre del 2008 l'Autorità ha stabilito, in tale provvedimento, che nell'attività di smaltimento, recupero e riuso dei supporti informatici prevista dal D.Lgs. 151/2005 (che comportava un rischio elevato di circolazione di componenti elettroniche usate contenenti dati personali), dovessero osservarsi con attenzione e cura gli obblighi che gravano sui titolari del trattamento relativamente alle misure di sicurezza nell'utilizzo dei dati personali: e questo sia per il titolare che "smaltisce", sia per quello che "riusa" (il quale, entrando in contatto con un apparato "rigenerato" contenente ancora dati personali del precedente proprietario, può incorrere in violazioni delle norme del D.Lgs. 196/2003).

2. Modalità di distruzione dei dati personali contenuti in documenti.

Secondo quanto previsto nel Provvedimento generale del Garante per la protezione dei dati personali del 13 ottobre 2008, è necessario distinguere la distruzione dei dati personali contenuti in documenti elettronici da quelli contenuti in documenti cartacei; e quindi, nel primo caso, distinguere ulteriormente le misure da adottare nel periodo precedente a quello di effettiva distruzione, dalle modalità da applicare proprio al momento della distruzione. In entrambe le ipotesi, le misure e gli accorgimenti possono essere attuati anche con l'ausilio di terzi tecnicamente qualificati (quali centri di assistenza, produttori e distributori di apparecchiature, che però attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle). Si tenga poi presente che se l'apparato è destinato ad essere riutilizzato, il soggetto che riusa è tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui suoi supporti di memoria, acquisendo dal precedente utente, ove possibile, l'autorizzazione a cancellarli o a renderli non più comprensibili nel caso siano ancora presenti. Vediamo nel dettaglio le differenti ipotesi.

2.1. *Documenti elettronici: misure preventive.*

Innanzitutto, l'intervento volto a garantire la sicurezza delle informazioni personali contenute in apparati elettronici destinati alla dismissione o al riuso può essere preventivo, cioè sin dal momento dell'utilizzo di tali apparecchiature nella propria struttura. Così, secondo il provvedimento del Garante, si può procedere alla 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; inoltre, tale metodologia può essere utilizzata anche nel momento della memorizzazione dei dati sui dischi rigidi

(*hard-disk*) dei *personal computer*, o su altro genere di supporto magnetico od ottico (CD-ROM, DVD-R, pen drive, …) in forma automaticamente cifrata al momento della loro scrittura, anche in questo caso tramite l'uso di parole-chiave riservate, note al solo utente. In entrambe le ipotesi senza modificare in alcun modo il comportamento e l'uso dei programmi *software* con cui i dati vengono trattati, magari grazie alla predisposizione "a monte" dei sistemi di cifratura, e quindi in modo non invasivo per l'attività dell'utente.

2.2. *Documenti elettronici: misure per la cancellazione*

Nel momento in cui si decida poi di cambiare l'utente del sistema informatico (ad esempio, si sposta il computer da un ufficio ad un altro della propria struttura), o comunque nel momento in cui si decida di dismettere l'apparato, le attenzioni da portare riguardano proprio la cancellazione dei dati sulle memorie ausiliarie, che può avvenire con diverse modalità.

Si può procedere alla 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* da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie", in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite appositi apparati elettronici di analisi e recupero di dati. Ancora, laddove effettuabile l'operazione, si può formattare "a basso livello" il dispositivo di tipo *hard disk*, attenendosi comunque alle istruzioni fornite dal produttore del dispositivo e tenendo conto (chiaramente nel caso si debba riutilizzare l'apparato) delle possibili conseguenze tecniche su di esso, che potrebbero portare alla sua successiva inutilizzabilità. Non solo, il provvedimento del Garante prevede anche la possibilità, nel caso si tratti di dispositivi non più funzionanti (ai quali potrebbero non essere applicabili le procedure di cancellazione *software* che richiedono l'accessibilità del dispositivo), di procedere alla "demagnetizzazione" 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. Infine, nel caso si debba dismettere l'apparato elettronico, l'effettiva cancellazione dei dati personali dai supporti in esso contenuti può anche risultare da procedure che, nel rispetto delle normative di settore,

comportino la distruzione fisica dei supporti di memorizzazione; questo attraverso il ricorso a metodi o strumenti diversi a secondo del loro tipo, quali ad esempio sistemi di punzonatura o deformazione meccanica, di distruzione fisica o di disintegrazione (usata per supporti quali CD-ROM, DVD o pen drive), di demagnetizzazione ad alta intensità.

2.3. *Documenti cartacei*

Più semplice, almeno a livello tecnico, la distruzione dei documenti cartacei, che può essere attuata attraverso appositi "distruggi documenti", oramai di uso comune, ma anche a prescindere da tali specifici apparecchi. La difficoltà maggiore che si incontra in questo caso dipende dall'attenzione che deve essere prestata all'operazione, vincendo abitudini e "distrazioni" del singolo incaricato del trattamento di dati personali. Dovrà essere allora cura del titolare, ed eventualmente dei responsabili, procedere ad un'opera di sensibilizzazione dei propri dipendenti, in modo da rendere la distruzione una vera e propria abitudine.

3. La conservazione e distruzione dei dati nella Regione Umbria

Analizzata l'importanza della disciplina stabilita dal D.Lgs. 196/2003 (e quindi dettagliata dal Garante per la protezione dei dati personali) con riferimento alla conservazione dei dati personali oggetto del trattamento da parte del titolare, e della loro necessaria distruzione, verifichiamo ora quanto deve essere applicato, di tale disciplina, nella vostra struttura.

Innanzitutto, in Regione Umbria, si deve ritenere che la conservazione dei dati personali dei propri dipendenti, collaboratori e fornitori segua le regole generali: tranne che per i trattamenti soggetti a specifiche discipline (come per quelle di natura fiscale, che impongono obblighi di conservazione delle informazioni, con termini anche di dieci anni), le informazioni relative agli individui dovranno essere distrutte quando è stata raggiunta la finalità per cui si era proceduto al trattamento. Per quanto invece concerne le informazioni relative alle interessate, coinvolte nel progetto antiviolenza di cui alla legge regionale 25 novembre 2016 n. 14, è opportuno sottolineare la necessità di conservare i dati delle donne (e dei minori) anche in relazione ad eventuali e futuri procedimenti giudiziari che le

possano vedere coinvolte: sul tema la Regione Umbria dovrebbe aver cura di verificare la sussistenza di normative ad hoc che indichino termini di conservazione puntuali, ovvero individuarne di propri in riferimento agli scopi perseguiti.

Per quanto riguarda le modalità concrete di adempimento di tale obbligo, richiamandosi a quanto già riportato nei precedenti paragrafi del presente scritto, si dovrà innanzitutto procedere nel richiamare l'attenzione dei propri incaricati alla necessità di rispettare le semplici regole indicate. Tralasciando gli aspetti relativi alla documentazione cartacea contenenti dati personali (la cui distruzione deve essere definitiva e tale che altri soggetti non possano venire a conoscenza del loro contenuto, risultato che può essere ottenuto anche tramite appositi strumenti, quali un semplice "distruggi documenti"), per quanto riguarda la documentazione elettronica si ritiene utile suggerirvi di procedere alla loro distruzione adottando strumenti tecnici tali da consentire una cancellazione definitiva, proprio per evitare che, anche dopo la cancellazione, soggetti esterni possano comunque recuperare tali dati. Ricordiamo, infatti, che la semplice cancellazione del file tramite il sistema operativo non corrisponde ad una cancellazione fisica del dato, ma equivale semplicemente ad un'allocazione dello spazio sul sistema di *storage* tale da poter riscrivere sopra quel determinato dato. In altre parole, il dato non viene cancellato, ma il sistema operativo si comporta come se fosse stato fisicamente rimosso. Dobbiamo aggiungere che persino la formattazione delle memorie non garantisce di non poter risalire al dato "apparentemente" eliminato. Il problema si pone in relazione al fatto che esistono appositi programmi in grado di recuperare tali file anche a distanza di parecchio tempo dalla cancellazione, programmi fra l'altro di facile reperibilità.

Consigliamo, quindi, di utilizzare appositi software che garantiscono l'effettiva rimozione fisica del file, programmi anche commerciali di non difficile acquisizione, che dunque implicano un relativo investimento per il loro uso: possiamo citare, tra i più noti, KillDrive, Ontrack Dataeraser Pro, Blanco Data Cleaner, Paragon Disk Wiper Pro e Acronis Drive Cleanser).

Ma siamo certi che tali aspetti sono già presi in considerazione, in maniera anche più precisa e competente dal punto di vista tecnico, dal vostro responsabile per la sicurezza della struttura I.T. di Regione Umbria S.r.l., anche nella sua qualità di Amministratore di Sistema.

Avv. Gianluigi Ciacci