

Jesolo Patrimonio S.r.l.

Regolamento per il riutilizzo e lo smaltimento di apparecchiature elettroniche e supporti di memorizzazione

Titolo documento:	Regolamento per il riutilizzo o lo smaltimento di apparecchiature elettroniche e supporti di memorizzazione
Codice documento:	Jesolo Patrimonio – REG Riutilizzo PC
Nome file:	Jesolo Patrimonio – REG Riutilizzo PC
Stato documento:	Prima emissione ufficiale
Versione:	1.0
Data creazione:	1 novembre 2013
Data ultimo aggiornamento	30 novembre 2013

Via Sant'Antonio, 11 – 30016 Jesolo (VE)

P. IVA 03540820275

Indice

Art. 1 - Definizioni	3
Art. 2 - Motivazione e obiettivo del presente Regolamento	7
Art. 3 - Ambito di validità e di applicazione del presente regolamento.....	9
Art. 4 - Responsabilità penale e civile	10
Art. 5 - Modalità tecniche per la gestione del riutilizzo	11
Art. 6 - Modalità tecniche per la gestione dello smaltimento.....	12
Art. 7 - Autorizzazione preliminare alla cancellazione dei dati	13
Art. 8 – Verbale di corretta esecuzione della cancellazione dei dati	14
Art. 9 – Soggetti tenuti alla verifica del presente regolamento.....	15

Art. 1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali, per brevità nel seguito chiamato anche semplicemente "Codice").

Ai sensi del 1° comma dell'art. 4 del Codice si intende per:

<p>a) "trattamento"</p>	<p>qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;</p>
<p>b) "dato personale"</p>	<p>qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;</p>
<p>c) "dati identificativi"</p>	<p>i dati personali che permettono l'identificazione diretta dell'interessato;</p>
<p>d) "dati sensibili"</p>	<p>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,</p>

	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;
f) “titolare”	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
g) “responsabile”	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
h) “incaricati”	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
i) “interessato”	la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
l) “comunicazione”	il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) “diffusione”	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n) “dato anonimo”	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
o) “blocco”	la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
p) “banca di dati”	qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
q) “Garante”	l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Ai sensi del 2° comma dell'art. 4 del Codice si intende, inoltre, per:

a) “misure minime”	il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
b) “strumenti elettronici”	gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
c) “autenticazione informatica”	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) “credenziali di autenticazione”	i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
e) “parola chiave”	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
f) “profilo autorizzazione”	l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
g) “sistema autorizzazione”	l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
h) “rischi”	Situazioni o comportamenti che possano generare un pericolo per i dati personali e/o sensibili. Per meglio valutare l'entità e le azioni da intraprendere il rischio prevede diversi livelli di soglia: basso, medio, grave o gravissimo;

Art. 2 - Motivazione e obiettivo del presente Regolamento

Il riutilizzo o lo smaltimento di apparecchiature elettroniche (es. Personal Computer, Server, palmari, tablet-PC etc.) e di supporti di memorizzazione (es. hard disk interni, hard disk esterni, cd-rom, dvd, chiavette usb, schede SD etc.) sono attività estremamente critiche dal punto di vista della sicurezza e della privacy dei dati personali, che devono pertanto essere rigidamente disciplinate.

Accade talvolta infatti che i dati del precedente utilizzatore – in alcuni casi estremamente riservati e delicati - non siano adeguatamente cancellati, e vengano pertanto portati a conoscenza di soggetti terzi non autorizzati; tra i casi più eclatanti che si sono verificati in tempi recenti possiamo evidenziare:

- il rinvenimento da parte dell'acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;
- il rinvenimento da parte dell'acquirente di un personal computer usato di decine di files e cartelle relativi alle patologie dei pazienti di una struttura sanitaria pubblica.

Obiettivo del presente regolamento è pertanto assicurare che il riutilizzo o lo smaltimento di apparecchiature elettroniche e di supporti di memorizzazione avvengano in condizioni di sicurezza, con la ragionevole certezza che i dati (personali, sensibili, giudiziari, di qualsiasi tipo) precedentemente memorizzati siano completamente cancellati con modalità tecniche che ne rendano impossibile il recupero.

E' infatti noto che la semplice operazione di cancellazione di un file o di una cartella, seguita dallo "svuotamento del cestino" (in ambiente Windows) non comporta la cancellazione fisica dei dati dal supporto di memorizzazione, che possono quindi essere recuperati con una certa semplicità.

E' pertanto necessario l'utilizzo di programmi di tipo "file wiping" o "file shredding", che comportano la riscrittura dei dati cancellati da sette a trentacinque volte, oppure



Via Sant'Antonio, 11 – 30016 Jesolo (VE)

P. IVA 03540820275

l'utilizzo di apparati che comportino la smagnetizzazione (“degaussing”) dei supporti di memorizzazione.



Via Sant'Antonio, 11 – 30016 Jesolo (VE)

P. IVA 03540820275

Art. 3 - Ambito di validità e di applicazione del presente regolamento

Le prescrizioni del presente regolamento si applicano alle seguenti apparecchiature di Jesolo Patrimonio S.r.l.:

- apparati di tipo “personal computer” fissi o portatili
- apparati di tipo tablet PC
- apparati di tipo server
- supporti di memorizzazione di massa, come ad esempio hard disk interni, hard disk esterni, cd-rom, dvd, chiavette usb, schede SD

e più in generale a qualsiasi apparato o dispositivo che possa contenere al suo interno qualsiasi tipo di dato (generico, personale, sensibile, giudiziario etc.).



Via Sant'Antonio, 11 – 30016 Jesolo (VE)

P. IVA 03540820275

Art. 4 - Responsabilità penale e civile

Dall'inosservanza delle disposizioni contenute nel presente regolamento possono derivare responsabilità di tipo:

- penale, ai sensi dell'art. 169 del Codice in materia di protezione dei dati personali, oppure
- civile, in caso di danni cagionati a terzi, ai sensi dell'art. 15 del Codice in materia di protezione dei dati personali e dell'art. 2050 del Codice Civile.



Via Sant'Antonio, 11 – 30016 Jesolo (VE)

P. IVA 03540820275

Art. 5 - Modalità tecniche per la gestione del riutilizzo

In caso di riutilizzo di apparecchiature elettroniche o di supporti di memorizzazione, si dovranno utilizzare appositi programmi di “file wiping” o di “file shredding” che forniscano idonee garanzie di non recuperabilità dei dati cancellati, nemmeno con le apparecchiature più sofisticate.

Sul mercato esistono varie soluzioni software, alcune delle quali di pubblico dominio. Allo stato attuale della tecnologia i programmi di file wiping più affidabili sono i seguenti:

- **Sdelete**, scaricabile dal sito www.microsoft.com, che è l'utility suggerita dalla Microsoft per tutti i sistemi Windows. Tale utility è conforme ai requisiti dello standard del DOD – Department Of Defense 5220.22-M, e fornisce idonee garanzie che i dati saranno cancellati in modo da renderne tecnicamente impossibile il recupero;
- **Ashampoo File Wiper**, scaricabile dal sito internet www.ashampoo.it, una tra le utility più diffuse ed affidabili allo stato attuale della tecnologia.

Art. 6 - Modalità tecniche per la gestione dello smaltimento

Per lo smaltimento degli apparati e dei supporti di memorizzazione, si dovrà distinguere tra il caso in cui il dispositivo sia ancora funzionante, dai casi in cui il dispositivo non sia funzionante.

Nel primo caso si potranno applicare le modalità tecniche previste per il riutilizzo; nel secondo caso, e cioè nel caso in cui il dispositivo non sia funzionante si dovranno adottare le seguenti tecniche:

- **Demagnetizzazione:** la demagnetizzazione (“degaussing”) permette l’“azzeramento” delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti che fanno parte del dispositivo e causandone l’inutilizzabilità successiva.
- **Distruzione fisica:** In determinati casi è necessario ricorrere alla distruzione fisica dei dispositivi di memoria. Tale procedura è l'unica praticabile con i supporti ottici a sola lettura (CD-ROM, DVD-R), che possono essere distrutti o polverizzati con appositi macchine analoghe ai "tritacarta" in uso negli uffici. Gli hard-disk possono essere resi inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superfici magnetiche (piatti) con l'azione deformante di uno strumento o con appositi punzonatori.



Via Sant'Antonio, 11 – 30016 Jesolo (VE)

P. IVA 03540820275

Art. 7 - Autorizzazione preliminare alla cancellazione dei dati

Poiché i dati (personali, sensibili, giudiziari etc.) contenuti negli apparati e nei supporti di memorizzazione costituiscono un prezioso patrimonio aziendale, e tenuto conto del fatto che in alcuni casi vi possono essere obblighi specifici di conservazione dei dati per un periodo minimo, prima di procedere alla cancellazione dei dati, chiunque sia il soggetto che materialmente effettua la cancellazione, dovrà chiedere ed ottenere in forma scritta l'autorizzazione alla cancellazione dei dati.

Detta autorizzazione dovrà essere rilasciata in forma scritta da un Responsabile del trattamento dei dati oppure dal Titolare. Detta autorizzazione potrà se del caso contenere indicazioni sui dati che prima di essere cancellati devono essere oggetto di salvataggio.



Via Sant'Antonio, 11 – 30016 Jesolo (VE)

P. IVA 03540820275

Art. 8 – Verbale di corretta esecuzione della cancellazione dei dati

Alla fine delle attività di cancellazione, il soggetto che ha materialmente effettuato le operazioni dovrà compilare apposito verbale nel quale dichiara di aver personalmente effettuato la cancellazione in forma permanente dei dati e il buon esito delle operazioni effettuate.

Il suddetto verbale dovrà inoltre contenere i riferimenti (es. marca, modello, numero di serie etc.) dell'apparato o del supporto oggetto del trattamento.



Via Sant'Antonio, 11 – 30016 Jesolo (VE)

P. IVA 03540820275

Art. 9 – Soggetti tenuti alla verifica del presente regolamento

La responsabilità di vigilare sulla corretta applicazione del presente Regolamento è affidata al Direttore Tecnico P.A. Igor Buosi, che potrà avvalersi della collaborazione di personale qualificato appositamente incaricato.