www.italiaoggi.it
ItaliaOggi Sette

Privacy, l'amministratore di sistema

di **Antonio Ciccia**

Imprese e p.a. devono avere un amministratore di sistema, secondo quanto previsto dal provvedimento del garante della privacy del 27 novembre 2008, pubblicato sulla *Gazzetta Ufficiale* del 24 dicembre 2008. La misura consiste nella individuazione e formale nomina di chi amministra i sistemi informativi di una azienda, di un ente o di uno studio professionale. Tale provvedimento ha, secondo il garante, lo scopo di elevare il livello di sicurezza nel trattamento dei dati effettuato con gli elaboratori. Così si potrà contrastare un certo lassismo nell'uso dei computer ed elaboratori. L'obiettivo di quel provvedimento è fare in modo che si faccia effettivamente attenzione alla sicurezza informatica, responsabilizzando enti pubblici, imprese e professionisti e obbligandoli a rivolgersi a persone preparate e capaci di assicurare un livello adeguato di tutela degli elaboratori. L'adempimento può, però, incontrare alcune difficoltà interpretative e attuative. A questo scopo il garante ha pubblicato alcune faq sul suo sito istituzionale. Sempre per superare queste difficoltà operative potranno essere utili i modelli di designazione dell'amministratore di sistema e di comunicazione con il soggetto esterno che gestisce la rete in outsourcing.

A CHI SI APPLICA

Il garante ha precisato in un suo comunicato del 10 dicembre 2009 chi è tenuto alla nomina dell'amministratore di sistema e a gli altri adempimenti connessi. Questo allo scopo di arginare «azioni promozionali da parte di consulenti rischiano di disorientare alcune aziende, soprattutto quelle di piccole dimensioni, esponendole a immotivati aggravi economici». A questo proposito il garante ha chiarito che le prescrizioni riguardano solo quei soggetti che, nel trattare i dati personali con strumenti informatici, devono ricorrere o abbiano fatto ricorso alla figura professionale dell'amministratore di sistema o a una figura equivalente; conseguentemente le prescrizioni non si applicano, invece, a quei soggetti anche di natura associativa che, generalmente dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi, possano fare a meno di una figura professionale specificamente dedicata alla amministrazione dei sistemi o comunque abbiano ritenuto di non farvi ricorso. Insomma quello che conta è il dato dimensionale e organizzativo (anche se non si stabiliscono espressamente livelli soglia).

LOGGING

Il provvedimento prevede, tra gli altri adempimenti, il cosiddetto logging e cioè la registrazione degli accessi dell'amministratore di sistema, con indicazione dei tempi di apertura e chiusura dell'intervento e con la registrazione dell'evento che ha generato l'intervento del sistemista. Il garante, nel comunicato del 15 dicembre 2009, ha precisato che si può utilizzare software open source a costo zero per il logging degli accessi degli amministratori di sistema. L'adempimento può essere realizzato senza fare ricorso a costosi applicativi

SANZIONI

Non nominare l'amministratore di sistema privacy può costare caro. L'omissione apre la strada alla applicazione della sanzione prevista dall'articolo 162, comma 2 ter, del Codice della privacy. In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da 30 mila a 180 mila euro. Sanzioni tra l'altro incrementabili se ricorrono situazioni aggravanti o in caso di non sufficiente deterrenza della sanzione edittale. Peraltro l'adempimento non deve essere realizzato dalle piccole e medie imprese, se trattano dati, anche in relazione a obblighi contrattuali, precontrattuali o di legge, esclusivamente per finalità di ordine amministrativo e contabile. Rientrano in quest'ultima categoria, e si è perciò esonerati dall'obbligo di nominare l'amministratore di sistema, i trattamenti necessari per la gestione

di ordinativi, le buste paga e l'ordinaria corrispondenza con clienti, fornitori, realtà esterne di supporto anche in outsourcing e dipendenti.

LE INDICAZIONI DEL GARANTE

Il garante ha fornito alcune indicazioni operative rispondendo ad alcune domande frequenti. Vediamo le risposte. L'obbligo di registrazione degli accessi logici riguarda i sistemi client «postazioni di lavoro informatizzate». La raccolta dei log serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso). Non è richiesto in alcun modo che vengano registrati dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema. Nei casi più semplici la registrazione può essere soddisfatta tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti software o hardware aggiuntivi. Per esempio, la registrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità. Il titolare, tuttavia, deve valutare se adottare strumenti più sofisticati (raccolta dei log centralizzata, dispositivi non riscrivibili, tecniche crittografiche per la verifica dell'integrità delle registrazioni). I più diffusi sistemi operativi garantiscono anche la inalterabilità delle registrazioni. Il requisito, chiarisce il garante, può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i log server centralizzati e «certificati». Il garante, poi, si spinge a dire che il provvedimento non si preoccupa della effettiva genuina generazione dei dati registrati: il provvedimento si limita a prevedere come forma minima di documentazione dell'uso di un sistema informativo, la generazione del log degli «accessi» (log-in) e la loro archiviazione per almeno sei mesi in condizioni di ragionevole sicurezza e con strumenti adatti, in base al contesto in cui avviene il trattamento. Non c'è, dice la risposta del garante senza alcuna pretesa di instaurare in modo generalizzato, e solo con le prescrizioni del provvedimento, un regime rigoroso di registrazione degli usage data dei sistemi informativi. Inoltre l'accesso applicativo non è compreso tra le caratteristiche tipiche dell'amministratore di sistema e quindi non è necessario, in forza del provvedimento del garante, sottoporlo a registrazione. Per la nomina dell'amministratore di sistema è sufficiente specificare l'ambito di operatività in termini più generali, per settori o per aree applicative, senza obbligo di specificarlo rispetto a singoli sistemi, a meno che non sia ritenuto necessario in casi specifici.

Il fac simile della nomina

A cura di Giuseppe Caruso e Carlo Bendin

DESIGNAZIONE DI INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI E DI AMMINISTRATORE DI SISTEMA E ISTRUZIONI

(ai sensi del Codice in materia di protezione dei dati personali e del Provvedimento del Garante per la protezione dei dati personali del 27/11/2008)

PREMESSO in diritto

• che il Codice:
- definisce Incaricati le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- stabilisce che le operazioni di trattamento possono essere effettuate solo da Incaricati, che operano sotto la diretta autorità del Titolare o del Responsabile, designate per iscritto, con individuazione puntuale dell'ambito del trattamento consentito;

• che il Garante per la protezione dei dati personali con Provvedimento n. 13 del 1° marzo 2007 ha rilevato che:
- compete ai datori di lavoro, nel rispetto delle norme in tema di diritti e relazioni sindacali, assicurare la funzionalità e il corretto impiego di internet ed email da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa ed adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- nell'individuare regole di condotta degli Amministratori di sistema o figure analoghe deve essere svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni;

• che il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, fra l'altro:
- segnala a tutti i Titolari la particolare criticità del ruolo degli Amministratori di sistema e la necessità di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di Amministratore di sistema;
- richiama l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di Amministratore di sistema (laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali), tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità con cui si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile;
- prescrive al riguardo ai Titolari accorgimenti e misure ai sensi dell'art. 154, comma 1, lett. c) del

Codice e fra l'altro che;

- l'attribuzione delle funzioni di Amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, che deve fornire idonea garanzia del pieno rispetto delle norme in materia di trattamento di dati, compreso il profilo relativo alla sicurezza;
- la designazione quale Amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- anche quando le funzioni di Amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale Incaricato del trattamento ai sensi dell'art. 30 del Codice, il Titolare e il Responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29 del Codice;
- siano previste forme per consentire la conoscibilità dell'identità degli Amministratori di sistema, per registrarne gli accessi e per verificarne periodicamente l'operato;
- che i dati personali devono essere trattati e conservati nel rispetto del Codice, delle altre norme e dei Provvedimenti del Garante per la protezione dei dati personali e delle misure di sicurezza, delle disposizioni, istruzioni, procedure, policy del Titolare e del Responsabile;
- che per qualsiasi necessità o per la risoluzione di qualsiasi problematica inerente al trattamento gli Incaricati e gli Amministratori di sistema dovranno rivolgersi al Responsabile e/o Titolare.

PREMESSO in fatto

- che X, con sede legale in .., Via .., Codice Fiscale e Partita I.V.A. ..., é Titolare del trattamento dei dati personali di..., effettuati anche mediante strumenti elettronici;
- che l'Area Y di X ha per finalità……;
- che l'Area Y è composta delle seguenti Unità.....;
- che W è lavoratore subordinato … del Titolare con ruolo di… addetto all'Unità…, con la seguente job description.....;
- che W si dichiara ed è effettivamente soggetto che per esperienza, capacità ed affidabilità fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati, ivi compreso il profilo relativo alla sicurezza;
- che W svolge attività che, ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, è definibile di Amministratore di sistema;

Tutto ciò premesso, il Titolare

dopo essersi attenuto a criteri di valutazione equipollenti a quelli richiesti per la designazione dei Responsabili ai sensi dell'art. 29 del Codice, avendo valutata l'esperienza, la capacità e l'affidabilità del designato, tenuto anche conto del curriculum del sig. W e del suo contenuto (inclusi, attività svolte, titoli di studio, certificazioni professionali, esperienze professionali, corsi di formazione, ecc.), considerata la natura delle attività da esso attualmente svolte, considerato che con la sottoscrizione della presente lo stesso si impegna formalmente a fornire, ed appare idoneo a fornire, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati ivi compreso il profilo relativo alla sicurezza

designa

- il Signor W nato a <…> () il <…>19, Codice fiscale <…>, residente …, Incaricato del trattamento dei dati personali dei ..... trattati. Il designato dovrà trattare (quindi esemplificativamente, organizzare, consultare, elaborare, raffrontare, ecc.) i dati personali comuni (*ed eccezionalmente sensibili e / o giudiziari, nei limiti consentiti dalle norme di legge e dai provvedimenti del Garante per la protezione dei dati personali*) dei soggetti indicati cui ha ed avrà accesso con strumenti elettronici e senza, esclusivamente per le finalità ed attività dell'Unità ……., e quindi per ….. e comunque per le finalità indicate nelle premesse della presente (*Che costituiscono parte integrante ed inscindibile della stessa*) il tutto sempre nell'ambito e conformemente alle mansioni allo stesso attribuite, e quindi ……., attenendosi ai criteri di legge, a quanto prescritto dai Provvedimenti del Garante ed alle istruzioni impartite, qui di seguito o successivamente, dal Titolare e/o dal Responsabile nonché alle procedure e policy interne

designa inoltre

- il predetto Signor W……..., Amministratore di sistema…. ed indica analiticamente l'ambito di operatività consentito allo stesso in base al profilo di autorizzazione assegnato e precisamente

Con la sottoscrizione del presente atto il Signor W<…> accetta le designazioni suddette, conferma la propria esperienza e capacità nella materia nonché la diretta ed approfondita conoscenza degli obblighi previsti dal Codice e/o altre norme applicabili, dai Provvedimenti del Garante, e dalla normativa e procedure aziendali e dalla presente. Si impegna a procedere al trattamento dei dati personali attenendosi quindi a quanto stabilito dalla normativa e Provvedimenti in materia ed in conformità alle istruzioni impartitegli dal Titolare e dal Responsabile, nonchè alle disposizioni, policy, procedure e regolamenti aziendali, ecc..

informa il designato che

- gli estremi identificativi delle persone fisiche Amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati nel documento programmatico sulla sicurezza;
- qualora l'attività riguardi, o dovesse in futuro riguardare, anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, il Titolare renderà nota o conoscibile

l'identità del designato nell'ambito della proprie organizzazione, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici, conformemente e con le modalità previste dal Garante per la protezione dei dati personali e dalle norme;

- sono adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di sistema e quindi del designato;
- le registrazioni (access log) comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate ed hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. In ogni caso è tassativamente vietato intervenire in alcun modo su di esse (ad es. cancellandole, modificandole, alterandole, ecc. o compiendo qualsiasi altra attività sulle stesse). Le registrazioni sono conservate per almeno sei mesi;
- l'operato del designato sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti e precisamente ….

fornisce le seguenti istruzioni al designato

precisando che rimangono ferme e confermate le precedenti istruzioni, regolamenti aziendali, procedure e policy, in quanto non espressamente derogate dalla presente e/o non incompatibili con la stessa.

Particolare cura il designato deve prestare al rispetto delle misure di sicurezza dei dati, minime ed ulteriori, adottate per il trattamento dei dati con strumenti elettronici o senza. Il designato deve quindi applicare le misure minime ed ulteriori e compiere tutte le attività di competenza necessarie al fine di garantire il corretto funzionamento di esse anche con riferimento agli strumenti elettronici affidati o con riferimento ai quali svolge attività di manutenzione, assistenza, sviluppo, ecc..

In ogni caso il designato può trattare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati e/o comunque i soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento e per svolgere le attività attribuite e le mansioni di competenza.

Deve rispettare le norme sul trattamento dei dati personali ed in particolare, per quanto di competenza, anche quelle in materia di informazioni da fornire (art. 13 del Codice), quelle sul consenso da richiedere (laddove applicabili), tenendo presente che i dati personali debbono essere trattati in modo lecito e secondo correttezza, per scopi determinati, espliciti e legittimi. i dati debbono essere esatti e, se necessario, aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità e conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi.

Gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, quando affidati al designato, devono essere da quest'ultimo conservati (con conseguente obbligo di custodia degli stessi) e restituiti al termine delle operazioni affidate. In caso di allontanamenti, anche momentanei, dall'ufficio debbono essere adottate le misure e precauzioni del caso, anche mediante l'uso di contenitori protetti rispetto ad accessi illeciti o comunque non autorizzati. A conclusione dell'attività lavorativa (per pausa, fine giornata, ecc.) le misure e precauzioni adottate dovranno essere in ogni caso conformi a quanto previsto dalle norme, a quanto indicato nella presente, nelle istruzioni, regolamenti aziendali, procedure e policy, e, comunque, adeguate alla durata dell'interruzione.

I dati non debbono mai, per nessuna ragione, essere abbandonati. Il designato non deve consentire a terzi non autorizzati di prenderne anche solo visione. Deve essere controllata la integrità dei dati stessi.

In caso di distruzione di documenti devono essere utilizzati distruggitori e, comunque, adottate le cautele del caso.

Gli atti e i documenti contenenti i dati sensibili e/o giudiziari devono essere custoditi in contenitori/archivi muniti di serratura e debbono essere ivi conservati, fino alla restituzione Quando gli atti e i documenti contenenti dati personali sensibili e/o giudiziari sono affidati al designato per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi dagli Incaricati stessi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e devono essere restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati sensibili e/o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura sono identificate e registrate. Nel caso in cui si renda necessario l'accesso agli archivi contenenti i dati dopo l'orario di chiusura degli stessi, il designato, al quale sia stato espressamente richiesto di effettuare detto accesso, e quindi formalmente ed espressamente autorizzato, deve effettuare un'apposita registrazione dell'accesso.

I supporti cartacei contenenti la riproduzione di informazioni relative al trattamento di dati personali sensibili e/o giudiziari devono essere conservati e custoditi con le stesse modalità esposte sopra per gli originali.

Il designato nello svolgere le attività deve rammentare che il trattamento di dati personali con strumenti elettronici è consentito solo agli Incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo. Ad ogni Incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

Si rammenta la necessità di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia della stessa. Essa non deve mai essere condivisa né inserita in programmi, file o su supporti cartacei dove possa essere rintracciata.

La parola chiave deve essere composta secondo

quanto prescritto dalle norme e dalle procedure e comunque da almeno otto caratteri. Non deve contenere riferimenti agevolmente riconducibili all'Incaricato.

Essa è modificata dall'Incaricato al primo utilizzo e, successivamente, almeno ogni 3 mesi (o anche prima, laddove si siano verificate situazioni che possano averne compromesso la segretezza; in questo caso dette situazioni dovranno essere immediatamente segnalate al Responsabile ed al Titolare), adempiendo agli obblighi e svolgendo le attività previste dalla disciplina e dalle procedure relative al preposto alla custodia della copia delle credenziali. Si richiamano espressamente con riferimento a tali questioni le previsioni delle procedure, istruzioni, regolamenti aziendali e policy aziendali da aversi qui per integralmente trascritte.

Non è consentita l'utilizzazione di codici identificativi personali e parole chiave di altri soggetti.

Il codice per l'identificazione non può essere assegnato ad altri Incaricati, neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Gli Incaricati debbono segnalare il mancato utilizzo per più di sei mesi di un codice identificativo al Titolare e/o al Responsabile.

Le credenziali di autenticazione devono sempre essere disattivate in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali.

Gli strumenti elettronici possono essere utilizzati solo dagli Incaricati che li hanno in uso o che sono stati preventivamente autorizzati. Non possono essere utilizzati da visitatori o da terzi. Lo strumento elettronico non deve essere mai lasciato incustodito e accessibile durante una sessione di trattamento. Anche per brevi assenze deve essere quanto meno attivato lo screen saver con password. In ogni altro caso è necessario chiudere la sessione. Eventuali anomalie al riguardo debbono essere prontamente segnalate. Le attività svolte durante la sessione abilitata con le credenziali dell'Incaricato sono automaticamente attribuite all'Incaricato stesso, che ne deve rispondere.

Il Titolare, anche con procedure ed istruzioni, ha assicurato la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. A tale scopo la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza ed è stato individuato preventivamente per iscritto il soggetto incaricato della loro custodia. Tale soggetto deve informare tempestivamente l'Incaricato dell'intervento effettuato.

Per gli Incaricati sono individuati profili di autorizzazione di ambito diverso ed è, quindi, utilizzato un sistema di autorizzazione. I profili di autorizzazione, di norma, per classi omogenee di Incaricati, sono stati individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, é verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione e contestualmente si provvede all'aggiornamento periodico, con cadenza almeno annuale, dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, eventualmente anche per classi omogenee di incarico.

Conformemente alle procedure vigenti è previsto il salvataggio dei dati con frequenza almeno settimanale, effettuato attraverso opportune procedure di back-up e conservazione degli stessi, anche in luoghi diversi da quelli in cui sono collocati i dispositivi di memorizzazione principali, con necessità da parte del designato di svolgere le (eventuali) attività al riguardo previste dalle procedure e dalle istruzioni. Il mantenimento dei dati salvati, così come di qualsiasi supporto di memorizzazione (il cui utilizzo sia stato eventualmente autorizzato), deve avvenire sempre in luoghi e con modalità che presentino misure di protezione analoghe a quelle definite per il trattamento dei dati, conformemente alle norme di legge e regolamentari ed alle specifiche previsioni e policy interne.

Deve essere sempre tenuto presente il rischio di perdita, cancellazione o distruzione anche accidentale dei dati, che possono comprometterne la disponibilità.

La disponibilità dei dati e del servizio informatico deve essere garantita attraverso i mezzi e le precauzioni esistenti, con effettuazione delle attività al riguardo previste, nel rispetto delle misure dei sistemi ripristino e di disaster recovery previste. Il designato deve segnalare immediatamente ogni anomalia o situazione particolare che dovesse verificarsi, così da consentire l'immediata adozione delle contromisure meglio viste ed il superamento di eventuali criticità.

Devono sempre essere utilizzati, conformemente alle istruzioni, i dispositivi ed i programmi antivirus, firewall, ecc., necessari per la protezione del sistema e degli strumenti e devono essere sempre rispettate le procedure per l'aggiornamento periodico, comunque almeno semestrale, dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne i difetti. Devono, inoltre, essere rispettate le istruzioni atte a prevenire contaminazioni, tanto per quanto attiene alla posta elettronica, che per altri utilizzi, rivolgendosi al Titolare o al Responsabile in ogni caso di dubbio.

È tassativamente vietato l'utilizzo personale ed improprio degli strumenti in dotazione, delle apparecchiature hardware e software, dei collegamenti intranet e/o internet, della posta elettronica, nonché dei dati a qualsiasi titolo posseduti, ricevuti, trasmessi dal Titolare. Debbono essere rispettate le istruzioni, procedure, regolamenti aziendali, policy ed i regolamenti sull'utilizzo di detti strumenti e le altre disposizioni interne in materia.

Tutti gli strumenti elettronici assegnati o a disposizione costituiscono strumento di lavoro. Pertanto, l'utilizzo di essi è consentito esclusivamente per finalità direttamente attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative ed interne e con esclusione di qualsivoglia uso per scopi privati e/o personali.

L'utilizzo di tali strumenti non configura alcuna titolarità dei dati o delle informazioni trattate, che appartengono al Titolare, ferme restando le disposizioni

specifiche con riferimento ai dati personali.

Il personal computer, e gli altri eventuali strumenti elettronici, sono affidati al designato, con ogni conseguente obbligo di custodia e di utilizzo appropriato. Il designato è tenuto ad informare immediatamente il Titolare e il Responsabile nell'ipotesi di furto, danneggiamento o malfunzionamento anche parziale degli stessi, del sistema o del software.

Il designato deve utilizzare gli strumenti elettronici con la massima attenzione e diligenza, essendo beni rilevanti anche ai fini della sicurezza. Gli strumenti sono configurati in modo da garantire il rispetto della normativa; tale configurazione non deve essere mutata. Ogni anomalia o disfunzione deve essere prontamente segnalata.

Non è consentito installare sugli strumenti elettronici softwares, anche se gratuiti (freeware o shareware), non distribuiti e/o comunque non espressamente autorizzati, né collegare ai personal computer o agli strumenti elettronici periferiche hardware o dispositivi non messi a disposizione dal Titolare.

Non è consentita la modifica delle impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, del software di posta elettronica e di ogni altro software installato sui personal computer o sugli strumenti elettronici o sul sistema.

Non è consentito caricare o comunque detenere nei personal computer o negli strumenti elettronici materiale informatico, dati ed informazioni personali o comunque di contenuto non attinente alla mansione ricoperta.

È in ogni caso tassativamente vietato caricare o detenere materiale informatico:

a) il cui contenuto (a mero titolo esemplificativo: testo, audio e video) sia coperto da diritto d'autore, salvo che si tratti di materiale, lecitamente acquisito per scopi esclusivamente aziendali, con espressa autorizzazione scritta del Titolare;

b) il cui contenuto attenga o riguardi dati sensibili o giudiziari (salvo che si tratti di dati che é indispensabile trattare con tali mezzi, conformemente alle disposizioni di legge e del Garante per la protezione dei dati personali ed istruzioni, per le mansioni attribuite) o che consenta di conoscere dati sensibili o giudiziari;

c) il cui contenuto sia contrario a norme di legge;

d) per finalità ludiche o di svago o comunque non lavorative.

Non è consentito al designato, salva diversa espressa autorizzazione, accedere al BIOS del personal computer o degli strumenti elettronici né impostare protezioni o password ulteriori rispetto alle credenziali di autenticazione predisposte che limitino l'accesso al personal computer, agli strumenti elettronici e/o alle relative periferiche.

Il designato deve, fra l'altro:

a) evitare qualsiasi uso di strumenti elettronici personali (pc, periferiche, dispositivi di memorizzazione, ecc.) sul luogo di lavoro o per usi lavorativi;

b) non alterare o disattivare le misure di sicurezza minime od ulteriori adottate ed anzi effettuare quanto di competenza per garantirne il funzionamento, segnalando tempestivamente ogni anomalia o disfunzione;

c) non impostare password o analoghe protezioni ai singoli archivi informatici (dischi, cartelle o files), ecc., al di fuori di quelle previste dalle procedure interne, dalla configurazione del sistema, o da specifiche istruzioni scritte.

Conformemente alle istruzioni organizzative e tecniche, deve essere garantita sempre la custodia e l'uso dei supporti rimovibili (Dvd, floppy disk, Cd Rom, memory stick, ecc.) su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

I supporti già utilizzati per il trattamento di dati sensibili e/o giudiziari possono essere riutilizzati solo qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti o resi inutilizzabili. È quindi vietato il reimpiego di supporti di memorizzazione utilizzati per il trattamento di dati sensibili e/o giudiziari per i quali non sia fornita la certificazione scritta dell'impossibilità tecnica di recupero dei dati in essi precedentemente contenuti.

In ogni caso, qualsiasi sia lo strumento utilizzato per il trattamento, i dati personali devono essere custoditi mediante l'adozione delle misure di sicurezza legalmente previste e di quelle ulteriori adottate o, comunque, necessarie, che sono state illustrate, con spiegazione dell'analisi dei rischi che incombono sui dati e delle misure 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. Sono stati illustrati anche i criteri e le modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Sono previsti interventi formativi con le modalità, nelle fattispecie e con i contenuti previsti dalle norme e dai Provvedimenti del Garante, cui si rinvia.

Il designato deve sempre tenere conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2 del Codice).

Nelle attività da svolgere (quali a titolo meramente esemplificativo, quelle di assistenza, consulenza, manutenzione, sviluppo, amministrazione di sistema, ecc.) con riferimento agli strumenti informatici si devono inoltre e sempre applicare:

- il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice);
- il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice);
- il principio in forza dei quali i trattamenti

devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice), osservando il principio di pertinenza e non eccedenza, trattando i dati «nella misura meno invasiva possibile»; eventuali attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere mirate sull'area di rischio, tenendo conto della normative in materia.

Vanno inoltre sempre applicate le norme ed i Provvedimenti del Garante, incluso esemplificativamente quello n. 13 del 1 marzo 2007 al cui contenuto, così come quello del 27 novembre 2008, si rinvia.

I trattamenti del designato devono essere ispirati ad un canone di liceità, trasparenza e correttezza.

Nel caso di interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti ed i soggetti preposti debbono svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza.

È tassativamente vietato qualsiasi trattamento effettuato con sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l'attività di lavoratori.

In applicazione del menzionato principio di necessità il Titolare promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a «minimizzare» l'uso di dati riferibili ai lavoratori.

Va ribadito che il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati – riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (*Artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale*). Il Titolare ha esplicitato una precisa policy per evitare un'aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione disponendo quindi che…… Sono stati adottati accorgimenti per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza, tramite …sono previste soluzioni utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza (*Si rinvia sul punto alle policy e discipline interne aziendali, da avere qui per trascritte*).

Per quanto attiene agli eventuali controlli sull'uso degli strumenti elettronici deve essere evitata ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. Infatti, come è noto, gli eventuale controlli sono leciti…… solo se sono rispettati i principi di pertinenza e non eccedenza. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Titolare può adottare eventuali misure che consentano la verifica di comportamenti anomali, preferendo controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Sono vietati comunque controlli prolungati, costanti o indiscriminati, come previsto nel Regolamento….

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

La conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata solo da particolari esigenze tecniche o di sicurezza, o da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla (v. art. 11, comma 1, lett. e), del Codice). Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1 e 5 del 2008 adottate dal Garante ed eventualmente dell'autorizzazione n. 7 del 2008 per i dati giudiziari) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti……

Resta fermo l'obbligo del designato di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità legalmente previste, senza realizzare attività di controllo a distanza.

All'atto della cessazione del rapporto con il Titolare il designato dovrà in ogni caso restituire tutti i dati personali trattati con espresso e formale divieto di conservarli, duplicarli, ecc.

Il designato dovrà inoltre:

1. segnalare al Titolare la necessità di adottare eventuali ulteriori misure;
2. informare immediatamente il Titolare in caso di situazioni anomale o di emergenze, adoperandosi immediatamente per risolverle, conformemente alle istruzioni ricevute, e/o comunque per attenuarne eventuali conseguenze;
3. fornire la massima collaborazione nelle verifiche periodiche del Titolare per consentirgli di vigilare sulla puntuale osservanza delle disposizioni di legge, dei provvedimenti del Garante

e delle proprie istruzioni;
4. prendere visione della documentazione in materia di privacy e sicurezza dei dati resa disponibile in via informatica o cartacea e a darvi integrale applicazione;
5. collaborare a garantire il rispetto della regola 25 dell'Allegato B che prevede che il Titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura per provvedere all'esecuzione di queste riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del presente disciplinare tecnico;
6. controllare periodicamente l'efficienza dei sistemi tecnici di competenza, redigere un apposito verbale, da consegnare al Titolare o al Responsabile, riportante i nominativi dei partecipanti al controllo, i riscontri e le verifiche effettuate, i parametri adottati e gli accorgimenti proposti per migliorare la sicurezza;
7. prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati, provvedere alla gestione delle procedure di back up e di ripristino ed assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
8. effettuare la distruzione e lo smaltimento dei supporti informatici di memorizzazione logica o verificare le modalità con le quali vengono effettuati da terzi, comunque nel rispetto delle norme e dei Provvedimenti del Garante (per esempio, del Provv. del 13 ottobre 2008);
9. aggiornare periodicamente, con frequenza almeno semestrale, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
10. suggerire l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a realizzare quanto previsto dall'art. 31 del dlgs n. 196/2003 e dai Provvedimenti del Garante;
11. collaborare alle attività di gestione ed attivazione dei sistemi di risposta automatica per le email degli assenti, come previsto dalla disciplina.;
12. adempiere ogni altro compito previsto dalla normativa.

In caso di richiesta di accesso o di esercizio dei diritti legalmente previsti avanzata da un interessato, l'Incaricato dovrà interessare immediatamente il Responsabile e/o il Titolare, attenendosi, comunque, alle procedure vigenti Il Titolare, comunque, in qualsiasi momento, attraverso Responsabili e/o Incaricati, potrà verificare la puntuale osservanza da parte del designato delle norme, dei Provvedimenti del Garante e delle istruzioni fornite in materia di trattamento dei dati personali e di protezione dei dati (incluse esemplificativamente quelle sulle misure minime ed ulteriori) e, quindi, dei compiti e delle responsabilità, come previste dal presente atto di designazione, dalle istruzioni e dalle norme. Potrà inoltre ed in particolare<…> Il designato conferma - con la sottoscrizione del presente atto - la piena accettazione della presente designazione e degli impegni, dichiarazioni e obblighi ivi previsti.

La designazione di Incaricato di trattamento e di Amministratore di sistema di trattamento si dovrà considerare comunque automaticamente revocata alla cessazione del rapporto di lavoro sopra indicato.

La presente individuazione dell'ambito del trattamento dei dati, che deriva dall'applicazione di norme imperative, non comporta alcuna modifica retributiva e/o contrattuale e/o mansionistica al rapporto di lavoro degli addetti/Incaricati.

Sono allegati al presente e ne fanno parte integrante i documenti normativi ed i provvedimenti sopra indicati.

Genova,

Il Titolare **Il Responsabile**