



Il codice sulla Privacy e le nuove misure

Domande e risposte sul codice della privacy

Cos'è la privacy ? Posso fare l'autocertificazione o devo fare il DPS? Chi è l'amministratore di sistema?

Domande e risposte per capire meglio il codice sulla privacy



Che cos'è la Privacy ?

Dal 1996 in Italia vige il "diritto alla protezione dei dati personali" a cui comunemente ci si riferisce come "**Legge sulla Privacy**": infatti il 31 dicembre 1996 è entrata in vigore la legge n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali". Nel 2003 tale legge è stata abrogata e sostituita dal decreto legislativo 196/03 noto come "**Codice in materia di protezione dei dati personali**"¹ entrato in vigore il primo gennaio 2004.

Il primo articolo del Codice chiarisce cosa si intende per privacy nell'ordinamento italiano; recita infatti tale articolo: "**chiunque ha diritto alla protezione dei dati personali che lo riguardano**". Tale protezione consiste nella garanzia che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla **riservatezza**, all'identità personale ed al diritto alla protezione dei dati personali.

Va chiarito che lo spirito della legge non è impedire il trattamento dei dati personali ma evitare che questo avvenga contro la volontà dell'avente diritto, ovvero secondo modalità "pregiudizievoli". Il Codice, in pratica, definisce la modalità di raccolta dei dati, gli obblighi di chi raccoglie, detiene o tratta dati personali e le responsabilità e sanzioni in caso di danni.

Nel 1997 è stato costituito il "**Garante per la protezione dei dati personali**", un organo collegiale composto da quattro membri eletto dal Parlamento che ha il compito di vigilare sul rispetto delle norme sulla privacy. Alle dipendenze del Garante è posto un Ufficio con un organico di circa 100 unità.

Il Garante ha sintetizzato² i contenuti delle norme sulla privacy come segue.

- **I dati personali sono una proiezione della persona.** La legge tutela la riservatezza, l'identità personale, la dignità e gli altri nostri diritti e libertà fondamentali.
- Il trattamento dei dati che ci riguardano deve rispettare **le garanzie** previste dalla legge.
- **La prima garanzia è la trasparenza.** Ognuno di noi ha il diritto di "sapere". Il diritto di conoscere se un soggetto detiene informazioni, di apprenderne il contenuto, di farle rettificare se erronee, incomplete o non aggiornate.
- **Conoscere i nostri diritti** e il modo per farli valere è semplice.

Chi deve adeguarsi alla normativa sulla privacy?

Chiunque nello svolgimento della propria attività tratti o utilizzi dati di carattere personale, riservato o sensibile, è tenuto ad adeguarsi al codice sulla privacy. In molti casi è sufficiente preparare una semplice autocertificazione (in appendice al documento vi è un esempio) in altri casi invece è necessario predisporre il DPS documento Programmatico sulla Sicurezza dei dati , che può essere redatto in forma semplice o completa.

In cosa consiste l'autocertificazione?

Il **27 novembre 2008** con un provvedimento a carattere generale dal titolo "[Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B\) al Codice in materia di protezione dei dati personali](#)"³, il Garante ha individuato modalità semplificate di applicazione delle misure minime di sicurezza. Tra le modalità semplificate vi è anche una "semplificazione" per il DPS.

Recita il provvedimento:

¹ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248>

² Brochure "La tutela dei dati personali: il primo Garante sei tu"
<http://www.garanteprivacy.it/garante/document?ID=1382763>

³ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1571218>

“ Fermo restando che per alcuni casi è già previsto per disposizione di legge che si possa redigere un'autocertificazione in luogo del documento programmatico sulla sicurezza (...), i soggetti pubblici e privati che trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare liberi professionisti, artigiani e piccole e medie imprese, possono redigere un documento programmatico sulla sicurezza semplificato.”

L'autocertificazione è quindi una dichiarazione sostitutiva dell'atto di notorietà, nella quale sotto la propria responsabilità penale si autocertifica l'adozione delle misure di sicurezza minime ed idonee (Art. 33, 24 e allegato tecnico al codice) in sostituzione della presentazione del DPS.

Chi può fare l'autocertificazione?

Il garante indica che chiunque tratti dati di carattere non sensibile, con o senza l'ausilio di strumenti elettronici, necessari agli adempimenti ordinari ed al funzionamento della propria attività può fare l'autocertificazione. Specifica inoltre che, tutti comunque sono tenuti ad adottare le misure minime di sicurezza.

Cosa si rischia con la nuova normativa ?

L'autocertificazione può essere resa solo dal titolare. L'art. 168 del D.lgs 196/2003 prevede il reato di falsità nelle dichiarazioni al Garante, pertanto dichiarare ad esempio di aver messo in atto misure minime di sicurezza o di effettuare solo trattamento di dati non sensibili o relativi allo stato di salute o all'adesione a sindacati dei propri dipendenti e che il trattamento è stato eseguito in osservanza delle misure di sicurezza richieste dal codice nonché dall'Allegato B) quando questo non corrisponde al vero costituisce reato punibile con la reclusione da 6 mesi a 3 anni.

La medesima dichiarazione rilasciata a pubblico ufficiale ad esempio durante una visita ispettiva oppure producendo il documento per partecipare ad un bando viene punita ai sensi delle norme previste dal cp.

- Falsa attestazione di fatti in atto pubblico art.483 C.P.: reclusione fino a 2 anni
- Uso di atto falso art.489 C.P.: reclusione fino a 1 anno e 4 mesi
- Dichiarazione mendace resa al pubblico ufficiale in atto pubblico: reclusione fino a 3 anni (Art.495 C.P.: dichiarare il falso direttamente in un atto pubblico o in una dichiarazione destinata a esservi riprodotta, dinanzi al pubblico ufficiale, relativamente all'identità, allo stato o a qualità personali proprie o di altri).

Cosa sono le misure minime?

Le misure minime sono misure di sicurezza che il garante indica per garantire la sicurezza dei dati dell'azienda e consistono in misure di protezione fisiche, armadi dotati di serrature, o tecnologiche, cioè misure che devono essere adottate da chi tratta i dati con strumenti di elaborazione dati.

Cosa si rischia nel non adottare le "misure minime"?

L'omessa adozione di alcune misure indispensabili ("minime"), le cui modalità sono specificate tassativamente nell'Allegato B) del Codice, costituisce anche reato; l'art. 169 del Codice prevede l'arresto sino a due anni o l'ammenda da 10 mila euro a 50 mila euro

Cos'è il DPS o Documento Programmatico sulla Sicurezza ?

Qualunque azienda, pubblica amministrazione, ente o associazione che sia titolare di un trattamento di dati personali, **sensibili o giudiziari** effettuato con strumenti elettronici deve redigere ed aggiornare per iscritto entro il 31 marzo di ogni anno un documento che riporti le misure di sicurezza adottate o che si programma di adottare per la tutela dei dati trattati.



Chi deve redigere il DPS?

Il DPS cade sotto la responsabilità del titolare (cioè del **legale rappresentante** dell'azienda o ente); questi può farsi coadiuvare nella redazione del Documento da un organo, ufficio o persona fisica a ciò legittimata in base all'ordinamento aziendale (art. 34, comma 1, lett. g), del Codice; regola 19 dell'Allegato B)).

Che contenuti deve avere il DPS?

Il DPS deve contenere, al minimo (regola 19 dell'allegato B, "[Disciplinare tecnico in materia di misure minime di sicurezza](#)"⁴, del D. Lgs. n.196):

- l'elenco dei trattamenti di dati personali;
- I compiti e le responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati,
- 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 (...);
- la previsione di interventi formativi degli incaricati del trattamento (...);
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

Inoltre a seguito della pubblicazione del provvedimento del Garante relativo agli "Amministratori di sistema" del novembre 2008 occorre allegare al DPS:

- l'elenco degli amministratori di sistema.

Il DPS va inviato al Garante?

No, va conservato presso il Titolare (o il Responsabile se nominato).

Il DPS è una misura minima per chi vi è tenuto?

S, il caso il DPS sia ritenuto necessario viene considerato una misura minima

Perché va citato il DPS nella relazione accompagnatoria al bilancio d'esercizio?

Scriva il Garante:

"Premesso che le scelte di fondo sulle modalità di trattamento sotto il profilo della sicurezza competono alle persone e agli organi legittimati ad adottare decisioni ed esprimere a vari livelli, in base al proprio ordinamento interno, la volontà della società, ente o altro organismo titolare del trattamento (art. 4, comma 1, lett. f), del Codice), il Codice ha introdotto una nuova regola per rendere meglio edotti gli organi di vertice del titolare del trattamento e responsabilizzarli in materia di sicurezza, **attraverso l'obbligo di riferire nella relazione di accompagnamento a ciascun bilancio di esercizio circa l'avvenuta redazione o aggiornamento del DPS che sia obbligatorio come misura "minima"** o che sia stato comunque adottato (regola 26 Allegato B)). Anche questa menzione rappresenta una misura "minima" nuova, indicata tra quelle di "tutela e garanzia" (regole 25 e 26)."

⁴ <http://www.garanteprivacy.it/garante/doc.jsp?ID=488497>

Chi controlla che le misure minime e gli altri adempimenti previsti dalla legge siano messi in pratica?

La Polizia Postale (con le sue 76 Sezioni sul territorio) e la Guardia di Finanza in forza di un protocollo di intesa con il Garante.

Se esiste una autorizzazione generale al trattamento dei dati, è possibile trattare i dati senza il consenso dell'interessato?

No, è solo possibile omettere la notifica al Garante e si può procedere con il trattamento dei dati, osservando tutte le prescrizioni.

Il documento DPS è solo un adempimento legale?

Il documento rappresenta non solo un adempimento legale ma un vero e proprio strumento di riferimento per l'azienda in materia di trattamento dei dati personali, e in generale di definizione delle strategie di sicurezza, e delle conseguenti policy che tutti i dipendenti, collaboratori, partner e fornitori devono adottare.

Non siamo collegati ad internet, non siamo già sicuri?

No. Il collegamento ad internet è solo una delle minacce e neanche la più importante. Secondo le statistiche di istituti di ricerca e polizie, circa tre quarti degli incidenti sono generati all'interno delle organizzazioni. Di questi, oltre la metà sono involontari, perchè... "errare è umano".

Le misure minime di sicurezza richieste dal Dlgs.196/2003 non sono esagerate rispetto alle necessità ed alle possibilità di una piccola azienda?

No. Probabilmente molte delle misure richieste dalla legge sono già prassi comune nella vostra azienda. Ai fini della conformità al Codice della Privacy, si tratta per lo più di formalizzare quanto già fate grazie al Documento Programmatico sulla Sicurezza. Eventuali misure aggiuntive non sono di norma molto onerose né da un punto di vista economico né da un punto di vista organizzativo.

I dati personali che abbiamo li facciamo elaborare da uno studio esterno, non è lui il titolare?

No. Anche se tutti i trattamenti (per esempio di paghe e contributi o contabili) sono effettuati all'esterno, i titolari di quei trattamenti siete voi e quindi voi ne risponderete in merito alla loro privacy e sicurezza.

La nostra rete è protetta dal "firewall", non siamo già sicuri?

No. Il firewall è un dispositivo utile, ma che, quando ben gestito, svolge solo una funzione ben precisa: proteggere la vostra rete informatica aziendale da specifici tipi di incidenti di origine esterna. Questo ha poco a che vedere con la Privacy ed il Dlgs.196/2003, che in particolare mira anche a proteggere i dati personali (informatici e non) e la vostra azienda sia da incidenti interni che esterni, deliberati o accidentali. Per esempio, il firewall non vi serve a proteggere i dati in caso di perdita accidentale per guasto o furto del computer e tantomeno a proteggere i vostri archivi cartacei dalle conseguenze di un incendio.



le novità normative introdotte nel 2009

Nel corso del 2009 la normativa sulla privacy è stato modificato in modo significativo. Le principali novità normative ed i relativi adempimenti di cui bisogna tener conto nell'aggiornamento del DPS per il 2009 sono:

- amministratore di sistema;
- rottamazione PC ed affini;
- legge 18 marzo 2008 sui crimini informatici;
- i nuovi reati introdotti nel d. lgs. 231/01 in materia di violazione del diritto di autore.

Amministratore di sistema

Si tratta del provvedimento "[Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema](#)"⁵ del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008.

Chi è l'amministratore di sistema?

Si tratta di una figura interna od esterna all'azienda che è incaricata di gestire il funzionamento del sistema e la sicurezza dei dati aziendali in particolare si deve occupare di :

- Verificare periodicamente che gli utenti cambino regolarmente la password di accesso al sistema
- Verificare che i sistemi antivirus ed antispam siano aggiornati e funzionino regolarmente
- Verificare che i sistemi operativi ed il software venga regolarmente aggiornato alle ultime versioni
- Controllare che i sistemi di Backup e Disaster recovery siano funzionanti e in perfetta efficienza
- Verificare che la rete sia protetta da accessi esterni non autorizzati

Che competenze deve avere un amministratore di sistema

Il Garante lo indica così: "L'attribuzione delle funzioni di **amministratore di sistema** deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza"

In sostanza deve dimostrare una provata esperienza nell'ambito della gestione di un sistema informatico e nel trattamento dei dati.

Cosa è necessario fare per nominare L'amministratore di sistema?

Il titolare del trattamento deve redarre una lettera d'incarico designandolo. 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.

⁵ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499>



E' necessario verificare l'operato dell'amministratore di sistema?

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Come può essere verificato l'operato degli amministratori di sistema. (LOG di Sistema)

Il garante indica che ,devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Chi deve nominare un amministratore di sistema?

Chiunque sia tenuto a produrre un DPS anche in forma semplice ed utilizzi una rete informatica aziendale nel trattamento dei dati personali o sensibili.

Quali sono i tempi di adozione del provvedimento?

Entro il 15 dicembre 2009

Rottamazione PC ed affini

Di cosa si tratta?

Si tratta del provvedimento "[Rifiuti di apparecchiature elettriche ed elettroniche \(Raee\) e misure di sicurezza dei dati personali](#)"⁶ del 13 ottobre 2008, in G.U. n. 287 del 9 dicembre 2008.

Il Garante richiede che ogni titolare del trattamento deve adottare appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possono verificarsi in occasione della dismissione dei menzionati apparati elettrici ed elettronici (artt. 31 ss. del Codice) . In pratica il Garante vuole che siano prevenuti accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere:

- reimpiegate o riciclate
- smaltite.

Legge N° 48 del 18 marzo 2008 sui crimini informatici

Di cosa si tratta?

Si tratta della "[Legge 18 marzo 2008, n. 48 - "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento](#)

⁶ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1571514>



[dell'ordinamento interno](#)⁷ che ha introdotto nuovi adempimenti per la sicurezza informatica in quanto ha modificato (art. 10) sia il "Codice in materia di protezione dei dati personali" sia (art. 7) il decreto legislativo 8 giugno 2001, n. 231 (la cosiddetta "Responsabilità amministrativa delle imprese").

Il **D. lgs. n. 231/2001** – "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n.300", si applica a tutte le persone giuridiche e alle società e associazioni anche prive di personalità giuridica, ad esclusione dello Stato, degli enti pubblici territoriali, degli altri enti pubblici non economici, nonché agli enti che svolgono funzioni di rilievo costituzionale.

Tale decreto introduce nell'ordinamento italiano il concetto di responsabilità delle società nei casi in cui persone fisiche commettano dei reati anche nell'interesse o a vantaggio della società stessa.

Le aziende devono in poche parole predisporre **preventive ed idonee misure di sicurezza** e di controllo per prevenire ed impedire che il management o i dipendenti commettano reati informatici quali quelli previsti dalla **legge n.48/2008 sulla "criminalità informatica"**. In mancanza di tali misure, nel caso il reato sia commesso e porti un vantaggio diretto o indiretto all'azienda, l'azienda ne risponde.

Di seguito l'elenco dei reati informatici trattati da questa legge.

- 420: attentato a impianti di pubblica utilità compreso il danneggiamento o la distruzione di sistemi informatici o telematici di pubblica utilità
- 491-bis: falsità in un documento informatico pubblico o privato
- 615-ter: accesso abusivo ad un sistema informatico o telematico
- 615-quater: detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- 615-quinquies: diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- 617-quater: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- 617-quinquies: installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- 635-bis: danneggiamento di informazioni, dati e programmi informatici
- 635-ter: danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- 635-quater: danneggiamento di sistemi informatici o telematici
- 640-quinquies: truffa del certificatore di firma elettronica

I nuovi reati introdotti nel d. lgs. 231/01 in materia di violazione del diritto di autore

Nel luglio 2009 il **D. lgs. n. 231/2001** è stato modificato con l'introduzione dell'art 25-novies in materia di violazione del diritto di autore che riguarda i seguenti reati.

- **art. 171, l. 633/1941 comma 1 lett a) bis:** messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa;
- **art. 171, l. 633/1941 comma 3:** reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione;
- **art. 171-bis l. 633/1941 comma 1:** abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o

⁷ <http://www.parlamento.it/parlam/leggi/080481.htm>



concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE;
predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori;

- **art. 171-bis l. 633/1941 comma 2:** riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati;
- **art. 171-ter l. 633/1941:** abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
- **art. 171-septies l. 633/1941:** mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione;
- **art. 171-octies l. 633/1941:** fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale.



I servizi sulla gestione della privacy offerti da Archimedia

Grazie ai servizi offerti da Archimedia è possibile mettersi in regola con facilità e in modo sicuro.

I servizi offerti sono :

- 1. Gestione Online dei Log Amministratori di Sistema**
Consente di adempiere alle prescrizioni del Garante mediante tenuta del registro dei LOG online.
- 2. Delega esterna dell' amministratore di sistema**
Archimedia mette a disposizione una figura con idoneo profilo professionale da nominare quale **amministratore di sistema**. Questo servizio è adatto alle strutture che non hanno un proprio amministratore di sistema, figura comunque prevista dalle prescrizioni del Garante.
- 3. Delega esterna come responsabile per il trattamento dei dati**
Oltre ai servizi precedenti Archimedia mette a disposizione può assumere il ruolo di **responsabile esterno per il trattamento dei dati** per gli adempimenti relativi alla privacy. Questo servizio è adatto alle imprese che non avendo responsabile interno del trattamento vogliono affidare esternamente la gestione degli obblighi derivanti dal codice sulla privacy e la gestione di redazione ed aggiornamento periodico del DPS
- 4. Gestione e monitoraggio on-line del sistema informativo del cliente**
Questo servizio permette al cliente di disporre di un monitoraggio attento e puntuale della propria infrastruttura IT . Il servizio prevede:

Monitoraggio di server

Monitoraggio e gestione semplici ed efficaci dello stato di salute di uno dei più cruciali sistemi aziendali: il server. Il monitoraggio del server aiuta a evitare i rischi di costose azioni correttive e di danni di notevole entità grazie al controllo preventivo della protezione di server, hardware e disco, delle prestazioni, delle applicazioni e del software

Monitoraggio di stazioni di lavoro

Con il monitoraggio delle stazioni di lavoro di si possono individuare immediatamente e risolvere rapidamente problemi periodici delle stazioni di lavoro, garantendone la disponibilità ottimale per tutti gli utenti e mantenendo il regolare svolgimento dell'attività aziendale.

Monitoraggio del sistema di backup

Il servizio effettua il monitoraggio sul regolare funzionamento del sistema di gestione delle copie di sicurezza e del backup prevenendo eventuali anomalie ed evitando improvvise perdite di dati.

Gestione di patch

Gli strumenti di gestione patch ottimizzano l'automatizzazione e gestione degli aggiornamenti software e delle patch di Microsoft

Creazione di report

Gli strumenti per la generazione di rapporti (o report) producono rapporti professionali e grafici utilizzabili per individuare l'andamento delle prestazioni del sistema e dimostrare ai clienti la necessità di aggiornamenti o sostituzioni.



Allegati

Mini glossario sulla Privacy

Dato personale: qualunque informazione relativa ad un individuo, ad una persona giuridica, ad un ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un numero di identificazione personale.

Dato sensibile: qualunque dato che può rivelare l'origine razziale, l'appartenenza etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti o sindacati, lo stato di salute e la vita sessuale.

Trattamento dei dati personali: qualunque operazione o complesso di operazioni, effettuate anche senza mezzi elettronici o automatizzati (raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione).

Titolare del trattamento: la persona giuridica o fisica cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati.

Informativa: contiene le informazioni che il titolare del trattamento deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è obbligato o meno a rilasciare i dati, quali sono gli scopi e le modalità del trattamento, come circolano i dati e in che modo esercitare i diritti riconosciuti dalla legge.

Consenso: la libera manifestazione della volontà con la quale l'interessato accetta – in modo espresso e, se vi sono dati sensibili, per iscritto - un determinato trattamento di dati che lo riguardano, sul quale è stato preventivamente informato da chi utilizza i dati.

Il Garante: un'Autorità indipendente composta da quattro membri eletti dal Parlamento. È stata istituita per la tutela dei diritti, delle libertà fondamentali e della dignità delle persone rispetto al trattamento dei dati personali. Controlla se il trattamento di dati personali da parte di privati e pubbliche amministrazioni è lecito e corretto. Esamina reclami, segnalazioni e ricorsi, svolge accertamenti anche su richiesta del cittadino, esegue ispezioni e verifiche. Prescrive modifiche necessarie od opportune per far adeguare i trattamenti alla disciplina vigente. Segnala al Parlamento e al Governo l'opportunità di interventi normativi per tutelare gli interessati. Esprime pareri su regolamenti e atti amministrativi di alcune amministrazioni pubbliche. Presenta al Parlamento e al Governo una relazione annuale sullo stato di attuazione della normativa che regola la materia.

Tratto dalla brochure del Garante per la protezione dei dati personali: "[La tutela dei dati personali: il primo Garante sei tu](#)".⁸

⁸ <http://www.garanteprivacy.it/garante/document?ID=1382763>



Esempio di autocertificazione

Dichiarazione sostitutiva di atto di notorietà (Art.47 D.P.R. 28 dicembre 2000, n.445)

Il Sottoscritto/a nato a [M] [F] Prov..... ilResidente aProv. Indirizzo N. ... in qualità di legale rappresentante /titolare della ditta individuale / società /ente con sede legale in p.iva Titolare del trattamento di dati personali effettuato ai sensi del D.lgs 196/2003.

Nella propria qualità di rappresentante del titolare / titolare del trattamento in conformità agli artt. 4 e 28 del D.lgs 196/03, "Codice in materia di protezione dei dati personali" redige la presente .

consapevole delle sanzioni penali richiamate dall'art.76 del d.P.R. 28.12.2000 n.445, in caso di dichiarazioni mendaci e di formazione o uso di atti falsi e dell'art. 168 D.lgs 196/2003

Dichiara

di rientrare nella tipologia indicata dall'art. 29 della legge n. 133 del 6 agosto 2008 ed in particolare di effettuare trattamenti di soli dati non sensibili e che l'unico dato sensibile è costituito dallo stato di salute o malattia dei propri dipendenti ovvero dall'adesione ad organizzazioni sindacali od a carattere sindacale.

Il Sottoscritto inoltre dichiara di aver provveduto a:

- definire la finalità del trattamento dei dati
- definire la modalità del trattamento dei dati
- definire gli strumenti utilizzati per il trattamento dei dati
- definire i profili di sicurezza

a tale scopo ha provveduto alla:

- individuazione in forma scritta degli incaricati al trattamento dei dati
- predisposizione delle misure minime di sicurezza ai sensi del D.lgs 196/2003
- vigilanza sulla corretta osservanza degli obblighi di legge e dei diritti riconosciuti dalla legge
- formazione del personale relativamente alle disposizioni previste dal Codice in materia di protezione dei dati personali

Il Sottoscritto dichiara infine:

- di effettuare trattamento di dati personali in modo lecito e corretto per scopi determinati, espliciti e legittimi legati alla propria attività di
- di trattare esclusivamente dati personali di tipo "comune" di clienti, fornitori, dipendenti, (altro)
- dati personale di tipo "sensibile" dei dipendenti esclusivamente relativi allo stato di salute o malattia senza indicazione della relativa diagnosi ovvero dall'adesione ad organizzazioni sindacali od a carattere sindacale.

I descritti trattamenti sono effettuati per fini legati:

1. all'esecuzione di obblighi derivanti da contratto nel quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
 2. all'espletamento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria, compresi gli obblighi in materia di gestione del rapporto di lavoro;
- in relazione a trattamenti effettuati per correnti finalità di amministrative e contabili sottraendosi pertanto all'obbligo di redazione del Documento Programmatico sulla Sicurezza così come previsto dall'art. 34 bis D.lgs 196/2003.

Esente da imposta di bollo ai sensi dell'art. 37 D.P.R. 28 dicembre 2000, n. 455

Data Firma Titolare (non autenticata)



Esempio di Lettera d'incarico per amministratore di sistema esterno**OGGETTO: NOMINA DI AMMINISTRATORE DI SISTEMA**

Ai sensi del "provvedimento" del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008, Il sottoscritto [**NOMINATIVO DEL TITOLARE TRATTAMENTO DATI**], in qualità di **titolare dello studio / azienda [DATI IDENTIFICATIVI]** e del trattamento dei dati personali ai sensi del D.Lgs. 196/2003, dato il rapporto di lavoro in essere e la documentata esperienza pluriennale nella gestione di sistemi informatici

nomina

La società Archimedia come amministratore di sistema.

Archimedia per svolgere il proprio lavoro potrà avvalersi del proprio personale adeguatamente preparato e specializzato per le attività richieste e svolgerà il proprio mandato presso **lo studio professionale / Azienda** come sopra identificato secondo le modalità e con gli strumenti tecnici messi a disposizione dal titolare e dal responsabile del trattamento.

- Come amministratore di sistema avrà il compito di generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dati, nel rispetto delle massime misure di sicurezza.
- Dovrà, inoltre, adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal D.lgs.196/2003 ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware.
- L'incaricato ha il compito di controllare periodicamente l'efficienza dei sistemi tecnici adottati e di 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.
- Prenderà tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up.
- Predisporrà la disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 mesi.
- Indicare al personale competente come effettuare la distruzione e lo smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego.
- Dovrà, inoltre, provvedere alla nomina di uno o più Custodi delle password a cui conferire il compito di custodire le parole chiave o password per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.
- predisporrà sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte Sua (nella sua qualità di "amministratore di sistema"); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le ricordiamo, che il provvedimento del Garante già citato, obbliga il titolare del trattamento alla "verifica" almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

La preghiamo di restituirci copia della presente, firmata per accettazione e per ricevuta della documentazione di cui sopra.

Il titolare del trattamento

_____, il _____

La preghiamo di sottoscrivere la presente per presa visione di quanto riportato.

_____, il _____

PER ARCHIMEDIA

Sig. _____



Esempio di Lettera d'incarico per amministratore di sistema interno**NOMINA DELL'AMMINISTRATORE DI SISTEMA**

(Pur non essendo più prevista dal D. Lgs. n. 196/2003, questa figura è molto importante ed è bene configurarla come un vero e proprio "responsabile", che può essere anche il "responsabile per le misure di sicurezza per la privacy")

Egr. Sig.

Oggetto: Nomina ad "amministratore del sistema informativo"

In relazione al rapporto di lavoro/di collaborazione con Lei in essere, considerando che per preparazione ed esperienza Lei fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali, con la presente Le conferiamo il compito di sovrintendere alle risorse del sistema informativo dello Studio legale e di consentirne l'utilizzazione.

In tale contesto sarà Suo compito:

- individuare per iscritto il/i soggetto/i incaricato/i della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla sua attività;
- individuare per iscritto gli altri soggetti, diversi dal/dagli incaricato/i della custodia delle parole chiave, che possono avere accesso ad informazioni che concernono le medesime;
- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 1 a 10 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 12 a 14 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- verificare costantemente che la nostra Società abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dall'art. 34 del D. Lgs. n. 196/2003, e dal Disciplinare tecnico, allegato B) al decreto legislativo medesimo, provvedendo senza indugio agli adeguamenti eventualmente necessari;
- suggerire al titolare del trattamento l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a realizzare quanto previsto dall'art. 31 del D. Lgs. n. 196/2003, che dispone che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- curare, su incarico del titolare del trattamento, l'adozione e l'aggiornamento delle misure "idonee" di cui al punto precedente;
- attivare e aggiornare con cadenza almeno semestrale idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo a Lei affidato, contro il rischio di intrusione e contro l'azione dei virus informatici;
- aggiornare periodicamente, con frequenza almeno annuale (*oppure semestrale se si trattano dati sensibili o giudiziari*), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- predisporre ed aggiornare, entro il 31 marzo di ogni anno, il documento programmatico sulla sicurezza previsto dal punto 19 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;

(Nota Bene: la redazione di tale documento è obbligatoria solo nei casi in cui si trattano dati sensibili e/o di carattere giudiziario con elaboratori elettronici; negli altri casi, in cui non vi è tale obbligo, è comunque

consigliabile prevedere la redazione e l'aggiornamento del D.P.S., che consente di tenere agevolmente sotto controllo le misure minime di sicurezza obbligatorie)

- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate in azienda.

Sarà Suo compito riferire periodicamente, ed in ogni caso con cadenza mensile, all'Amministratore Delegato della nostra Società/al titolare del trattamento (Avv. _____) sullo svolgimento dei Suoi compiti, dandogli inoltre piena collaborazione nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate aziendalimente.

Al fine di una migliore comprensione dei Suoi compiti specifici relativi alla corretta e sicura gestione del sistema informativo aziendale, alleghiamo alla presente il testo dell'art. 34 del D. Lgs. n. 196/2003, e del Disciplinare tecnico, allegato B) al decreto legislativo medesimo.

La preghiamo di restituirci copia della presente, firmata per accettazione e per ricevuta della documentazione di cui sopra.

Distinti saluti.

Data, _____

Firma della Società/Titolare del trattamento

Per ricevuta ed accettazione _____ (data e firma)



Estratto del provvedimento del garante relativo agli amministratori di sistema ed alla registrazione degli accessi

4. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici

Di seguito sono indicati gli accorgimenti e le misure che vengono prescritti ai sensi dell'art. 154, comma 1, lett. c) del Codice, a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici, esclusi, allo stato, quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; [Provv.](#) Garante 6 novembre 2008).

I seguenti accorgimenti e misure lasciano impregiudicata l'adozione di altre specifiche cautele imposte da discipline di settore per particolari trattamenti o che verranno eventualmente prescritte dal Garante ai sensi dell'art. 17 del Codice.

Per effetto del presente provvedimento:

4.1 Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

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.

4.2 Designazioni individuali

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.

4.3 Elenco degli amministratori di sistema³

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal [provvedimento](#) del Garante n. 13 del 1° marzo 2007 (in *G.U.* 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., *intranet* aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo differente uno specifico settore.

Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

4.4 Verifica delle attività³

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

4.5 Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

5. Tempi di adozione delle misure e degli accorgimenti

Per tutti i titolari dei trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, le misure e gli accorgimenti di cui al punto 4 dovranno essere introdotti al più presto e comunque entro, e non oltre, il termine che è congruo stabilire, in centoventi giorni dalla medesima data.