REG PRY 00

Gestione degli adempimenti ai sensi del D.Lgs 196/2003 Gruppo Veritas

Conforme al D.Lgs 196/2003
Conforme alla Norma UNI EN ISO 9001:2008
Componente del modello Organizzativo ex D. Lgs 231/01

INDICE

Preparazione	Verifica	Approvazione
Resp. Gestione Dati Personali Privacy *M. Simionato* *(FIRMATO)*	**Dir. Qualità Ambiente Patrimonio Servizi per l'Utenza e Bollettazione di Gruppo** *M. Calligaro* *(FIRMATO)* **Dir. Risorse Umane e Organizzazione di Gruppo** *C. Bellon* *(FIRMATO)*	**Direttore Generale** *A. Razzini* *(FIRMATO)* **APPROVATO nel CdA del: 09.09.2016**

Variazioni: modifiche normative ed organizzative

1 SCOPO

Il decreto legislativo n. 196 del 30 giugno 2003, stabilisce i principi generali in materia di protezione dei dati personali.

Il presente regolamento definisce le modalità di gestione dei dati personali in ambito aziendale allo scopo di:

- garantire che il trattamento dei dati personali detenuti da VERITAS S.p.A. si svolga nel rispetto dei diritti di riservatezza e protezione degli stessi ed in osservanza dei principi di proporzionalità, necessità, finalità e correttezza;
- stabilire modalità, termini e condizioni di gestione in osservanza di quanto sopra definito;
- garantire, ai fini della protezione dei dati personali detenuti da VERITAS S.p.A., che gli accessi ai sistemi informatici e agli archivi cartacei siano strutturati per assicurare un adeguato livello di riservatezza, conservazione, esattezza, correttezza, completezza, pertinenza e rintracciabilità delle informazioni ivi contenute.

2 CAMPO DI APPLICAZIONE

Il presente regolamento si applica a Veritas Spa e, per quanto compatibile, a tutte le aziende del Gruppo VERITAS ed a tutte le attività che contemplano il trattamento di dati personali, comprese le attività affidate a terzi (attività affidate in outsourcing).

Veritas SpA e le società del gruppo Veritas, debbono adottare il presente Regolamento attraverso una specifica deliberazione a cura dell'organo competente.

3 RESPONSABILITÀ

La tabella seguente descrive le attività e le responsabilità:

Attività	Referente
Titolare dei dati personali e delle modalità di trattamento	Direttore Generale/AD della società
Responsabili dei dati personali	Dirigenti aree/Responsabili
Incaricati al trattamento	Addetti incaricati presso le specifiche aree
Amministratore di sistema (vedi profili di incarico)	Responsabile e Addetti Sistemi Informativi
Analisi misure di sicurezza, elaborazione Documento Programmatico sulla Sicurezza	Ufficio Gestione Dati Personali Privacy VERITAS
Definizione informative trattamento dati	Ufficio Gestione Dati Personali Privacy VERITAS
Definizione lettere d'incarico al trattamento dati (interne ed esterne all'azienda)	Ufficio Gestione Dati Personali Privacy VERITAS
Audit di controllo sull'osservanza in azienda delle disposizioni impartite nel D.Lgs 196/2003 e dalle procedure aziendali in materia	Addetto Qualità e Ambiente VERITAS
Responsabile del trattamento e archiviazione registrazioni provenienti dagli audit di controllo	Addetto Qualità e Ambiente VERITAS
Gestione dell'attività formativa *"autoformazione"* e della formazione in aula	Ufficio Gestione Dati Personali Privacy di concerto con Risorse Umane
Formazione stagisti, cambi mansione e nuovi assunti	Addetto Qualità e Ambiente di concerto

	con Ufficio Gestione Dati Personali Privacy VERITAS
Gestione informazioni/trasmissioni dati al Garante	Direttore Affari Legali e Societari di Gruppo/ Affari Legali della Società
Tenuta sotto controllo e aggiornamento delle informative (anche cartellonistica) relative alla Privacy	Ufficio Gestione Dati Personali Privacy VERITAS

4 DEFINIZIONI

Di seguito si precisa il significato delle principali definizioni tecniche utilizzate nel presente Regolamento (*D.lgs 196/2003 Art. 4 e provvedimento del Garante del 27.11.2008)*:

Garante: l'autorità in materia che viene eletta dalle camere (*D.lgs 196/2003 Art. 153*); si tratta di un organo collegiale che opera in piena autonomia e con indipendenza di giudizio e di valutazione;

trattamento: qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti le 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;

dato personale: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati od identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato;

dati sensibili: i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale;

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;

dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

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;

responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali;

incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

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;

diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

sistema di autorizzazioni: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo del richiedente.

estremi identificativi Amministratore di Sistema: si tratta del minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza. In molti casi possono coincidere con nome, cognome, funzione o area organizzativa di appartenenza.

5 REGOLE PER IL TRATTAMENTO DEI DATI

5.1 Modalità di trattamento e requisiti dei dati

Le operazioni di trattamento possono essere effettuate solo da incaricati che operino sotto la diretta autorità del Titolare o Responsabile del dato. Gli incaricati devono attenersi scrupolosamente alle procedure in materia impartite dalle Società del Gruppo VERITAS. Tali procedure, definite in ottemperanza al D.Lgs 196/2003, vengono trasmesse agli incaricati attraverso specifica attività formativa in materia e, qualora necessario, con ulteriori eventuali comunicazioni scritte, (ad esempio il presente Regolamento, la pubblicazione *Privacy Guida ad uso dei dipendenti, Regolamento Informatico aziendale,* specifiche comunicazioni aziendali, ecc …).

Si sottolinea che **gli incaricati sono da considerarsi tali qualora la loro designazione sia stata fatta per iscritto dal Titolare o dal Responsabile del dato oggetto di trattamento, e, solo qualora sia stato altresì designato l'ambito del trattamento loro consentito** (D.Lgs 196/2003, Art. 30).

I dati personali oggetto di trattamento devono rispettare i seguenti requisiti di legge:

- essere trattati in modo lecito e secondo correttezza;
- essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- essere esatti e, se necessario, aggiornati;
- essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o vengono trattati;
- essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati non trattati secondo queste modalità e non aventi tali requisiti non possono essere utilizzati.

5.2 Informativa sulla privacy all'interessato e consenso al trattamento dati

Le operazioni di raccolta dati personali devono sempre essere svolte dopo aver dato informazione scritta od orale all'interessato circa (D.Lgs 196/2003 Art. 13):

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti dell'interessato (di cui all'*art. 7* del codice in materia di trattamento dati personali e al *Capitolo 7* della presente procedura);
- gli estremi identificativi del titolare e se designato del responsabile e le modalità attraverso le quali identificare e rintracciare i nominativi aggiornati dei responsabili per VERITAS S.p.A.

Qualora i dati personali non fossero raccolti in presenza dell'interessato, l'Informativa gli dovrà essere obbligatoriamente consegnata all'atto della registrazione dei dati stessi o trasmessa con la prima comunicazione utile.

Il trattamento dati personali da parte delle Società del Gruppo VERITAS è possibile solo con il consenso espresso da parte dell'interessato, (*D.Lgs 196/2003 Art. 23*) fatti salvi i casi espressamente previsti dalla legge.

Affinché il consenso abbia validità:

- deve essere riferito ad uno specifico trattamento chiaramente individuato e deve essere documentato per iscritto;
- deve essere stata comunicata all'interessato la relativa Informativa al trattamento;

- in caso di trattamento dati sensibili deve essere stato raccolto in forma scritta.

L'introduzione nel sistema di gestione di nuove informative sulla privacy, o modifiche alle informative esistenti, deve sempre essere concordata con l'ufficio Gestione Dati Personali Privacy di Gruppo.

5.3 Comunicazione e diffusione dei dati personali

Il codice in materia di trattamento dati personali vieta la comunicazione e la diffusione di dati personali per i quali è stata ordinata la cancellazione o per i quali è trascorso il periodo di tempo di conservazione necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. Inoltre non possono essere comunicati e diffusi dati per finalità differenti da quelle indicate nell'Informativa di trattamento.

Sono escluse dai divieti sopra citati le richieste fatte alle Società del Gruppo VERITAS, purché siano conformi alla legge, da forze di polizia, autorità giudiziaria, organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa, sicurezza dello Stato, prevenzione, accertamento o repressione di reati.

5.4 Trattamento dati sensibili

I dati sensibili possono essere oggetto di trattamento solo con il **consenso scritto dell'interessato** (*D.Lgs 196/2003, Art. 23 - 4*), e previa autorizzazione del Garante. Devono essere trattati nell'osservanza dei presupposti e dei limiti stabiliti dal codice in materia di trattamento dati personali e della legge (*D.Lgs 196/2003, Art. 26*) e **non possono essere diffusi**.

Qualora sia necessario **per la gestione del rapporto di lavoro**, (anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza), adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria, tali dati possono essere oggetto di trattamento senza il consenso scritto da parte dell'interessato, in tal caso previa autorizzazione da parte del Garante (*D.Lgs 196/2003, Art. 26, 4-d*)

I **dati sensibili** trattati dalle Società del Gruppo VERITAS sono:

- i dati idonei a rilevare lo stato di salute dei dipendenti trattati dall'area Servizio di Sorveglianza Sanitaria: tali dati non possono essere diffusi (*D.Lgs 196/2003, Art. 26, 5*);
- i dati inerenti le adesioni politiche e sindacali dei dipendenti trattati presso l'area Risorse Umane e Organizzazione di Gruppo;

5.5 Trattamento dati giudiziari

Il trattamento di dati giudiziari può avvenire soltanto se autorizzato da disposizione di legge o da un provvedimento del Garante. Le disposizioni o provvedimenti in materia devono specificare, (*D.Lgs 196/2003, Art. 27*):

- le rilevanti finalità di interesse pubblico del trattamento;
- i tipi di dati trattati;
- la tipologia di operazioni eseguibili.

I **dati giudiziari** trattati dalle Società del Gruppo VERITAS sono:

- i dati giudiziari di dipendenti, fornitori, esterni, aziende, società controllate, trattati presso le aree Affari legali e Societari e Approvvigionamenti;
- I dati giudiziari raccolti in occasione di avvisi di selezione esterna e relativi ai partecipanti alla selezione (ex art. 17 Regolamento in materia di reclutamento del personale) trattati e detenuti presso la Direzione Risorse Umane e Organizzazione di Gruppo.

5.6 Soggetti che effettuano il trattamento

In materia di trattamento dati personali il *D.Lgs 196/2003* individua tre figure che operano con funzioni differenti nella gestione del dato:

- **titolare del trattamento**, (*D.Lgs 196/2003, Art. 28*) che con autonomia di potere decisionale esercita sulle finalità e sulle modalità del trattamento, compreso quanto concerne l'ambito della sicurezza. Il titolare ha facoltà di designare per iscritto eventuali responsabili di trattamento. Attraverso verifiche periodiche il titolare vigila sull'osservanza in azienda delle disposizioni impartite nel D.Lgs 196/2003 e dalle procedure aziendali in materia, (D.Lgs 196/2003, Art. 29 e Capitolo 5 della presente procedura)
- **responsabile del trattamento**, (*D.Lgs 196/2003, Art. 29*) che, nell'ambito dei compiti affidatigli analiticamente e per iscritto direttamente dal titolare, deve garantire il rispetto delle disposizioni vigenti in materia di trattamento dati, anche sotto il profilo della sicurezza. Per esigenze organizzative possono essere designati più responsabili di trattamento, anche mediante specifica suddivisione dei compiti. Il responsabile, nell'esercitare i suoi compiti, deve attenersi alle istruzioni impartite dal titolare;
- **incaricati del trattamento**, (*D.Lgs 196/2003, Art. 30*) che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni da loro impartite (attività formativa, comunicazioni aziendali, procedure, ecc…). La

designazione degli incaricati e dell'ambito di trattamento loro consentito viene effettuata dal titolare o dal responsabile **per iscritto.**

Qualora siano affidate in **outsourcing** attività di trattamento dati personali svolte in autonomia**, i soggetti esterni interessati al trattamento dati devono essere individuati dal referente aziendale del contratto, in fase di definizione dello stesso**. Le lettere d'incarico a tali soggetti vengono predisposte dall'Ufficio Gestione Dati Personali Privacy di VERITAS S.p.A., sottoscritte dai soggetti terzi individuati, ed inserite nella documentazione di affidamento. Per la gestione di tale attività è fondamentale il supporto della Direzione Energia e Approvvigionamento di Gruppo e degli uffici Approvvigionamento delle società del Gruppo VERITAS, in particolare dell'area Approvvigionamenti Beni e Servizi, che trasmetterà all'Ufficio Gestione Dati Personali Privacy tutte le informazione utili alla predisposizione della lettera di nomina a Responsabile Esterno di Trattamento Dati (riferimenti societari ditta aggiudicatrice, oggetto dell'appalto, codice gara, codice CIG, data scadenza contratto, ecc.), nonché copia del documento di nomina firmato/perfezionato dal soggetto aggiudicatario.

5.7 Gestione documenti inerenti la privacy

Di norma i documenti, gli atti e le informative relativi alla privacy vengono predisposti, di concerto con gli uffici richiedenti, dall'Ufficio Gestione Dati Personali Privacy che ne cura anche l'archiviazione.

Nell'eventualità che, per motivi di urgenza o di altra natura, debbano essere prodotti documenti inerenti la privacy da parte dei diversi uffici aziendali delle Società del Gruppo VERITAS, quali ad esempio informative ex art.13 D.Lgs 196/2003, lettere di nomina ad incaricati o a responsabili esterni ex art.29 e 30 del D.Lgs 196/2003, ecc…, copia di detta documentazione prodotta sarà trasmessa all'Ufficio Gestione Dati Personali Privacy per opportuna conoscenza, verifica ed archiviazione aziendale.

La modulistica inerente la privacy è disponibile sul portale aziendale Il Milione, nella sezione Sistema di Gestione.

5.8 Misure di sicurezza

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in base alle conoscenze acquisite, al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo i rischi di distruzione e perdita dei dati stessi. Deve inoltre essere ridotto al minimo il rischio di accesso non autorizzato ai dati, e

le possibilità di trattamento non consentito o non conforme alle finalità per cui le informazioni sono state raccolte, *(D.Lgs 196/2003, Art. 31)*

5.8.1 Misure di sicurezza nei trattamenti con strumenti elettronici

Il trattamento di dati personali attraverso l'utilizzo di strumenti elettronici è consentito solo qualora siano adottate le seguenti misure minime di sicurezza (D.Lgs 196/2003, Art. 34 e Disciplinare Tecnico B):

- **Autenticazione informatica:** gli incaricati devono essere dotati di credenziali di autenticazione personali che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali ed i dispositivi di autenticazione devono inoltre essere ed uso esclusivo dell'incaricato. Gli aspetti tecnici e di gestione dei sistemi relativi all'autenticazione informatica sono a cura dell'Amministratore di Sistema.
- **Adozione di procedure di gestione delle credenziali di autenticazione**: gli incaricati devono assicurare la segretezza della componente riservata delle credenziali di autenticazione e la diligente custodia dei dispositivi in loro possesso. È responsabilità del titolare/responsabile di formare gli incaricati sulla corretta custodia di credenziali e dispositivi.
- **Utilizzazione di un sistema di autorizzazione:** La parola chiave, quando prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere modificata da quest'ultimo al primo utilizzo dello strumento e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi
- Qualora sia utilizzato un codice per l'identificazione esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.
  Gli aspetti tecnici per la gestione del sistema di autenticazione, (ad es. composizione e lunghezza della password, rinnovo password a cadenza predeterminata), sono a cura dell'Amministratore di Sistema.
- **Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici**: eventuali credenziali di

autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali devono essere disattivate anche in caso di perdita della qualità delle stesse.

La rintracciabilità delle informazioni necessarie all'Amministratore di Sistema per garantire tali aggiornamenti è data dalle comunicazioni inerenti tale materia provenienti dall'area Organizzazione e Risorse Umane.

- **Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici**: gli incaricati non devono lasciare incustodito e accessibile gli strumenti elettronici loro affidati durante una sessione di trattamento. Contro il rischio di intrusione sono attivi e continuativamente aggiornati idonei strumenti di protezione dei dati gestiti direttamente dall'area Infrastrutture Tecnologiche (Amministratore di Sistema). La cadenza massima prevista nel Disciplinare Tecnico B di aggiornamento di tali sistemi è semestrale.

  Gli aspetti tecnici e di gestione dei sistemi relativi protezione informatica dei dati sono a cura dell'Amministratore di Sistema.

- **Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi:** per tali procedure si rimanda ai sistemi in uso (compresi gli eventuali affidamenti a ditte specializzate) adottati dall'area Sistemi informativi – Infrastrutture Tecnologiche.

  Gli aspetti tecnici e di gestione relativi all'adozione di procedure per la custodia di copie di sicurezza, ripristino dati e sistemi informatici sono a cura dell'Amministratore di Sistema.

- **Tenuta di un aggiornato documento programmatico sulla sicurezza (DPS):** il documento programmatico sulla sicurezza viene aggiornato annualmente secondo quanto previsto dal D.Lgs 196/2003 attraverso un'attività di raccolta di dati relativi ai trattamenti svolti in azienda eseguita su schede specifiche per ogni incaricato.

  La raccolta e l'elaborazione dei dati utilizzati per l'aggiornamento del DPS sono a cura dell'Ufficio Gestione Dati Personali – Privacy.

- **Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.**

Gli aspetti tecnici e di gestione relativi alla gestione dei dati sensibili riguardanti lo stato di salute dei dipendenti sono a cura del Responsabile dell'area Sorveglianza Sanitaria con il supporto tecnico dell'Amministratore di Sistema per la scelta dei sistemi informatici.

Nel caso di dati trattati dalle Società del Gruppo VERITAS si utilizza un sistema informatico separato.

Qualora siano adottate misure minime di sicurezza avvalendosi di soggetti esterni alle Società del Gruppo VERITAS, l'installatore deve rilasciare all'azienda una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del Disciplinare Tecnico B. Copia del documento deve essere trasmessa anche all'Ufficio Gestione Dati Personali – Privacy.

5.8.2 Ulteriori misure di sicurezza nei trattamenti di dati sensibili o giudiziari con strumenti elettronici

Dovendo i dati sensibili o giudiziari essere protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici, le Società del Gruppo VERITAS hanno adottato le seguenti misure di sicurezza:

- Gli incaricati sono informati (corso di auto formazione on-line e distribuzione della presente procedura) che la custodia e l'uso dei supporti rimovibili su cui sono memorizzati dati sensibili o giudiziari deve essere fatta al fine di evitare accessi non autorizzati e trattamenti non consentiti.
- I supporti rimovibili contenenti dati sensibili o giudiziari, qualora non più utilizzati, sono distrutti o resi inutilizzabili a cura dell'Amministratore di Sistema. Tali supporti vengono dati in utilizzo ad altri incaricati solo dopo aver reso inutilizzabili le informazioni in essi precedentemente contenute.
- Sono state adottate in azienda idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici che li contengono. Tali misure prevedono tempi compatibili con quanto previsto dal D.Lgs 196/2003 e provvedimenti successivi (sette giorni);
- Il trattamento dei dati idonei a rivelare lo stato di salute dei dipendenti viene gestito in una banca dati secondo le modalità di cui all'art 22 del codice in materia di trattamento dati personali, consentendo quindi il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati.

5.8.3 Misure di sicurezza nei trattamenti senza l'ausilio di strumenti elettronici

Il trattamento di dati personali senza l'ausilio di strumenti elettronici è consentito solo qualora siano adottate le seguenti misure minime di sicurezza (D.Lgs 196/2003, Art. 35 e Disciplinare Tecnico B):

Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative: gli ambiti di trattamento consentiti ai singoli incaricati vengono aggiornati con cadenza almeno annuale. La lista degli incaricati è redatta per dipendente e relativa specifica autorizzazione al trattamento. ***La raccolta e l'elaborazione di tali informazioni, utilizzate anche per l'aggiornamento del DPS annuale, sono a cura dell'Ufficio Gestione Dati Personali – Privacy. È cura invece del titolare/responsabile di area d'individuare e trasmettere a tale funzione le informazioni relative ai trattamenti svolti nell'area di loro competenza.***

- **Adozione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti:** gli incaricati sono informati (corso di auto formazione on-line e distribuzione della presente procedura) circa le modalità di controllo e custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento (vedi paragrafo 4.7.2 "Gestione di documenti e atti contenenti dati personali, sensibili o giudiziari").

  È responsabilità del titolare/responsabile di formare gli incaricati sulla corretta custodia documentale.

- **Adozione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati:** gli archivi aziendali che richiedono accesso selezionato sono quelli presenti negli uffici del Servizio di Sorveglianza Sanitaria dove sono state adottate idonee misure di custodia e controllo degli accessi come la chiusura a chiave delle stanze e degli armadi e l'utilizzo delle chiavi di accesso in carico esclusivamente al Responsabile e al suo incaricato.

5.9 Gestione di documenti e atti contenenti dati personali, sensibili o giudiziari

I documenti cartacei trattanti dati personali, sensibili o giudiziari non devono essere lasciati incustoditi o trasportati al di fuori delle sedi aziendali senza autorizzazione del titolare o

responsabile del trattamento. Particolare attenzione va posta inoltre nel caso in cui tali dati siano in unica copia.

Per il trattamento di atti e documenti contenenti dati sensibili o giudiziari è necessario che i medesimi siano controllati e custoditi dagli incaricati sino al termine delle operazioni per le quali sono stati loro affidati, in maniera tale che ad essi non possano accedere persone prive di autorizzazione.

L'archiviazione di tali documenti deve essere effettuata:

- con sistematicità alla fine delle operazioni per cui sono stati trattati i dati;
- con un metodo che ne renda possibile una veloce rintracciabilità, anche al fine di poter garantire i diritti dell'interessato;
- in luoghi sicuri e adeguati al grado di riservatezza dei dati trattati, (ad esempio in armadi e cassetti chiusi a chiave). L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato.

Per quanto riguarda il trattamenti di atti e documenti contenenti dati sensibili o giudiziari è necessario che i medesimi siano controllati e custoditi dagli incaricati sino al termine delle operazioni per le quali sono stati loro affidati, in maniera tale che ad essi non possano accedere persone prive di autorizzazione.

5.10 Gestione delle emergenze

Nel caso in cui si verifichino perdite, diffusioni non consentite o accessi non autorizzati di dati personali l'incaricato al trattamento dovrà immediatamente informare per iscritto il Responsabile dell'attività, che provvederà a predisporre le necessarie azioni correttive al ripristino dei livelli minimi di sicurezza previsti, quantificare l'eventuale perdita o diffusione di dati, predisporre eventuali azioni preventive ed informare il Titolare dei dati e l'Ufficio Gestione Dati Personali Privacy di Gruppo.

5.11 Amministratore di Sistema (D.Lgs 196/2003, provvedimento del 27.11.2008)

Per Amministratore di Sistema si intende quella figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza qualora questi consentano di intervenire su dati personali. Si tratta pertanto di operatori dotati di specifici privilegi informatici, che nello svolgimento delle loro consuete attività possono essere concretamente "responsabili" di specifiche fasi lavorative, le quali possono comportare elevate criticità rispetto alla protezione dei dati personali. Tali attività vanno considerate come trattamento di dati personali, anche se le informazioni accessibili non sono consultabili "in chiaro".

Non sono considerati invece Amministratori di Sistema tutti quei soggetti che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software, ad esempio per scopi di manutenzione a seguito di guasti o malfunzioni.

Le misure di sicurezza e gli accorgimenti adottati dalle Società del Gruppo VERITAS relativamente alla definizione e alle funzioni assegnate alla figura in oggetto sono le seguenti:

- la funzione di Amministratore di Sistema è attribuita, a seguito di valutazione fatta dall'area Risorse Umane e Organizzazione, a personale qualificato in grado di garantire il rispetto delle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza. Tale designazione è individuale e riporta l'elenco analitico degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato (vedi Profili Professionali);
- **a**ll'atto della designazione di un amministratore di sistema viene fatta un'elencazione analitica degli ambiti di operatività ad esso consentiti in base al profilo di autorizzazione assegnato. La descrizione degli ambiti operativi è puntuale, analogamente a quanto previsto al comma 4 dell'art. 29 del Codice riguardante i responsabili del trattamento;
- nel Documento Programmatico sulla Sicurezza sono riportati gli estremi identificativi aggiornati degli Amministratori di Sistema incaricati;
- da parte degli Amministratori di Sistema sono stati adottati sistemi di autenticazione informatica ai sistemi di elaborazione e agli archivi elettronici (registrazione degli accessi logici). Tali tipi di registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e vengono conservate per un periodo non inferiore a sei mesi;
- per i servizi di Amministratori di Sistema affidati in outsourcing il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Tali misure di sicurezza e accorgimenti sono stati adottati in riferimento a quanto definito dal *provvedimento del 27.11.2008.*

5.12 Videosorveglianza

Nella installazione e gestione di impianti di Videosorveglianza presso le sedi dell'azienda devono essere osservate le indicazioni del Garante Privacy, di cui al provvedimento in materia di Videosorveglianza del 08.04.2010, e quando previsto negli accordi sindacali sulla Videosorveglianza.

In merito ai sistemi di videosorveglianza, per ottemperare alle disposizioni in termini di privacy, sono attualmente previste le seguenti condizioni:

- stipula di apposito accordo sindacale con le OO.SS. dei CCNL applicati in Azienda ex art. 4 L. 300/70 ovvero presentazione istanza all'Ispettorato del lavoro competente;
- i dati raccolti devono rispettare il principio di pertinenza e di non eccedenza, cioè vengono registrate solo le immagini strettamente necessarie a perseguire gli obiettivi di tutela della sicurezza e dell'incolumità del patrimonio e delle persone;
- l'accesso alle registrazioni è previsto solo per il Responsabile del trattamento dei dati nominato dalla Direzione;
- la visualizzazione delle registrazioni avviene solo ed esclusivamente per verificare fatti anomali inerenti la sicurezza;
- il trattamento dei dati avviene secondo correttezza e solo per ragioni di sicurezza e tutela del patrimonio e incolumità delle persone (le immagini non possono essere utilizzate per finalità differenti).
- in caso di registrazione, il periodo di conservazione delle immagini deve essere limitato al massimo a 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini.
- di ogni nuova installazione e/o modifica di sistemi di videosorveglianza deve essere data tempestiva comunicazione all'ufficio Gestione Dati Personali – Privacy.
- i sistemi di videosorveglianza installati in azienda devono essere segnalati da uno specifico cartello informativo, sulla base del modello elaborato dal Garante Privacy, posto in prossimità di ogni singola telecamera.

- si definisce che, per ogni sistema di videosorveglianza, il responsabile del trattamento dati è il dirigente cui si riferisce il sito nel quale sono installate le telecamere; mentre gli incaricati del trattamento dati sono: il responsabile del sito o comunque il primo riporto del dirigente in quel sito, per la parte accesso ai locali in cui materialmente si trovano conservati i dati, e il Responsabile Sistemi IT, o chi per lui, per la parte relativa all'estrazione dei dati ed alla loro messa a disposizione per le diverse esigenze.

5.13 Geo - localizzazione

Nell'installazione e gestione di impianti di geo - localizzazione su mezzi e/o dispositivi aziendali, devono essere osservate le indicazioni del Garante Privacy, di cui al provvedimento in materia di geo - localizzazione del 04.10.2011.

In merito ai sistemi di geo - localizzazione, per ottemperare alle disposizioni in termini di privacy, sono attualmente previste le seguenti condizioni:

- stipula di apposito accordo sindacale con le OO.SS. dei CCNL applicati in Azienda ex art. 4 L. 300/70, ovvero presentazione istanza all'Ispettorato del lavoro competente.
- nomina del Responsabile del Trattamento dati ed eventuale nomina di Responsabile Esterno del trattamento dati se il sistema di rilevazione dati è gestito presso terzi;
- ricognizione e nomina degli incaricati abilitati a collegarsi e ad operare sul sistema;
- i dati raccolti devono rispettare il principio di pertinenza e di non eccedenza, pertanto la posizione dei mezzi o dei dispositivi NON deve venire monitorata continuamente;
- definizione di tempi di conservazione dei dati trattati (indicativamente non superiore a 180 giorni);
- ogni nuova installazione e/o modifica di sistemi di geo - localizzazione deve essere tempestivamente comunicata all'ufficio Gestione Dati Personali – Privacy;
- dev'essere predisposta idonea Informativa estesa per i dipendenti
- si dovranno anche collocare all'interno dei veicoli vetrofanie recanti la dizione "VEICOLO SOTTOPOSTO A LOCALIZZAZIONE" o comunque avvisi ben visibili che segnalino la circostanza della geo - localizzazione del veicolo, anche avvalendosi del seguente modello elaborato dal garante Privacy.

5.14 Centri di Raccolta

Nella conduzione dei centri di raccolta devono essere osservate le regole per il corretto trattamento dei dati personali così come previsto dalla "Informativa sul trattamento dei dati personali acquisiti con conferimento di materiali nei centri di raccolta", (**M PRY AZ 03**). Tale informativa è appesa presso tutti i Centri di Raccolta.

Per quanto attiene all'accettazione dei rifiuti di apparecchiature elettriche ed elettroniche (RAEE) dovrà essere compilato il modulo **M ECO 09** "Conferimento di particolari tipologie di RAEE". Per il conferimento presso i Centri di Raccolta di materiale derivante da piccoli lavori di manutenzione e ristrutturazione domestica, è invece prevista la compilazione del modulo **M ECO 08.**

6 CONTROLLO E AUDIT

Le misure di sicurezza, organizzative, fisiche e logiche da adottare per il trattamento dei dati personali sono delineate ai sensi e per gli effetti *dell'articolo 34, comma 1, del D.Lgs 196/2003* nel Documento Programmatico sulla Sicurezza redatto con cadenza annuale. Tale documento viene aggiornato annualmente e riguarda tutte le attività gestite dalle Società del Gruppo VERITAS concernenti tale materia, comprese quelle affidate a fornitori esterni.

L'area Qualità e Ambiente effettua audit di controllo atti a verificare l'effettiva adozione e applicazione delle misure di sicurezza previste e del complesso di operazioni concernenti il trattamento dei dati personali. I punti di controllo delle verifiche sono definiti e aggiornati in ottemperanza a quanto previsto dal D.Lgs 196/2003 e relativi provvedimenti, qualora essi siano applicabili alla realtà aziendale.

Con cadenza semestrale l'area Qualità e Ambiente inoltre effettua, verifiche circa **l'operato degli Amministratori di Sistema** secondo quanto previsto dal *provvedimento del 27.11.2008* (punto 4.4 *Verifica delle attività*).

Obbiettivo di questi audit è:

- verificare che l'Amministratore di Sistema svolga le sua attività nell'esercizio delle sue funzioni;
- verificare che l'Amministratore di Sistema svolga le sua attività conformemente alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.

Le risultanza degli audit, oltre che ai referenti dell'area verificata, vengono trasmesse anche all'Ufficio Gestione Dati Personali Privacy che le utilizza per aggiornare lo stato delle informazioni in materia in suo possesso.

7 DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

A seguito dell'approvazione del d.l. 9 febbraio 2012, n. 5 - convertito, con modificazioni, nella legge 4 aprile 2012, n. 35 (pubblicata sulla Gazzetta Ufficiale del 6 aprile 2012, n. 82) - è venuto meno l'obbligo di redigere e aggiornare il Documento Programmatico per la Sicurezza dei dati personali (DPS).

Verificato, però, che tutte le altre norme sulla sicurezza dei dati personali, previste dal D.Lgs. 196/2003, sono rimaste in vigore e considerato anche l'obbligo di provvedere all'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati (art.li 34 e 35 del Codice Privacy), l'azienda ritiene opportuno continuare a predisporre un documento annuale di verifica ed aggiornamento della propria situazione rispetto alla sicurezza dei dati personali e agli adempimenti privacy.

In particolare, entro il 31 Marzo di ogni anno, l'Azienda predisporrà il Documento di Aggiornamento degli Adempimenti Privacy, basato sullo schema del precedente DPS.

Il Documento Programmatico sulla Sicurezza dev'essere predisposto ed approvato dal C.d.A. delle Società del Gruppo VERITAS entro il 31 marzo di ogni anno. Per la redazione di tale documento il Titolare dei dati delle Società del Gruppo VERITAS ha nominato un responsabile aziendale che si occupa di raccogliere tutte le informazioni idonee alla compilazione del documento in oggetto.

Tale responsabile aziendale risulta, attualmente, in capo all'Ufficio Gestione Dati Personali – Privacy.

Nello specifico il Documento Programmatico sulla Sicurezza riporta (*Disciplinare Tecnico B del D.Lgs 196/2003*):

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

- l'analisi dei rischi che gravano sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno.

L'Ufficio Gestione Dati Personali Privacy, incaricato per l'elaborazione del DPS, per la predisposizione dello stesso, trasmette annualmente a tutti i Responsabili di trattamento aziendali la modulistica predefinita utile all'individuazione di tutte le informazioni necessarie e utili alla mappatura dei trattamenti per dipendente gestiti dalle Società del Gruppo VERITAS ed affidati a fornitori esterni.

È cura dei Responsabili di trattamento restituire all'Ufficio Gestione Dati Personali Privacy nei tempi indicati tutte le informazioni richieste per ogni incaricato, segnalando eventuali cambiamenti rispetto all'anno precedente. È altresì cura dei Responsabili di trattamento, al di fuori del momento di raccolta dati in oggetto, d'informare tempestivamente l'Ufficio Gestione Dati Personali Privacy di eventuali cambiamenti alla struttura organizzativa che interessino anche il trattamento dei dati personali.

I moduli utilizzati per la raccolta e comunicazione dati all'Ufficio Gestione Dati Personali Privacy sono:

- M-Privacy-01 e 01-A Scheda rilevazione trattamenti e Indicazioni per la compilazione
- M-Privacy-02 Conferma situazione anno precedente
- M-Privacy-03 Verifica situazione trattamenti
- M-Privacy-04 Scheda B Rilevazione rischi associati al trattamento dati
- M-Privacy-05 Scheda Trattamenti Videosorveglianza

A seguito della rilevazione dati viene aggiornato il DPS e vengono definite e sottoscritte le lettere di incarico agli incaricati.

Oltre alla revisione annuale del DPS viene garantito anche un aggiornamento in continuo sulla scorta della mobilità del personale. La rintracciabilità delle informazioni necessarie per garantire tali aggiornamenti è data dalle comunicazioni inerenti tale materia provenienti dall'area Organizzazione e Risorse Umane di Gruppo.

8 DIRITTI DELL'INTERESSATO

L'interessato ha diritto di ottenere dalle Società del Gruppo VERITAS la conferma circa l'esistenza o meno di dati personali che lo riguardano.

Eventuali richieste di conferma circa l'esistenza o meno di dati personali, devono essere rivolte per iscritto dall'interessato al titolare o al responsabile del dato delle Società del Gruppo VERITAS (anche attraverso un incaricato aziendale), tale richiesta va inviata in copia all'Ufficio Gestione Dati Personali – Privacy. La trasmissione può avvenire mediante lettera raccomandata, telefax o posta elettronica.

Eventuali richieste formulate oralmente devono comunque essere prese in carico e registrate dalle Società del Gruppo VERITAS a cura dell'incaricato o del responsabile interessato a trattamento oggetto di indagine, e trattate come quelle giunte in azienda per iscritto.

In particolare all'interessato devono esser rese disponibili le seguenti indicazioni, (*D.Lgs 196/2003 Art. 7*):

- origine dei dati personali;
- finalità e modalità del trattamento;
- logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- estremi identificativi del titolare, dei responsabili e del rappresentante designato (*D.Lgs 196/2003 Art. 5*)
- soggetti o categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

Inoltre, l''interessato ha diritto di ottenere l'aggiornamento dei dati e la loro cancellazione o trasformazione in forma anonima, o il blocco degli stessi qualora siano stati trattati in violazione della legge.

Qualora sussistano legittimi motivi l'interessato ha diritto di opporsi al trattamento dei dati personali che lo riguardano anche se tali dati sono pertinenti allo scopo di raccolta. Ha inoltre il diritto di opporsi al trattamento degli stessi qualora siano utilizzati a fini pubblicitari, di vendita, ricerca di mercato o per l'esercizio di altra comunicazione di tipo commerciale.

L'interessato, al fine di esercitare i diritti in materia di trattamento dati personali, può conferire delega o procura scritta a persone fisiche, enti, associazioni od organismi. In tal caso la persona che agisce per conto dell'interessato deve esibire e allegare alla richiesta copia della procura in oggetto, (ovvero di una delega sottoscritta in presenza di un incaricato aziendale o

sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato).
Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta deve invece essere avanzata da persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

I diritti di cui sopra, qualora concernenti persone decedute, possono essere esercitati dai legittimari ovvero dai soggetti che agiscano a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
L'intervello di tempo per rinnovare le richieste di questa tipologia non può essere minore di novanta giorni, salva l'esistenza di giustificati motivi (D.Lgs 196/2003 Art. 9).
Le azioni che titolare, responsabili e incaricati delle Società del Gruppo VERITAS intraprendono per la gestione di questa tipologia di richieste devono sempre essere volte ad agevolare l'accesso ai dati personali da parte dell'interessato, riducendo per quanto possibile i tempi di riscontro al richiedente. I dati richiesti possono essere comunicati al richiedente verbalmente o in forma scritta, purché sia sempre garantita la comprensione delle informazioni rilasciate.

9 RIFERIMENTI NORMATIVI E DOCUMENTALI

Riferimenti	
M ECO 08	Modulo per il conferimento di materiale proveniente da piccoli lavori di manutenzione e ristrutturazione domestica
M ECO 09	Modulo per il conferimento di particolari tipologie di RAEE
M PRY AZ 03	Informativa sul trattamento dei dati personali acquisiti con conferimento di materiali nei centri di raccolta
D.Lgs 196/2003	Codice in materia di protezione dei dati personali
D.Lgs 196/2003 B	Disciplinare tecnico in materia di misure minime di sicurezza
D.Lgs 196/2003 provvedimento	Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009 *(Gazzetta Ufficiale n. 149 del 30 giugno 2009)*
D.Lgs 196/2003 provvedimento	Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali - 13 ottobre 2008 (*Gazzetta Ufficiale n. 287 del 9 dicembre 2008*)
D.Lgs 196/2003 provvedimento	Provvedimento in materia di videosorveglianza - 8 aprile 2010 *(Gazzetta Ufficiale n. 99 del 29 aprile 2010)*
D.Lgs 196/2003 provvedimento	Provvedimento in materia di geo-localizzazione - 4 ottobre 2011
Guida operativa per redigere il DPSS	Codice in materia di protezione dei dati personali - allegato
Modello per l'interessato	Modulo per l'esercizio dei diritti in materia di protezione dati personali - allegato
Regolamento per l'utilizzo del sistema informatico GRUPPO VERITAS S.p.A.	
Privacy – Guida ad uso dei dipendenti	