SOMMARIO

Avvertenza: i modelli rappresentano delle tracce predisposte in conformità alle disposizioni del Codice in materia di protezione dei dati personali: tuttavia vanno sempre verificati e personalizzati alle effettive esigenze della singola impresa.

Modelli e tabelle per la guida sulla privacy in azienda

MODELLI - RAPPORTI CON L'INTERESSATO

CONSENSO INFORMATO DIPENDENTI

Per la corretta gestione del rapporto di lavoro in base al Codice sulla privacy, l'azienda deve assolvere ai due obblighi fondamentali che la stessa legge impone a tutela dell'interessato:

- *informare compiutamente il dipendente sui trattamenti che si intendono effettuare e chiedere, di conseguenza, un consenso consapevole.*

Il modello di informazione e consenso per i dipendenti presenta alcune peculiarità.

- *consenso informato dei familiari: per alcuni trattamenti contributivi e previdenziali si possono trattare anche dati dei familiari del dipendente dei quali dovrà essere acquisito il consenso informato mediante sottoscrizione del modulo;*
- *consenso scritto: nel rapporto di lavoro si possono trattare dati sensibili per i quali è necessario acquisire un consenso scritto;*

I trattamenti descritti nel modello riportato di seguito si riferiscono esclusivamente a quelli necessari in base alle norme vigenti per la gestione del rapporto di lavoro. I trattamenti di dati "particolari" (quelli sensibili e giudiziari), inoltre, sono conformi alle autorizzazioni generali periodiche che il Garante ha emanato in materia e che elencano i trattamenti autorizzati.

Si sottolinea, peraltro, che il Codice ammette il trattamento dei dati sensibili anche senza il consenso dell'interessato, (rispettando sempre le autorizzazioni generali del Garante), solo in alcuni casi tassativi, tra i quali, "quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del Codice di deontologia e di buona condotta di cui all'articolo 111" (art. 26 – 4°comma, lett. d del codice) .

Modello di consenso informato per i lavoratori dipendenti

Egr. Sig./Gent.ma Sig.ra

La scrivente Società comunica che, per l'instaurazione e la gestione del rapporto di lavoro con Lei in corso, è titolare di dati Suoi e dei Suoi familiari (1) qualificati come dati personali ai sensi del Codice in materia di protezione dei dati personali (d. lgs.vo 30.6.2003 n. 196).

1) La informiamo, pertanto, che tali dati verranno trattati con il supporto di mezzi cartacei, informatici o telematici:

- per l'eventuale assunzione, laddove questa non sia già intervenuta;
- per l'elaborazione ed il pagamento della retribuzione;
- per l'adempimento degli obblighi tutti legali e contrattuali, anche collettivi, connessi al rapporto di lavoro;
- .....

2) Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità per l'azienda di dare esecuzione al contratto o di svolgere correttamente tutti gli adempimenti, quali quelli di natura retributiva, contributiva, fiscale e assicurativa, connessi al rapporto di lavoro (2).

3) Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati in Italia e trasferiti all'estero (3) esclusivamente per le finalità sopra specificate a:

- Enti pubblici (INPS, INAIL, Direzione provinciale del lavoro, Uffici fiscali...);

- Fondi o casse anche private di previdenza e assistenza;
- Studi medici in adempimento degli obblighi in materia di igiene e sicurezza del lavoro;
- Società di assicurazioni;
- Istituti di credito;
- Organizzazioni sindacali cui lei abbia conferito specifico mandato;
- Fondi integrativi;
- Organizzazioni imprenditoriali cui aderisce l'azienda;
- ..... *(completare con tutte le categorie di soggetti esterni cui si comunicano i dati per le finalità indicate).*

Inoltre, nella gestione dei suoi dati possono venire a conoscenza degli stessi le seguenti categorie di incaricati e/o responsabili interni ed esterni individuati per iscritto ed ai quali sono state date specifiche istruzioni scritte:

- dipendenti dell'ufficio del personale;
- titolari e dipendenti della società di elaborazione della paghe, in qualità di incaricati o responsabili esterni *(se nominati)*;
- professionisti o società di servizi per l'amministrazione e gestione aziendale che operino per conto della nostra azienda;
- ……..

Relativamente ai dati medesimi potrete esercitare i diritti previsti dall'art. 7 del d.lgs.vo n. 196/2003 (di cui viene allegata copia) nei limiti ed alle condizioni previste dagli articolo 8, 9 e 10 del citato decreto legislativo;

4) In relazione al rapporto di lavoro, l'azienda potrà trattare dati che la legge definisce "sensibili" in quanto idonei a rilevare ad esempio:

a) uno stato generale di salute (assenze per malattia, maternità, infortunio o l'avviamento obbligatorio) idoneità o meno a determinate mansioni (quale esito espresso da personale medico a seguito di visite mediche preventive/periodiche o richieste da Lei stesso/a);
b) l'adesione ad un sindacato (assunzione di cariche e/o richiesta di trattenute per quote di associazione sindacale), l'adesione ad un partito politico o la titolarità di cariche pubbliche elettive (permessi od aspettativa), convinzioni religiose (festività religiose fruibili per legge);
c) ..... *(eventuali altri trattamenti su dati sensibili, sempre strettamente pertinenti all'esecuzione del rapporto di lavoro.*

(*N.B.: si ricorda che i trattamenti di dati sensibili e giudiziari individuati devono essere ricompresi tra i trattamenti e le finalità previste dai provvedimenti generali di autorizzazione emessi dal Garante per disciplinare i trattamenti di questi dati effettuabili nei rapporti di lavoro*).

I dati di natura sensibile, concernenti lo stato di salute, che tratta il medico competente nell'espletamento dei compiti previsti dal D.Lgs.vo n. 626/1994 e dalle altre disposizioni in materia di igiene e sicurezza nei luoghi di lavoro, per l'effettuazione degli accertamenti medici preventivi e periodici, verranno trattati presso il datore di lavoro esclusivamente dallo stesso medico quale autonomo titolare del trattamento, per il quale la società chiede espresso consenso(4). I soli giudizi sull'inidoneità verranno comunicati dal medico allo stesso datore di lavoro.

5) Tutti i dati predetti e gli altri costituenti il Suo stato di servizio verranno conservati anche dopo la cessazione del rapporto di lavoro per l'espletamento di tutti gli eventuali adempimenti connessi o derivanti dalla conclusione del rapporto di lavoro stesso **(5)**.

6) Titolare del trattamento dei Suoi dati personali è ..... *(indicare la denominazione o ragione sociale dell'azienda e relativa sede).* Responsabile/i del trattamento dei suoi dati è/sono ..... *(da riportare qualora in azienda sono stati nominati uno o più responsabili -interni od esterni- del trattamento dei dati personali relativi ai dipendenti)* ***(6)****.*

Data .....

Timbro e firma azienda
.....

****

Il/I sottoscritto/i (1) in calce identificato/i dichiara/no di aver ricevuto completa informativa ai sensi dell'art. 13 del decreto legislativo 196/2003, unitamente a copia dell'art. 7 del decreto medesimo, ed esprime/ono il consenso al trattamento ed alla comunicazione dei propri dati qualificati come personali dal citato decreto con particolare riguardo a quelli cosiddetti sensibili nei limiti, per le finalità e per la durata precisati nell'informativa.

Data .....

(1)
COGNOME NOME REL. DI PARENTELA FIRMA

---

(1) Da inserire quando si trattino anche dati relativi ai familiari (ad esempio assegni per il nucleo familiare, permessi per assistenza ai familiari, ecc....). Il consenso deve essere sottoscritto dai familiari maggiorenni.

(2) Qualora il conferimento di alcuni dati non sia obbligatorio per legge o per contratto è necessario precisare la natura facoltativa, le finalità specifiche, nonché le conseguenze del mancato conferimento. Per il trattamento dei dati sensibili necessari alla gestione del rapporto di lavoro in assenza del consenso si rinvia all'art. 26-4°comma, lett.d.

(3) Mentre in ambito UE non è necessario il consenso, esso legittima sempre il trasferimento dei dati in ambito extra UE. È opportuno quindi precisare se il trasferimento dei dati riguarda i paesi UE, o quelli extra UE. Peraltro il Codice prevede anche alcune ipotesi di esonero dal consenso (artt. 43 e 44) anche attraverso autorizzazioni emanate dal Garante: le attuali autorizzazioni riguardano Ungheria, Svizzera, Canada; per gli USA il Garante si è richiamato all'accordo cosiddetto "safe harbor") Il Garante ha, inoltre, emanato delle clausole contrattuali-tipo per il trasferimento dei dati all'estero che permettono il trasferimento senza consenso.

(4) Da inserire nei casi in cui vi siano dipendenti sottoposti a sorveglianza sanitaria ai sensi della normativa vigente. In questo modello il medico (da identificare) è qualificato quale titolare autonomo del trattamento. Pertanto, in questo modello, si chiede il consenso per suo conto. In alternativa dovrà richiederlo direttamente il medico (secondo un modello riportato di seguito); in ulteriore alternativa potrebbe essere qualificato quale responsabile del trattamento (predisponendo in tal caso lo specifico atto di nomina riportato tra la modulistica).

(5) L'art. 11, lett. e del Codice precisa che i dati vanno conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati.

(6) Nel caso di nomina di più responsabili, il Codice ha introdotto la facoltà di indicare nell'informativa un solo responsabile (se è designato quello competente a ricevere e gestire le richieste dell'interessato di esercizio dei diritti previsti dall'art. 7). In tal caso la norma precisa che deve essere anche indicato "il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili".
Nel caso di trattamento da parte di un titolare stabilito in un altro stato, ma che utilizza strumenti situati in Italia, l'art. 5 impone di designare un "rappresentante stabilito nel territorio dello Stato" da indicare anche nell'informativa.

CONSENSO INFORMATO RICHIESTO DAL MEDICO COMPETENTE

Nell'azienda vi possono essere dipendenti sottoposti a sorveglianza sanitaria in base alla normativa vigente.

Per questi dipendenti è quindi necessario che il consenso informato comprenda anche questo particolare trattamento di dati (anche sensibili) compiuto dal medico competente.

Qualora non si voglia utilizzare il modello generale di consenso informato per i dipendenti, ma si preferisca separare questo consenso informato, si può utilizzare il modello riportato di seguito. Il medico competente è indicato quale "titolare del trattamento".

Questo modello dovrà essere predisposto direttamente dal medico competente qualora egli adempia agli obblighi previsti dalla normativa sulla sicurezza nella gestione di un contratto di somministrazione di lavoro di cui agli artt. 20 e ss del d.lgs.vo. 276/2003

Modello di consenso informato richiesto dal medico competente per i lavoratori dipendenti sottoposti a sorveglianza sanitaria

---

Egr. Sig./Gent.ma Sig.ra

Lo scrivente dott. ....., nominato medico competente dal Suo datore di lavoro (*utilizzatore nel caso di contratto di somministrazione*) per lo svolgimento dei compiti previsti dal D.Lgs.vo n. 626/1994, comunica che, nell'espletamento dei compiti di sorveglianza sanitaria, è titolare (1) di Suoi dati qualificati come dati personali ai sensi del Codice in materia di protezione dei dati personali (d. lgs.vo n. 196/2003).

1) La informiamo, pertanto, che tali dati verranno trattati con il supporto di mezzi cartacei, informatici o telematici *(indicare le esatte modalità di trattamento utilizzate)* per effettuare, in conformità alle norme di legge, la sorveglianza sanitaria prevista dall'art. 16 del d.lgs.vo n. 626/1994.

2) Il conferimento dei dati è obbligatorio per l'attuazione degli obblighi previsti dal d.lgs.vo n. 626/1994, e pertanto l'eventuale rifiuto a fornirli, in tutto o in parte, può dar luogo all'impossibilità per il medico competente di svolgere i compiti affidatigli dal datore di lavoro (*o utilizzatore*)in conformità allo stesso decreto legislativo.

3) Ferme restando le comunicazioni agli organi sanitari e di controllo competenti eseguite in adempimento di specifici obblighi di legge, l'esito complessivo, riferito all'idoneità alla mansione, verrà comunicato per iscritto al datore di lavoro (*o utilizzatore)* ed allo stesso dipendente interessato.

Relativamente ai dati medesimi potrete esercitare i diritti previsti dall'art. 7 del d.lgs.vo n. 196/2003 (di cui viene allegata copia) nei limiti ed alle condizioni previste dagli articolo 8, 9 e 10 del citato decreto legislativo**;**

4) Il sottoscritto medico competente potrà trattare dati che la legge definisce "sensibili" in quanto idonei a rilevare lo stato di salute nell'espletamento dei compiti assegnati dal d.lgs.vo n. 626/1994, e specificatamente nell'effettuazione di:

- accertamenti preventivi sull'idoneità alla mansione specifica;
- accertamenti periodici per controllare lo stato di salute del dipendente ed esprimere il giudizio di idoneità alla mansione specifica;

5) Tutti i dati predetti verranno conservati sotto la esclusiva e diretta responsabilità dello stesso medico competente mediante l'istituzione di una cartella sanitaria e di rischio custodita presso il datore di lavoro (*o utilizzatore).*

6) I dati della cartella sanitaria, dopo la risoluzione del rapporto di lavoro, verranno consegnati in copia al dipendente e, nei casi previsti (2) consegnati in originale all'ente competente.

Data .....

Firma del medico competente

.....

****

Il sottoscritto in calce identificato dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del decreto legislativo n. 196/2003, unitamente a copia dell'art. 7 della Legge medesima, ed esprime il consenso (3) al trattamento ed alla comunicazione dei propri dati qualificati come personali dal citato decreto con particolare riguardo a quelli cosiddetti sensibili nei limiti, per le finalità e per la durata precisati nell'informativa.

Data .....

Firma

.....

Modello di consenso informato da predisporre a cura del medico competente nei casi in cui vi siano dipendenti sottoposti a sorveglianza sanitaria ai sensi della normativa vigente.

(1) Nel presente modello il medico competente è qualificato quale titolare del trattamento; qualora si voglia qualificarlo, invece, responsabile del trattamento effettuato dall'azienda datore di lavoro, è necessario predisporre uno specifico atto di nomina del medico (riportato tra i modelli), in alternativa a questo modello di consenso informato, ed integrare in tal senso il modello generale di consenso informato per i dipendenti.

(2) Per l'esposizione agli agenti cancerogeni e agli agenti biologici, è prevista la consegna degli originali all'Ispesl competente.

(3) Per il trattamento dei dati sensibili necessari alla gestione del rapporto di lavoro, anche in materia di igiene e sicurezza, in assenza del consenso si rinvia all'art. 26-4°comma, lett.d.

CONSENSO INFORMATO PER CLIENTI E FORNITORI

I dati dei clienti e fornitori costituiscono "dati personali" ai fini Codice per la protezione dei dati personali: infatti, la legge italiana sulla privacy definisce dati personali anche le informazioni su persone giuridiche, enti ed associazioni (art. 4 1°comma, lett.b).

Di conseguenza nei confronti dei clienti e fornitori l'azienda dovrà adempiere agli obblighi di legge posti a tutela dell'interessato di cui si trattano i dati: l'informativa completa sui trattamenti che si effettuano e la richiesta di consenso espresso al trattamento.

Il modello riportato di seguito si riferisce ai trattamenti strettamente inerenti all'esecuzione dei contratti in corso ed all'assolvimento degli obblighi fiscali relativi al rapporto. Gli adempimenti di informativa e consenso possono essere assolti sia utilizzando un modello a sé stante, sia inserendo in documenti contrattuali (condizioni generali di contratto, ordini, conferme d'ordine …) una clausola apposita sulla privacy "clausola privacy".

Modello di informativa e consenso per clienti e fornitori*

Spett.Ditta/Società

La scrivente Società informa che per l'instaurazione e l'esecuzione dei rapporti contrattuali con voi in corso è in possesso di dati anagrafici e fiscali (1)acquisiti anche verbalmente direttamente o tramite terzi, a voi relativi, dati qualificati come personali dalla legge.

Con riferimento a tali dati vi informiamo che:

- i dati vengono trattati in relazione alle esigenze contrattuali ed ai conseguenti adempimenti degli obblighi legali e contrattuali dalle stesse derivanti nonché per conseguire una efficace gestione dei rapporti commerciali (2).

  I dati verranno trattati in forma scritta e/o su supporto magnetico, elettronico o telematico;
- il conferimento dei dati stessi è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli o al successivo trattamento potrà determinare l'impossibilità della scrivente a dar corso ai rapporti contrattuali medesimi;
- il mancato conferimento, invece, di tutti i dati che non siano riconducibili ad obblighi legali o contrattuali verrà valutato di volta in volta dalla scrivente e determinerà le conseguenti decisioni rapportate all'importanza dei dati richiesti rispetto alla gestione del rapporto commerciale;
- ferme restando le comunicazioni e diffusioni effettuate in esecuzione di obblighi di legge, i dati potranno essere comunicati in Italia e/o all'estero (3) a:
- nostra rete di agenti
- società di factoring
- istituti di credito
- società di recupero crediti
- società di assicurazione del credito
- società di informazioni commerciali
- professionisti e consulenti,
- aziende operanti nel settore del trasporto;
- ..... (*completare con tutte le altre categorie di soggetti cui si comunicano i dati per le finalità indicate*)
- ai soli fini della tutela del credito e della migliore gestione dei nostri diritti relativi al singolo rapporto commerciale (4); per le medesime finalità i dati potranno venire a conoscenza delle seguenti categorie di incaricati e/o responsabili:

  ……
- i dati verranno trattati per tutta la durata dei rapporti contrattuali instaurati e anche successivamente per l'espletamento di tutti gli adempimenti di legge nonché per future finalità commerciali;

- relativamente ai dati medesimi la vostra Ditta/Società può esercitare i diritti previsti dall'art**.** 7 del d.lgs.vo n. 196/2003 (di cui viene allegata copia) nei limiti ed alle condizioni previste dagli articolo 8, 9 e 10 del citato decreto legislativo;
- titolare del trattamento dei dati è la nostra Società (indicare denominazione/ragione sociale e sede);
- responsabile del trattamento (5) dei suoi dati personali è ... *(solo se designato indicare nominativo e qualifica se persona fisica, denominazione e sede se impresa)* che ai fini della presente legge ha il seguente indirizzo ..... .

Data .....
Firma .....

** "Clausola privacy":*

La modulistica relativa all'informativa ai clienti/fornitori (ed all'eventuale consenso) naturalmente può essere inserita in documenti contrattuali o precontrattuali (condizioni generali di contratto, ordini, conferme d'ordine ...).

Fac-simile di consenso per fornitori e clienti (6)

La scrivente Ditta/Società dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 d.lgs.vo. 196/2003 unitamente a copia dell'art. 7 del decreto medesimo, ed esprime il consenso al trattamento ed alla comunicazione dei propri dati qualificati come personali dalla citata legge nei limiti, per le finalità e per la durata precisati nell'informativa.

Data .....

Timbro e firma del fornitore/cliente (*legale rappresentante*)
.....

(1) L'art. 13 – 4°comma del codice, nel caso di dati raccolti presso terzi, impone di indicare anche le "categorie di dati trattati" nell'informativa all'interessato.

(2) individuare eventuali ulteriori finalità specifiche (ad esempio marketing, promozionali, statistici e di controllo qualità, affidamenti ....); per le comunicazioni commerciali,promozionali, pubblicitarie, di vendita diretta effettuate mediante telefax, e-mail, sms, mms, l'art. 130 detta regole particolari.

(3) La parola "all'estero" è da inserire solo se sussiste la necessità (v. art. 44 del decreto e art. 43, lett. h per l'esonero dall'obbligo per i dati relativi alle persone giuridiche);

(4) è necessario, in base alle indicazioni dell'Autorità Garante, individuare analiticamente tutte le categorie di soggetti cui potranno essere comunicati i dati ed anche le relative finalità di comunicazione.

Si può, eventualmente, anche aggiungere l'ipotesi della diffusione con il relativo ambito;

(5) Nel caso di nomina di più responsabili, il Codice ha introdotto la facoltà di indicare nell'informativa un solo responsabile: se è designato quello competente a ricevere e gestire le richieste dell'interessato di esercizio dei diritti previsti dall'art. 7; in tal caso la norma precisa che deve essere anche indicato "il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili".

(6) Si ricorda che nel trattamento dei "normali" dati di fornitori e clienti per la necessaria esecuzione del contratto non è obbligatorio acquisire il consenso.

Infatti gli art. 24 per il trattamento elenca una serie di ipotesi in cui non è necessario il consenso dell'interessato, tra questi evidenziamo:

a) dati necessari per l'esecuzione di obblighi derivanti da contratto o per adempiere prima della conclusione del contratto a specifiche richieste dello stesso interessato;

b) dati raccolti e detenuti in base agli obblighi di legge, regolamento o normativa comunitaria;

c) dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

d) dati relativi allo svolgimento di attività economiche dell'interessato;

Questi esoneri **non** si applicano tuttavia al trattamento dei "dati sensibili" che, peraltro, non sono, in via generale, trattati nei rapporti commerciali con clienti e fornitori.

INFORMATIVA PER CLIENTI E FORNITORI

I modelli riportati di seguito contengono la sola informativa ai clienti e fornitori e sono proposti nella forma di clausole sintetiche.

L'assenza della richiesta di consenso al trattamento si basa sulle ipotesi di esonero previste dall'art. 24

(soprattutto alle lettere a, b e d) del Codice sulla privacy.

La sussistenza di questi casi – tassativi- di esonero dal consenso deve essere verificata con attenzione.

Per le comunicazioni commerciali,promozionali, pubblicitarie, di vendita diretta effettuate mediante telefax, e-mail, sms, mms, l'art. 130 detta regole particolari, condizionando (4°comma) l'esonero dal consenso a precise cautele a tutela del cliente.

Modello di sola informativa per clienti e fornitori (*)

Clausola "Tutela dei dati. Decreto legislativo n. 196/2003" per clienti e fornitori

I dati personali anagrafici e fiscali (1)acquisiti direttamente e/o tramite terzi dall'impresa .... *(denominazione e sede),* titolare del trattamento, vengono trattati in forma cartacea, informatica, telematica (2) per esigenze contrattuali e di legge, nonchè per consentire una efficace gestione dei rapporti commerciali.

Gli indirizzi di posta elettronica forniti potranno essere utilizzati dall'impresa per l'invio di materiale pubblicitario relativo a servizi analoghi a quelli oggetto del rapporto commerciale in essere (3).

Il mancato conferimento dei dati, ove non obbligatorio, verrà valutato di volta in volta dall'azienda titolare del trattamento e determinerà le conseguenti decisioni rapportate all'importanza dei dati richiesti rispetto alla gestione del rapporto commerciale.

I dati potranno essere comunicati in Italia e/o all'estero (4), esclusivamente per le finalità sopra indicate e, conseguentemente, trattati solo a tali fini dagli altri soggetti, a:

- nostra rete di agenti
- società di factoring
- istituti di credito
- società di recupero crediti
- società di assicurazione del credito
- società di informazioni commerciali
- professionisti e consulenti,
- aziende che operano nel settore dei trasporti;
- ..... (*completare con tutte le categorie di soggetti cui si comunicano i dati per le finalità dichiarate).*

per le medesime finalità i dati potranno venire a conoscenza delle seguenti categorie di incaricati e/o responsabili:

……

L'interessato potrà esercitare tutti i diritti di cui all'art. 7 del d.lgs.vo n. 196/2003 (tra cui i diritti di accesso, rettifica, aggiornamento, di opposizione al trattamento e di cancellazione).

Responsabile del trattamento (4) è ..... *(da indicare solo se nominato uno specifico responsabile; indicare la qualifica e aggiungere "pro tempore")*.

(1) L'art. 13 – 4°comma del codice, nel caso di dati raccolti presso terzi, impone di indicare anche le "categorie di dati trattati" nell'informativa all'interessato.

(2) In relazione alle modalità di trattamento.

(3) L'articolo 130-4° comma del Codice prevede l'esonero dal consenso in questo caso: l'interessato ha sempre diritto di opporsi all'uso promozionale.

(3) La parola "all'estero" è da inserire solo se sussiste la necessità (v. art. 44 del decreto e art. 43 lett.h per l'esonero dall'obbligo per i dati relativi alle persone giuridiche);

(4) Nel caso di nomina di più responsabili, il Codice ha introdotto la facoltà di indicare nell'informativa un solo responsabile (se è designato quello competente a ricevere e gestire le richieste dell'interessato di esercizio dei diritti previsti dall'art. 7). In tal caso la norma precisa che deve essere anche indicato "il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili".

** "Clausola privacy":*

Anche la modulistica relativa all'informativa ai clienti/fornitori (ed all'eventuale consenso) naturalmente può essere inserita in documenti contrattuali o precontrattuali (condizioni generali di contratto, ordini, conferme d'ordine ... ***) in forma di clausola in cui, sinteticamente, si riportano gli elementi dell'informativa.***

INFORMATIVA PER CLIENTI E FORNITORI IN INGLESE

Il Codice sulla privacy si applica a tutti i trattamenti effettuati in territorio italiano di dati personali: pertanto l'azienda è tenuta a rispettare l'obbligo di informativa anche nei riguardi di clienti e fornitori stranieri (comunitari od extracomunitari).

Il modello riportato contiene una traduzione in inglese dell'informativa standard.

Modello di sola informativa in inglese per clienti e fornitori

"Personal Data Protection - Law n.196/2003 - Clause for clients and suppliers"

Personal data collected directly and/or through third parties by the controller .....(1), are processed in printed, computing and telematic form (2) for the performance of contractual and lawful obligations as well as for the effective handing of business relations, also for future use.

The non-submittal of data, where not compulsory, will be evaluated from time to time by the controller and the resulting decisions to be made will take into account the importance of the requied data in respect of the business relation management.

Data may be disclosed, strictly in accordance with the above-mentioned purposes, and consequently processed, only in relation to the said purpose, by the other subjects (3):

- our agents organization
- factoring companies
- banks
- credit recovery companies
- credit insurance company
- business information companies
- professional and consultants
- ..... *(completare con tutte le categorie di soggetti cui si comunicano i dati per le finalità indicate)*

In relation to the same purposes, data may be processed by the following classes of executors or processors: **.....**

The data subjects may exercise all the rights set forth in art.7 of L.n.196/2003 (including the rights of data access, updating, objects to data processing and cancellation)

The processor is ..... (4)

(1) Denominazione e sede

(2) In relazione alle modalità di trattamento

(3) La parola "all'estero" è da inserire solo se sussiste la necessità (v. art. 44 del decreto e art. 43 lett.h per l'esonero dall'obbligo per i dati relativi alle persone giuridiche);

(4) Da indicare solo se nominato uno specifico responsabile; specificare anche la qualifica e aggiungere preferibilmente "pro-tempore"

Nel caso di nomina di più responsabili, il Codice ha introdotto la facoltà di indicare nell'informativa un solo responsabile (se è designato, quello competente a ricevere e gestire le richieste dell'interessato di esercizio dei diritti previsti dall'art. 7); in tal caso la norma precisa che deve essere anche indicato "il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili".

ATTIVITA' DI MARKETING

Premessa
In generale, l'art. 7- 4°comma, lett.b) del Codice precisa che l'interessato ha il diritto di opporsi, comunque, al trattamento ai fini di comunicazione commerciale, invio di materiale pubblicitario,di vendita diretta o di ricerca di mercato.
Per l'attività di comunicazione commerciale, l'invio di materiale pubblicitario o di vendita diretta effettuato mediante telefax, posta elettronica, messaggi sms e mms esistono, nella legge sulla privacy, disposizioni particolari.
L'art. 130 del Codice, infatti, impone in questi casi sempre il consenso dell'interessato.
Solo nel caso di utilizzo dell'indirizzo di posta elettronica fornito da un cliente nel contesto di una precedente attività di vendita, a certe condizioni, è possibile non richiedere il consenso dal cliente stesso, comunque debitamente informato; in tal caso, comunque, l'interessato dovrà essere informato in ogni invio di messaggi del diritto di opporsi in ogni momento al trattamento, in maniera agevole e gratuita (art. 130 - 4°comma).

Vi sono, inoltre, altre leggi che, per finalità diverse dalla tutela dei dati personali, dettano particolari disposizioni relative all'attività di marketing:
per i servizi a distanza forniti per posta elettronica, l'art. 9 del d.lgs.vo 9.4.2003 n.70 prevede che il destinatario del messaggio sia informato del diritto di opporsi al ricevimento in futuro di analoghi messaggi;
per la conclusione dei contratti a distanza tra operatori e consumatori, l'art. 10 del d.lgs.vo 22.5.1999 n. 185 impone, nel caso di uso del telefono, di posta elettronica o di fax per le comunicazioni, il consenso preventivo del consumatore.

Modello di informativa e richiesta di consenso per potenziali clienti per l'invio comunicazioni commerciali mediante l'uso di sistemi automatizzati di chiamata senza intervento di operatore, via e-mail, telefax, Mms, Sms.

Per l'attività di comunicazione commerciale, ricerche di mercato, l' invio di materiale pubblicitario o di vendita diretta effettuato mediante telefax, posta elettronica, messaggi sms e mms , l'art. 130 del Codice impone sempre il preventivo consenso dell'interessato (cosiddetto sistema dell'OPT-IN). Inoltre il destinatario dei messaggi deve essere informato del diritto di opporsi, in tutto o in parte, a tale genere di trattamento. Ad esempio, via e-mail è possibile attivare un sistema sensibile di attivazione del consenso che invii automaticamente al mittente il consenso espresso con un semplice click del mouse nello spazio apposito.
L'utilizzo di altri mezzi di comunicazione (la posta cartacea) non necessita invece del preventivo consenso, ma il destinatario dovrà essere informato del diritto di opporsi, in tutto o in parte, a tale genere di trattamento (cosiddetto sistema dell'OPT-OUT).

Spettabile ……..

La nostra società, ... *(denominazione e sede*), avrebbe il piacere di inviarVi comunicazioni commerciali relative ai propri prodotti/servizi del settore …….. mediante l'utilizzo del Vostro indirizzo e-mail (*oppure: al Vostro numero di telefax*)

Nel caso in cui acconsentiate a tale utilizzo dei Vostri dati, Vi ricordiamo che, ai sensi del Codice della Privacy D.lgs n. 196/2003, potrete opporVi in qualsiasi momento al trattamento in oggetto, mediante l'invio di una e-mail al seguente indirizzo …….o l'invio di un telefax al n. ……..

Potrete inoltre esercitare tutti i diritti di cui all'art. 7 del D.lgs.vo n. 196/2003 (tra cui i diritti di accesso, rettifica, aggiornamento e di cancellazione).

Responsabile del trattamento è ..... *(da indicare solo se nominato uno specifico responsabile; indicare la qualifica e aggiungere "pro tempore")* (1).

° ACCONSENTO ° NON ACCONSENTO

---

(1) Nel caso di nomina di più responsabili, il Codice ha introdotto la facoltà di indicare nell'informativa un solo responsabile (se è designato quello competente a ricevere e gestire le richieste dell'interessato di esercizio dei diritti previsti dall'art. 7). In tal caso la norma precisa che deve essere anche indicato "il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili".

Modello di sola informativa per clienti per invio comunicazioni commerciali via coordinate e-mail
già raccolte dal titolare in precedenti rapporti commerciali

Il testo può essere adattato ed inserito nella informativa generale inviata ai clienti o trasformata in "clausola privacy" nei contratti

Nei casi in cui il titolare del trattamento possegga le coordinate di posta elettronica fornite dai propri clienti nel contesto di precedenti vendite di un prodotto o servizio, il Codice della Privacy – art. 130 – prevede che tale coordinate e-mail possano essere utilizzate per l'attività di comunicazione commerciale, l'invio di materiale pubblicitario o di vendita diretta anche senza il preventivo consenso dei clienti in questione a condizione che:

1. *il titolare intenda proporre servizi analoghi a quelli oggetto della precedente vendita;*
2. *l'interessato sia adeguatamente informato, in particolare della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente (cosiddetto sistema OPT-OUT);*
3. *l'interessato non rifiuti tale uso inizialmente o in occasione di successive comunicazioni.*

Gentile Cliente,

ai sensi dell'art. 130, comma 4 del Codice della Privacy, D.lgs. n. 196/2003, le Vostre coordinate di posta elettronica da Voi forniteci nel contesto dei nostri precedenti rapporti commerciali, saranno utilizzate per l'invio di comunicazioni o materiale pubblicitario (*o: per finalità di vendita diretta*).

Titolare del trattamento è la nostra impresa…….. *(denominazione e sede)* e per le finalità sopra indicate i dati suddetti potranno venire a conoscenza delle seguenti categorie di incaricati e/o responsabili:

Ufficio marketing

……

Vi ricordiamo che potrete opporVi in ogni momento al trattamento in oggetto, mediante l'invio di una e-mail al seguente indirizzo e-mail …….. o di un telefax al n. ……. , nonchè esercitare tutti i diritti di cui all'art. 7 del d.lgs.vo n. 196/2003 (tra cui i diritti di accesso, rettifica, aggiornamento, cancellazione. Responsabile del trattamento (4) è ..... *(da indicare solo se nominato uno specifico responsabile; indicare la qualifica e aggiungere "pro tempore")*.

(1) L'articolo 130-4° comma del Codice prevede l'esonero dal consenso in questo caso: l'interessato ha sempre diritto di opporsi all'uso promozionale.

(2) Nel caso di nomina di più responsabili, il Codice ha introdotto la facoltà di indicare nell'informativa un solo responsabile (se è designato quello competente a ricevere e gestire le richieste dell'interessato di esercizio dei diritti previsti dall'art. 7). In tal caso la norma precisa che deve essere anche indicato "il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili".

Marketing verso i clienti mediante posta elettronica.
Avviso sul diritto di opposizione

L'art. 130 – 4°comma, a tutela del cliente destinatario di invii promozionali, pubblicitari e commerciali, oltre a richiedere obbligatoriamente una corretta preventiva informazione allo stesso cliente sulle specifiche finalità di marketing nel trattamento dei dati, impone di informarlo al momento della raccolta ed in occasione dell'invio di ogni comunicazione, del diritto di opporsi in ogni momento al trattamento, in modo agevole e gratuito.
Analogamente (anche se per esigenze diverse dalla tutela della privacy) l'art. 9 del d.lgs.vo 9.4.2003 n.70 precisa che il destinatario di un messaggio deve ricevere l'indicazione che può opporsi al ricevimento in futuro di tali comunicazioni.
Pertanto, è opportuno che nei messaggi e-mail inviati ai clienti, già informati del particolare uso per attività di marketing dei loro dati, contengano sempre un chiaro avviso standard sull'esercizio dei diritti dell'art. 7, e specificatamente sul diritto di opposizione gratuita allo specifico trattamento.

Modello di avviso nelle e-mail al cliente sul diritto di opposizione

In ogni momento l'interessato, destinatario del messaggio, ha diritto di opporsi al trattamento per invio di comunicazioni commerciali, di materiale pubblicitario o di vendita diretta (1), cliccando sul sottostante indirizzo e-mail (2). L'interessato può, inoltre, esercitare tutti i diritti di accesso sui propri dati previsti dall'art.7 del d.lgs.vo n. 196/2003, tra i quali i diritti di rettifica, aggiornamento e cancellazione, inviando un messaggio all'indirizzo ……@ …… .it

(1Individuare quale concreta finalità ricorre.

(2) Con questa modalità tecnica si dovrebbe far partire un messaggio predefinito di richiesta di cancellazione; in alternativa indicare un indirizzo elettronico cui inviare un messaggio di richiesta di cancellazione.

Modello di informazione per potenziali clienti da contattare nell'attività di marketing

I dati identificativi (1) dell'impresa sono stati acquisiti presso elenchi e registri pubblici o comunque documenti conoscibili da chiunque (1) per svolgere in futuro la nostra attività di marketing.

Verranno trattati dall'azienda in forma cartacea e/o informatica o telematica e verranno utilizzati esclusivamente presso la nostra società (2) in relazione alle nostre esigenze, anche future, di acquisizione di nuovi clienti mediante invio di proposte commerciali.

La società garantisce la massima riservatezza nel trattare i dati e la possibilità di richiedere gratuitamente la cancellazione (o la rettifica) dei vostri dati contenuti nel nostro archivio.L'impresa ha facoltà di esercitare tutti i diritti dell'art.7 del d.lgs.vo n.196/2003 ed in particolare di opporsi in tutto od in parte al trattamento (3).

(1) Nel caso di dati personali acquisiti presso terzi (diversi dall'interessato) l'art. 13-4° comma impone di specificare nell'informativa anche la categoria di dati che vengano trattati. In base all'art. 24, lett.c), nel caso di raccolta di dati da elenchi pubblici non è necessario il consenso al trattamento da parte dell'interessato; se i dati vengono, invece, raccolti da altre fonti, vanno specificate, verificando contemporaneamente se si rimane all'interno dei casi in cui è previsto l'esonero dal consenso, secondo lo stesso art. 24. Il Garante ha più volte ricordato che l'acquisizione nella rete internet (solo di fatto accessibile a tutti) degli indirizzi di posta elettronica non ne consente l'utilizzo per fini promozionali e di marketing, in assenza del consenso preventivo dell'interessato (delibera generale del Garante 29.5.2003), anche al fine di evitare il fenomeno dello "spamming".

(2) Qualora si preveda la comunicazione dei dati ad altri soggetti, va modificato il periodo (vedi anche art. 43 per il trasferimento dati all'estero).

(3) L'art. 7-4°comma, lett.b) del Codice precisa che l'interessato ha il diritto di opporsi, comunque, al trattamento ai fini di comunicazione commerciale, invio di materiale pubblicitario,di vendita diretta o di ricerca di mercato.

Modello di clausola per le pubblicità con "coupon" (*)
su riviste (*)

La ditta ..... *(denominazione, ragione sociale)* titolare del trattamento garantisce la massima riservatezza dei dati - facoltativi - forniti che non verranno comunicati a terzi (1) e serviranno esclusivamente (2) per l'invio di materiale illustrativo dei nostri prodotti (*). L'interessato con la compilazione e l'invio del coupon esprime il consenso al trattamento indicato.

Potrà in ogni momento richiedere gratuitamente la rettifica o la cancellazione dal nostro archivio elettronico (3) comunicandolo a ..... *(sede e indirizzo della ditta)* (4).

(1) qualora sia prevista la cessione a terzi va specificato, individuando le relative categorie di terzi.

(2) Naturalmente se le finalità del trattamento sono anche altre e diverse va specificato.

(3) o cartaceo.

(4) L'art. 7, 4°comma lett.b) del Codice impone espressamente di informare l'interessato del suo diritto di opporsi al trattamento ai fini di informazione commerciale o invio di materiale pubblicitario.

(*) Per l'attività di comunicazione commerciale, l' invio di materiale pubblicitario o di vendita diretta effettuato mediante telefax, posta elettronica, messaggi sms e mms esistono disposizioni particolari. L'art. 130 del Codice, infatti, impone in questi casi il consenso dell'interessato. Solo nel caso di utilizzo dell'indirizzo di posta elettronica fornito da un cliente nel contesto dell' attività di vendita, a certe condizioni, è possibile non richiedere il consenso dal cliente stesso, comunque debitamente informato ; in tal caso, comunque, l'interessato dovrà essere informato in ogni invio di messaggi del diritto di opporsi in ogni momento al trattamento, in maniera agevole e gratuita (art.130 - 4°comma).

Per i servizi distanza forniti per posta elettronica, l'art. 9 del d.lgs.vo 9.4.2003 n.70 prevede che il destinatario del messaggio sia informato del diritto di opporsi al ricevimento in futuro di analoghi messaggi.

Per la conclusione dei contratti a distanza tra operatori e consumatori, l'art. 10 del d.lgs.vo 22.5.1999 n. 185 impone, nel caso di uso del telefono, di posta elettronica o di fax per le comunicazioni, il consenso preventivo del consumatore.

Nel caso particolare di trattamento di dati con strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, si rientra in uno dei casi tassativi in cui è ancora obbligatoria la notifica del trattamento al Garante (art. 37, lett.d).

INFORMATIVA PER SISTEMI DI VIDEOSORVEGLIANZA

Anche le immagini ed i suoni che permettono di identificare in modo diretto od indiretto i soggetti interessati costituiscono "dati personali".

Pertanto, anche gli impianti di videosorveglianza installati per ragioni di sicurezza e di tutela del patrimonio aziendale determinano un trattamento di dati per il quale è necessario rispettare i principi e gli obblighi della Codice sulla privacy.

Il Garante per la protezione dei dati personali ha emesso uno specifico provvedimento con il quale ha fornito un "decalogo" delle regole da osservare per non violare la privacy:in attesa del futuro Codice di deontologia e buona condotta in materia (art. 134) è necessario seguire le indicazioni del Garante.

Innanzitutto è necessario fornire agli interessati un'informativa (sia pure sintetica).

Il Garante ha anche ricordato che per questa particolare forma di trattamento permangono le problematiche connesse alla disciplina dei controlli a distanza dettata dall'art. 4 della Legge n. 300/1970 (statuto dei lavoratori), cui rinvia espressamente anche l'art. 114 del codice sulla privacy.

Di seguito si riporta un modello di informativa che può essere realizzata anche mediante cartelli collocati in prossimità delle telecamere o degli accessi all'azienda.

Modello di informativa sui sistemi di videosorveglianza

L'azienda utilizza un sistema di videosorveglianza degli accessi al solo fine di garantire la sicurezza ed il patrimonio aziendale e prevenire atti illeciti.

Le immagini non vengono registrate e sono visionate esclusivamente dal personale addetto alla sorveglianza (oppure: le immagini sono registrate e conservate esclusivamente a cura del personale addetto alla sorveglianza e sono cancellate dopo ….. giorni (1).

Le immagini sono consultabili solo dal personale incaricato o dall'autorità giudiziaria o di polizia.

(1) principio fondamentale (richiamato anche dal Garante) da rispettare nell'utilizzo degli impianti di videosorveglianza è quello di pertinenza e non eccedenza del trattamento (art.11).

Pertanto, è necessario registrare solo le immagini indispensabili (valutando anche la localizzazione delle telecamere) e definire con precisione i tempi di conservazione delle immagini.

CONSENSO INFORMATO PER CURRICULA

Molte imprese organizzano al proprio interno una banca dati per la ricerca del personale.

Anche in tal caso nei confronti degli interessati che si propongono vanno adempiuti gli obblighi di legge relativi all'informativa ed al consenso. In attesa del futuro Codice di deontologia e buona condotta in materia (art. 111) è necessario seguire i principi generali.

È, pertanto, necessario per l'azienda acquisire un consenso informato che legittimi il trattamento dei dati.

Si consiglia, se possibile, di utilizzare un modulo predisposto dall'azienda per omogeneizzare l'informativa da far sottoscrivere all'interessato

Modello di consenso informato per curricula*

**** Il modello di consenso informato può essere opportunamente inserito nelle schede che vengono fatte compilare alle persone che cercano lavoro.***

Egregio Signor .....

La scrivente impresa svolge l'attività di trattamento di dati relativo alle persone che si rivolgono alla stessa azienda alla ricerca di impiego, mediante la compilazione di schede.

Si informa, pertanto, che i dati dalla stessa raccolti a Lei relativi, vengono acquisiti e trattati in forma cartacea e/o su supporto magnetico, elettronico o telematico unicamente al fine di valutare il possibile interesse alla futura costituzione di un rapporto contrattuale da determinarsi nel contenuto; i dati verranno trattati fino ad un massimo di ..... mesi/anni (1), successivamente verranno cancellati, salvo diversa segnalazione dell'interessato.

Il conferimento dei dati stessi pertanto è facoltativo e il suo rifiuto a fornirli ed al successivo trattamento determinerà l'impossibilità per la scrivente di inserire i dati nel proprio archivio e conseguentemente di instaurare eventuali rapporti.

I dati acquisiti verranno trattati esclusivamente per l'attività di ricerca del personale svolta per le proprie esigenze aziendali (2).

Relativamente ai dati medesimi Lei può esercitare i diritti previsti dall'art. 7 del d.lgs.vo n. 196/2003 di cui per Sua opportuna informazione viene consegnata copia.

Titolare del trattamento è ..... *(indicare la denominazione o ragione sociale dell'azienda e relativa sede)*.

Responsabile del trattamento (3) dei Suoi dati personali è ..... *(solo se designato indicare nominativo e qualifica se persona fisica, denominazione e sede se impresa)* che ai fini della presente legge ha il seguente indirizzo .....

Data .....

Firma .....

Fac-simile di consenso per curricula (4) (5)

Il sottoscritto dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del decreto legislativo 196/2003, unitamente a copia dell'art. 7 della legge medesima ed esprime il consenso al trattamento (1) dei propri dati personali anche sensibili qualificati dalla citata legge nei limiti e per le finalità precisati nell'informativa.

Autorizzo inoltre, l'azienda ad effettuare tutti i trattamenti sopra indicati fino a quando ritenuto utile dall'azienda stessa e comunque non oltre alla mia richiesta di cancellazione della banca dati.

Data .....

Firma .....

(1) Appare molto importante, al fine di rispettare il principio di pertinenza alle finalità dichiarate (art.11 lett. e), precisare nell'informativa il termine entro cui l'impresa conserverà i dati del richiedente.

(2) In caso di eventuale comunicazione /diffusione all'esterno dell'azienda va naturalmente mutata l'indicazione dell'ambito di trattamento (finalità ulteriori della banca dati e categoria di soggetti cui comunicare i dati), nonché deve essere richiesto esplicito consenso alla stessa comunicazione o diffusione.

(3) Nel caso di nomina di più responsabili, il Codice ha introdotto la facoltà di indicare nell'informativa un solo responsabile: se è designato quello competente a ricevere e gestire le richieste dell'interessato di esercizio dei diritti previsti dall'art. 7; in tal caso la norma precisa che deve essere anche indicato "il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili".

(4) Il D.P.R. n. 442/2000 sulla disciplina del collocamento detta disposizioni particolari per i "servizi competenti" che svolgono il servizio di collocamento.

(5) Si ricorda alle aziende che ai sensi dell'articolo 9 del d.lgs. 276/2003 coloro che effettuano comunicazione in forma anonima relative ad attività di ricerca e selezione del personale a mezzo stampa, internet, televisione in qualità di potenziali datori di lavoro devono fornire adeguata informativa ai candidati al momento del ricevimento del curriculum. Si suggerisce di far compilare il modello di consenso informato qui sopra riportato e inserito nelle schede standard che ciascuna azienda normalmente predispone per coloro che cercano lavoro. Gli articoli 8 e 9, 2° e 3° comma del citato decreto, inoltre, dispongono norme particolari in materia di privacy per chi svolge professionalmente attività di ricerca del personale per terzi.

NOMINA MEDICO COMPETENTE QUALE RESPONSABILE DEL TRATTAMENTO(*)

Nel modello riportato di seguito il medico competente per la sorveglianza sanitaria viene inquadrato quale responsabile del trattamento dei dati – anche sensibili- che tratta nell'adempimento del suo incarico professionale (in precedenza, invece, è stato riportato il modello di consenso informato al medico competente quale titolare del trattamento)

Modello di nomina del medico competente per i lavoratori dipendenti sottoposti a sorveglianza sanitaria quale responsabile del trattamento

Egr. dr.....

Ai sensi dell'art. 29 del decreto legislativo 196/2003 e delle intese intercorse, e nell'ambito dell'incarico professionale assegnato, Le comunichiamo la nomina a responsabile del trattamento delle banche dati di seguito individuate e di quelle che in futuro le verranno affidate nell'ambito dello stesso incarico quale medico competente per lo svolgimento dei compiti previsti dal D.Lgs.vo n. 626/1994.

Nell'espletamento del suo incarico dovrà attenersi alle disposizioni vigenti disposte dalla legislazione in materia di igiene e sicurezza nei luoghi di lavoro, e specificatamente:

1) I dati personali per i quali Le viene conferito l'incarico potranno essere trattati con il supporto di mezzi cartacei, informatici o telematici *(indicare le esatte modalità di trattamento utilizzate)* per effettuare, in conformità alle norme di legge, la sorveglianza sanitaria prevista dall'art. 16 del D.Lgs.vo n. 626/1994.

2) Ferme restando le comunicazioni agli organi sanitari di controllo competenti eseguite in adempimento di specifici obblighi di legge, i soli giudizi sull'inidoneità verranno da Lei comunicati per iscritto al datore di lavoro ed allo stesso dipendente interessato.

3) In qualità di medico competente potrà trattare anche dati che la legge definisce "sensibili" in quanto idonei a rilevare lo stato di salute nell'espletamento dei compiti assegnati dal D.Lgs.vo n. 626/1994, e specificatamente nell'effettuazione di:

- accertamenti preventivi sull'idoneità alla mansione specifica;
- accertamenti periodici per controllare lo stato di salute del dipendente ed esprimere il giudizio di idoneità alla mansione specifica;

5) Tutti i dati predetti verranno conservati sotto la esclusiva e diretta responsabilità dello stesso medico competente mediante l'istituzione di una cartella sanitaria e di rischio custodita presso il datore di lavoro. Lei dovrà coordinarsi con l'azienda per l'individuazione e l'applicazione delle necessarie misure di sicurezza atte a garantire la riservatezza ed integrità dei dati.

6) Il medico competente deve garantire al dipendente interessato tutti i diritti previsti dall'art. 7 del decreto legislativo 196/2003 e i diritti di informazione previsti dalle norme sull'igiene e la sicurezza nei luoghi di lavoro.

7) I dati della cartella sanitaria, dopo la risoluzione del rapporto di lavoro, dovranno essere consegnati in copia al dipendente, e, nei casi previsti (1), consegnati in originale all'ente competente.

Data .....
Firma del legale rappresentante
.....
Firma del medico per accettazione
.....

(*) Modello di nomina del responsabile del trattamento specifico dei dati sensibili del lavoratore soggetto a sorveglianza sanitaria ai sensi della normativa vigente, da utilizzare qualora il medico **non** venga qualificato titolare del trattamento.

(1) Per l'esposizione agli agenti cancerogeni ed agli agenti biologici è prevista la consegna degli originali all' Ispesl competente.

NOMINA DEL RESPONSABILE DEL TRATTAMENTO INTERNO

La legge prevede la possibilità di individuare, nell'ambito dell'organizzazione aziendale, uno o più soggetti cui l'azienda (titolare del trattamento) delega le funzioni fondamentali ed i relativi poteri per la corretta attuazione degli obblighi di legge e per garantire l'effettuazione di trattamenti leciti e conformi ai principi della stessa legge.

La nomina è, tuttavia, facoltativa: spetta alla singola azienda valutare l'opportunità di creare questa funzione aziendale.

Possono essere individuati anche più responsabili del trattamento, sia all'interno dell'azienda (ripartendo funzioni e poteri per aree aziendali), sia all'esterno (individuando quali responsabili anche società di servizi che svolgono particolari trattamenti per conto dell'azienda) . La figura dell' "amministratore di sistema" richiamata dal dpr n. 318/1999, ora abrogato, potrebbe trovare la propria collocazione nell'organigramma aziendale tra i responsabili del trattamento.

La scelta del responsabile deve cadere su soggetti professionalmente idonei.

In ogni caso sul titolare del trattamento permane un obbligo di vigilanza sull'operato del responsabile.

La nomina deve essere deliberata dal soggetto titolare del relativo potere in base alle norme statutarie (ad es.: consiglio di amministrazione, presidente o amministratore delegato, amministratore unico, socio amministratore …)

Modello di nomina ed istruzioni al responsabile del trattamento

Egregio Sig.....

Ai sensi dell'art. 29 del decreto legislativo 196/2003 ed in base alle intese intercorse, in considerazione delle funzioni da Lei espletate nell'azienda, Le comunichiamo la nomina a responsabile del trattamento delle banche dati di seguito individuate e di quelle che in futuro Le verranno affidate **(1)**(*individuare i trattamenti e le relative banche dati che, rientrando nelle competenze del responsabile vengono a lui affidati)*.

Nel suo incarico dovrà attenersi alle istruzioni impartite... *(individuare le istruzioni necessarie per rispettare tutti gli obblighi della legge compreso il profilo della sicurezza):*

- catalogare analiticamente le banche dati con tutti gli elementi necessari, anche ai fini della eventuale notifica al Garante;
- individuare gli incaricati del trattamento e successivamente diramare le istruzioni scritte necessarie per un corretto, lecito, sicuro trattamento; le istruzioni dovranno essere integrate con le adeguate prescrizioni sulle misure di sicurezza da applicare, definite in base al sistema di sicurezza richiamato più avanti.
- attuare gli obblighi di informazione e acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- ove necessario**,** predisporre la notificazione iniziale e le eventuali successive variazioni verificando l'esattezza e la completezza dei dati contenuti *(se vi sono più responsabili, naturalmente dovrà esservi un coordinamento tra i diversi soggetti per adempiere a questo obbligo)*;
- predisporre la richiesta di autorizzazione preventiva al trattamento di dati sensibili (***caso del tutto eccezionale****: solo quando necessaria*) da inviare al Garante; applicare le disposizioni contenute nelle autorizzazioni generali del Garante relative al trattamento dei dati sensibili e giudiziari in azienda;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del decreto legislativo n.196/2003, in ordine all'accesso ai dato e a tutti i diritti di aggiornamento,rettificazione,cancellazione e di opposizione(*);

- collaborare per l'attuazione delle prescrizioni del Garante;
- predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni dell'art. 31 del decreto legislativo n. 196/2003**,** nonché adeguare il sistema alle norme regolamentari in materia di sicurezza, curandone l'applicazione da parte degli incaricati.(2)

Per l'espletamento dell'incarico assegnato le vengono altresì attribuiti i necessari poteri economici e organizzativi.

---

(1) La nomina di un "responsabile del trattamento" è facoltativa (art**.**29 d.lgs.vo 196/2003). Possono essere nominati anche più responsabili **-**art. 29 3°comma**-** dipendenti od esterni: in tal caso naturalmente vanno individuate le competenze, le aree o le funzioni per le quali ogni singolo responsabile assume l'incarico (ad es. area personale, area informatica, area commerciale, elaborazione paghe…).

(2) La mansione particolare di realizzare e gestire il sistema delle misure di sicurezza può essere attribuita ad un responsabile del trattamento con specifiche competenze in materia di sistemi informatici e misure di sicurezza (nel precedente regolamento sulle misure di sicurezza, tali compiti venivano assegnati all'"**amministratore di sistema**").

(*) Il Codice prevede la facoltà di riportare nell'informativa il solo responsabile designato a ricevere le richieste di accesso,aggiornamento,cancellazione od opposizione (ed in genere di esercizio di tutti i diritti elencati nell'art.7) avanzate dall'interessato: per avvalersi di questa semplificazione è necessario definire quale responsabile (in presenza di più responsabili nominati) è designato a svolgere questa specifica funzione.

NOMINA DEL RESPONSABILE DEL TRATTAMENTO ESTERNO

Modello di nomina del responsabile esterno del trattamento

Spett. Ditta .....

Ai sensi dell'art. 29 del decreto legislativo 196/2003 e delle intese intercorse, e nell'ambito dell'incarico professionale (contratto d'opera, di servizi, appalto….) assegnato, vi comunichiamo la nomina a responsabile del trattamento delle banche dati di seguito individuate e di quelle che in futuro Vi verranno affidate nell'ambito dello stesso incarico professionale (1) (*individuare i trattamenti per i quali si nomina il responsabile: ad es. gestione ed elaborazione paghe)*.

Nel vostro incarico dovrete attenerVi alle istruzioni impartite... *(individuare le istruzioni necessarie per rispettare tutti gli obblighi della legge compreso il profilo della sicurezza):*

- catalogare analiticamente le banche dati con tutti gli elementi necessari, anche ai fini della eventuale notifica al Garante;
- individuare gli incaricati del trattamento e successivamente diramare le istruzioni scritte necessarie per un corretto, lecito, sicuro trattamento; le istruzioni dovranno essere integrate con le adeguate prescrizioni sulle misure di sicurezza da applicare definite in base al sistema di sicurezza richiamato più avanti.
- attuare gli obblighi di informazione e acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- predisporre la notificazione iniziale e le eventuali successive variazioni verificando l'esattezza e la completezza dei dati contenuti *(se l'incarico riguarda solo alcuni trattamenti, la responsabilità per la redazione della notifica e delle successive variazioni dovrà riguardare solo la parte di trattamenti attribuiti al responsabile)*;
- predisporre la richiesta di autorizzazione preventiva al trattamento di dati sensibili (***caso eccezionale***: *solo quando necessaria*) da inviare al Garante; applicare le disposizioni contenute nelle autorizzazioni generali del Garante relative al trattamento dei dati sensibili e giudiziari in azienda;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del decreto legislativo n.196/2003, in ordine all'accesso ai dato e a tutti i diritti di aggiornamento,rettificazione,cancellazione e di opposizione(*);
- collaborare per l'attuazione delle prescrizioni del Garante;
- predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni dell'art. 31 del decreto legislativo n.196/2003, nonché adeguare il sistema alle norme regolamentari in materia di sicurezza, curandone l'applicazione da parte degli incaricati (2).

(1) La nomina di un "responsabile del trattamento" è facoltativa (art.29 d.lgs.vo 196/2003). Possono essere nominati anche più responsabili -art. 29 3°comma- dipendenti od esterni: in tal caso naturalmente vanno individuate le competenze, le aree o le funzioni per le quali ogni singolo responsabile assume l'incarico (ad es. area personale, area informatica, area commerciale, elaborazione paghe…).
Il Codice prevede la facoltà di riportare nell'informativa il solo responsabile designato a ricevere le richieste di accesso,aggiornamento,cancellazione od opposizione (ed in genere di esercizio di tutti i diritti elencati nell'art.**7**) avanzate dall'interessato: per avvalersi di questa semplificazione è necessario definire quale responsabile (in presenza di più responsabili nominati) è designato a svolgere questa specifica funzione.

(2)La mansione particolare di realizzare e gestire il sistema delle misure di sicurezza può essere attribuita ad un responsabile del trattamento con specifiche competenze in materia di sistemi informatici e misure di sicurezza (nel precedente regolamento sulle misure di sicurezza, tali compiti venivano assegnati all'"**amministratore di sistema**").

(*) Il modello di nomina di responsabile esterno può essere opportuno in caso di affidamento a società esterne di alcuni particolari trattamenti e delle relative banche dati (ad es. per la gestione ed elaborazione di paghe) in cui maggiore è l'importanza e la delicatezza del trattamento per la presenza di dati "sensibili".

Trattandosi di responsabile esterno, è opportuno, in relazione all'attuazione delle misure di sicurezza obbligatorie (vedi il disciplinare allegato al Codice), invitare formalmente per iscritto il responsabile ad adottare le misure necessarie a garantire un trattamento sicuro dei dati, e chiederne conferma scritta.

L'alternativa alla nomina di responsabile esterno per quei trattamenti, è l'individuazione di queste società o professionisti esterni quali autonomi titolari di trattamento cui comunicare i dati personali.

ISTRUZIONE AGLI INCARICATI

Il Codice sulla privacy (art. 30) impone all'azienda titolare del trattamento di designare gli "incaricati del trattamento" e di fornire a tutte queste persone incaricate del trattamento delle istruzioni scritte. La designazione e la definizione delle istruzioni viene compiuta dal titolare del trattamento o dal/i responsabile/i se nominato/i. Almeno una volta all'anno l'azienda deve verificare ed, eventualmente, aggiornare l'elenco degli incaricati e dei relativi ambiti di trattamento consentiti (punti 14-15 e 27 del disciplinare tecnico). La finalità di queste istruzioni scritte è quella di individuare gli specifici trattamenti che l'incaricato può legittimamente effettuare conformemente alle proprie mansioni aziendali.

Pertanto, le istruzioni devono contenere l'individuazione delle banche dati cui l'incaricato può accedere, la definizione delle finalità per le quali si effettuano i trattamenti, l'eventuale ambito di comunicazione e/o diffusione all'esterno.

Inoltre, in forza degli specifici obblighi in materia di sicurezza imposti all'azienda dal Codice e dal disciplinare allegato al Codice, è necessario dettare anche prescrizioni puntuali sulle misure di sicurezza adottate a tutela dei dati: queste misure dovranno essere osservate da ogni singolo incaricato. Dal punto di vista gestionale delle misure di sicurezza per i trattamenti informatici, le diverse mansioni (e ,di conseguenza, le banche dati con le relative diverse finalità di trattamento) si concretizzano in un sistema di autenticazione all'accesso del sistema informatico che prevede diversi profili di autorizzazione (punti 12-13 e 14 del disciplinare tecnico).

Modello di designazione ed istruzioni per gli incaricati del trattamento

Le istruzioni possono essere nominative od anche per gruppi omogenei di lavoro o per funzioni aziendali (art. 30 2° comma e punti 15 e 27 del disciplinare tecnico); in caso di cambiamento di mansioni che comportino la variazione delle finalità del trattamento da svolgere o il mutamento dei data base accessibili, è necessario modificare le istruzioni scritte già fornite. Possono essere designate quali incaricati solo persone fisiche.

Egr. Signor.....

Il decreto legislativo 30 giugno 2003 n. 196 sulla tutela della riservatezza nel trattamento di dati personali ha introdotto rilevanti obblighi a carico dell'impresa, obblighi la cui inosservanza è sanzionata penalmente ed espone a responsabilità civili.

Questa decreto ha la finalità di garantire che il trattamento di dati personali si svolga nel pieno rispetto dei diritti dell'interessato, sia esso persona fisica che società, ente od associazione.

La legge prescrive (art. 30) che vengano impartite da parte del titolare *(od anche dal responsabile del trattamento*, *se nominato)* specifiche istruzioni agli "incaricati del trattamento" e, cioè, a coloro che, nell'ambito dell'organizzazione stessa ed in relazione alle mansioni affidate, trattano dati personali sia mediante sistemi informatici che mediante documenti cartacei.

Pertanto, nell'ambito delle mansioni a lei assegnate, viene designato "incaricato del trattamento" e le vengono impartite le seguenti istruzioni atte a garantire un trattamento lecito, corretto e sicuro dei dati.

Accesso a banche dati aziendali

Le banche dati cui è autorizzato ad accedere per effettuare i trattamenti (sia informatici che cartacei), sempre strettamente pertinenti alle mansioni svolte e per le finalità previste dall'azienda, rispettando i principi fondamentali sanciti dall'art. 11 del decreto legislativo n.196/2003, sono le seguenti:..... *(es. banca dati clienti, banca dati controllo qualità..... ecc....).*

(n.b.: vanno evidenziate e specificate in modo particolare le banche dati ... (es. dipendenti e curricula) o comunque i trattamenti che possono contenere anche dati "sensibili", quali quelli

inerenti allo stato di salute, l'origine razziale od etnica, le convinzioni religiose, filosofiche, politiche o sindacali, e quelli "giudiziari", ricordando che tali trattamenti, in attesa dei codici di buona condotta, devono essere perfettamente conformi alle prescrizioni contenute nelle autorizzazioni generali emanate dal garante in materia).

Creazione nuove banche dati. Gestione programmi

Senza preventiva autorizzazione del ..... *(titolare o del responsabile del trattamento, se nominato)* non è permesso realizzare nuove ed autonome banche dati, con finalità diverse da quelle già previste.

Trattamento dei dati personali

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dall'azienda e, pertanto, in conformità alle informazioni che l'azienda ha comunicato agli interessati. L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informativa e/o consenso elaborati dall'azienda.

L'incaricato deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

Comunicazione e diffusione dei dati

In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, è autorizzata la comunicazione dei dati stessi esclusivamente ai seguenti soggetti esterni indicati dall'azienda: ..... *(es. per area commerciale**:** istituti di credito per i pagamenti, società di recupero crediti per attività di recupero, società di assicurazione del credito, legali per recupero crediti**,** es. per area personale: istituti di credito per i pagamenti, enti pubblici -INPS, INAIL- organizzazioni sindacali cui è stato conferito il mandato, fondi o casse anche private di previdenza ed assistenza.....)*.

Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dall'impresa.

Misure di sicurezza

Ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dall'impresa, nonchè quelle che in futuro verranno comunicate.

Sistemi informatici *(le indicazioni si riferiscono alle <u>sole</u> misure minime**)***

Per ogni incaricato viene creata una "credenziale di autenticazione" che consente l'accesso in rete ai dati, attraverso una procedura di autenticazione (1) (logon). A tal fine, ad ogni incaricato è stata assegnata in via riservata una credenziale per l'autenticazione che consiste in un codice identificativo (user id) ed una parola chiave riservata (password). Tale parola chiave non va comunicata ad altri incaricati; le variazioni disposte autonomamente dallo stesso incaricato con periodicità semestrale (trimestrale in caso di trattamento di dati sensibili o giudiziari) devono essere comunicate, sempre in modo riservato, al custode delle credenziali.

La postazione informatica non va lasciata incustodita lasciando accessibili i dati; tutti i supporti magnetici utilizzati vanno riposti negli archivi; i supporti non più utilizzati possono essere eliminati solo dopo che i dati contenuti sono stati resi effettivamente inutilizzabili.

Si ricorda che l'azienda titolare del trattamento, nei casi in cui è indispensabile ed indifferibile accedere ai dati trattati dall'incaricato ed agli strumenti informatici in dotazione allo stesso sia per le esigenze produttive aziendali sia per la sicurezza ed operatività dello stesso sistema informatico (ad esempio nei casi di prolungata assenza od impedimento dell'incaricato), potrà accedere mediante intervento del custode delle credenziali nominato dall'azienda stessa.

.....

*(individuare eventualmente le prescrizioni **ulteriori** rispetto a quelle minime imposte per applicare specifiche misure di sicurezza informatiche).*

L'incaricato non può installare ed utilizzare programmi per elaboratore non autorizzati dall' azienda nè privi di licenza che legittimino l'uso. (2) *(inserimento opportuno per il rispetto della normativa del diritto d'autore a tutela del software, e per evitare possibili danni al sistema derivanti da virus od incompatibilità tecniche).*

Gli strumenti informatici e telematici messi a disposizione *(a seconda dei casi: computer, software,navigazione su internet, e- mail)* costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate (2).

Trattamenti cartacei

In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, potrà accedere agli archivi relativi alle banche dati di tipo cartaceo .... ubicate presso ..... *(indicare l'ufficio in cui sono collocati gli armadi contenenti gli archivi).*

*(prescrizioni da aggiungere, qualora tra le banche dati accessibili all'incaricato, rientrino dati sensibili o giudiziari)*L'incaricato nel trattare documenti contenenti dati sensibili o giudiziari è tenuto a custodirli fino alla restituzione in modo da evitare l'accesso agli stessi dati a persone prive di autorizzazione. L'incaricato deve, inoltre, custodire gli archivi contenenti documenti con dati sensibili e giudiziari, ed evitare che personale non autorizzato vi acceda. L'accesso fuori dall'orario di lavoro impone la registrazione e identificazione delle persone ammesse ai locali.

I documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'azienda.

data .....

Firma del titolare o responsabile del trattamento

.....

(firma dell'incaricato per presa visione)

.....

---

(1) La procedura di autenticazione può anche prevedere l'utilizzo di dispositivi di autenticazione elettronici (smart card) o di rilevazione biometrica (impronta digitale).

(2) Si possono eventualmente aggiungere prescrizioni in ordine alle questioni della tutela del diritto d'autore sul software (possesso di regolari licenze su tutto il software installato e divieto di installazione di software non coperto da licenza o, comunque, non preventivamente autorizzato dall'azienda), sulla tutela del know-how aziendale (individuazione di aree e tipologie di documenti di maggior rilievo per l'azienda da contraddistinguere quali documenti o aree in cui si gestisce know-how riservato dell'azienda) e sull'uso quali strumenti di lavoro della posta elettronica e della navigazione di internet anche ai fini della tutela dai virus.

Queste indicazioni non concernono in senso stretto la tutela della privacy, ma sono consigliabili per una corretta gestione dei sistemi informatici e delle informazioni in azienda: questo insieme di prescrizioni potrebbero essere oggetto di un separato "*Codice di comportamento o regolamento aziendale*" (riportato tra i modelli) adottato dall'azienda e comunicato ai dipendenti.

ISTRUZIONI AI RESPONSABILI DI AREA

Nelle organizzazioni più complesse potrebbe essere opportuno ripartire anche su responsabili di area l'attività concreta di applicazione delle procedure predisposte per garantire un corretto trattamento dei dati personali.

Questi responsabili di area potrebbero essere incaricati preventivamente di analizzare i flussi di dati trattati nella propria struttura e di comunicare le banche dati esistenti al responsabile del trattamento, al fine di collaborare con lo stesso per la realizzazione del sistema organizzativo e successivamente di verificare l'attuazione delle prescrizioni da parte degli incaricati.

Modello di istruzioni per i responsabili di area

Oggetto: Codice sulla tutela della privacy decreto legislativo n. 196 del 30.6.2003.

Il decreto legislativo n.196/2003 relativo alla tutela della privacy prevede una protezione della sfera personale sia dei singoli che delle società. Questa legge, i cui obiettivi sono di tutelare i dati personali sia delle persone fisiche che di quelle giuridiche ed in generale le imprese, impone un uso lecito e corretto delle informazioni acquisite e la verifica dell'esattezza e completezza degli stessi dati al fine di evitare pesanti responsabilità civili e penali.

Con il termine "trattamento di dati" si intendono tutte le operazioni contabili e amministrative compiute in azienda, comprese le attività di comunicazione e diffusione all'esterno dell'organizzazione aziendale, che i vari uffici svolgono per l'adempimento delle proprie funzioni. Pertanto, il trattamento di dati personali relativi a clienti, fornitori, dipendenti od altre categorie di soggetti di cui si utilizzano le informazioni nell'esercizio dell'attività aziendale, è consentito solo avendo soddisfatto agli obblighi di informazione e, ove necessario, di consenso.

Considerata la delicatezza dell'argomento e le responsabilità che ne derivano in caso di mancato rispetto della normativa, si chiede a tutti i responsabili di area:

- di verificare con estrema attenzione l'esistenza presso il proprio ufficio di archivi contenenti dati personali determinando la natura e tipologia dei dati (fiscali, anagrafici, economici...) la cui gestione interna o la divulgazione esterna rientrano nel campo di applicazione della legge a tutela della riservatezza dei dati personali;
- di comunicare all'ufficio (*) .... le eventuali banche dati gestite, le modalità di archiviazione delle informazioni contenute, le finalità di trattamento, nonché le eventuali ipotesi di comunicazione o diffusione;
- di informare per iscritto il personale della propria area, che possa essere coinvolto nella gestione di tali banche dati, dei contenuti della presente comunicazione, assicurandosi che venga da loro usata la necessaria riservatezza in ogni occasione di trattamento delle informazioni. Si ricorda che ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito, predisposte dalla società, anche in conformità alle misure minime di sicurezza obbligatoriamente fissate con norma regolamentare.
- assicurarsi che i singoli incaricati della propria area ricevano ed applichino le prescrizioni contenute nelle istruzioni scritte elaborate dalla società.

Esempio per area commerciale:

……..

In particolare si richiama l'attenzione, per la particolare "delicatezza", sull'uso delle informazioni commerciali che vengono utilizzate ed archiviate presso l'ufficio commerciale: in nessun caso tali informazioni possono essere trasmesse all'esterno dell'azienda, al di fuori dei casi individuati nelle istruzioni scritte agli incaricati, senza preventivo consenso della direzione.

Determinati dati, inoltre, contraddistinti in modo specifico, costituiscono a tutti gli effetti di legge know-how aziendale, patrimonio esclusivo della stessa azienda, di cui è vietata qualsiasi forma di comunicazione.

Ogni altra comunicazione all'esterno (diversa da quelle autorizzate per iscritto) dovrà comunque essere preventivamente concordata con la direzione.

Si allegano, per maggiore ulteriore informazione, il testo in stralcio degli artt. 7- 30- 31 del decreto n.196/2003.

(*) indicare il responsabile del trattamento (se nominato).

ISTRUZIONI PER GLI AGENTI

La rete commerciale delle aziende si basa anche sugli agenti, che trattano costantemente i dati – anche relativi alla solvibilità – dei clienti o dei potenziali clienti: è necessario, pertanto, determinare l'esatto ruolo degli agenti in ordine al trattamento dei dati. Gli agenti potrebbero, infatti, disporre autonomamente dei dati (divenendo, così, titolari del trattamento): in tal caso l'azienda preponente procede alla comunicazione dei dati all'agente (e in tal senso deve essere formulata l'informativa ai propri clienti).

In alternativa l'agente potrebbe trattare i dati esclusivamente per conto della stessa azienda preponente senza poterne disporre autonomamente.

In questa seconda ipotesi l'agente sarebbe inserito in modo incisivo nell'organizzazione dell'azienda, anche sotto il profilo dell'applicazione del sistema di misure di sicurezza adottate dalla stessa azienda.

Il modello riportato di seguito individua l'agente come semplice incaricato.

Modello di istruzioni per gli agenti

Oggetto: Codice sulla tutela della privacy. Decreto legislativo n. 196 del 30.6.2003.

Il decreto legislativo n.196/2003 relativo alla tutela della privacy prevede una protezione della sfera personale sia dei singoli che delle società. Questa legge, i cui obiettivi sono di tutelare i dati sia delle persone fisiche che di quelle giuridiche ed in genere delle imprese, vietando usi scorretti o illeciti delle informazioni e imponendo la verifica dell'esattezza e completezza degli stessi dati, al fine di evitare lesioni anche nel campo delicatissimo della loro immagine, impone a tutti gli operatori dell'azienda o comunque a persone da essa incaricate che possono accedere per motivi di servizio ad archivi di dati personali di prestare la massima attenzione nel trattare i dati e, comunque di non divulgare (comunicare o diffondere) alcuna informazione se non d'intesa con la direzione e nei casi consentiti.

Si ricorda, inoltre, che ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a vietare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati.

Pertanto, tutte le informazioni a voi trasmesse dall'azienda preponente in relazione allo svolgimento della propria attività di impresa e da voi eventualmente conservate nell'esercizio dell'attività di agenzia e riguardanti dati di nostri clienti, vanno custodite con la massima riservatezza e in nessun modo divulgate all'esterno.

Considerata la delicatezza dell'argomento e le responsabilità che ne derivano in caso di mancato rispetto della normativa, si chiede la massima collaborazione nell'ottemperare a tali disposizioni di legge, assicurandosi che le medesime cautele nel trattamento dei dati vengano rispettate anche da eventuali vostri collaboratori.

In conformità al regolamento contenente le specifiche disposizioni sugli standards di sicurezza, dovrete, comunque, rispettare alcune misure minime di sicurezza fisiche o informatiche (1), quali il sistema di autenticazione informatica di accesso per gli archivi informatici,, l'installazione di un programma idoneo antivirus... (individuare le misure minime obbligatorie prescritte in base al sistema informatico posseduto), gli armadi chiusi ad accesso selezionato per gli archivi cartacei.

Per completezza si allegano alla presente copia dell'art. 7 sui diritti dell'interessato e degli articoli 23 e 24 sui requisiti per la comunicazione e la diffusione dei dati.

(1) *Gli agenti vengono nel modulo individuati quali* ***"incaricati del trattamento"*** *rientranti, di fatto, nell'organizzazione aziendale. L'ipotesi è utilizzabile, ad esempio, nel caso in cui gli agenti sono inseriti nel sistema informatico aziendale e possono pertanto accedere ad una serie di banche dati o di dati del preponente. Pertanto, in tal caso, l'azienda risponderà degli abusi nell'utilizzo dei dati ed è quindi necessario imporre le prescrizioni sopra indicate.*

L'alternativa è qualificare gli agenti preferibilmente quali autonomi titolari di trattamenti.

In caso di individuazione quali titolari saranno responsabili in proprio dei trattamenti effettuati.

NOMINA DEL CUSTODE DELLE COPIE DELLE CREDENZIALI

Il disciplinare allegato al Codice (punto 10) ha confermato la necessità di introdurre in azienda la figura del "custode delle copie delle credenziali per l'autenticazione" nel caso di trattamenti informatici, figura già prevista ("custode delle parole chiave") dal precedente regolamento sulle misure di sicurezza (D.P.R. n. 318/99).

Questa figura svolge un ruolo fondamentale nella gestione delle misure minime di sicurezza di tipo informatico, assumendo dei precisi compiti operativi nella gestione, modifica e custodia delle passwords o parole chiave (che costituiscono la componente riservata della credenziale per l'autenticazione) assegnate ai singoli incaricati del trattamento.

Naturalmente tale figura può coincidere con un responsabile del trattamento.

Modello di lettera di nomina per il custode delle parole chiave

La figura del soggetto preposto alla custodia della copia delle credenziali è obbligatoria a norma del punto 10 del disciplinare tecnico allegato al Codice: è opportuno individuare una figura professionalmente competente nella gestione informatica delle passwords. Qualora sia stato nominato un "responsabile del trattamento" per la parte informatica, quest'unico soggetto può rivestire anche la qualifica di custode delle parole chiave.

Egr. Signor .....

Le norme che regolamentano l'attuazione delle misure minime obbligatorie per la sicurezza nel trattamento dei dati personali (attualmente il disciplinare tecnico allegato al Codice sulla privacy emanato con decreto legislativo n. 196/2003), impongono che ogni incaricato del trattamento dei dati sia munito di credenziali per l'autenticazione costituito da un codice per l'identificazione (user id) associato ad una parola chiave riservata (password) (1) per l'accesso ai dati personali presenti nei singoli elaboratori e/o nei sistemi informatici in rete.

L'assegnazione, la gestione e la variazione della parola chiave deve essere caratterizzata dalla riservatezza: a tal fine lo stesso disciplinare tecnico (punto 10) impone la individuazione e la nomina di un "soggetto incaricato della loro custodia".

In considerazione delle mansioni da Lei svolte in azienda e della sua qualificazione professionale, viene, pertanto incaricato "custode delle parole chiave riservate" attribuite ai singoli incaricati al trattamento in azienda.

Nell'espletamento delle sue funzioni dovrà applicare le misure di sicurezza disposte dall'impresa e, specificatamente, nelle gestione delle parole chiave dovrà:

- ricevere dai singoli incaricati del trattamento comunicazione riservata della sostituzione di password effettuata;
- custodire le stesse parole chiave con modalità (*fisiche ed organizzative)* atte a garantire la segretezza delle stesse parole chiave e la loro integrità (*rinviare o richiamare quelle predisposte dall'azienda o fissate nell'eventuale documento programmatico sulla sicurezza*);
- collaborare con il responsabile del trattamento e/o con l'amministratore del sistema *(se nominati)*per la corretta gestione delle misure di sicurezza relative alle stesse parole chiave.
- intervenire sul profilo autorizzativo del singolo incaricato per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale in caso di prolungata assenza od impedimento dell'incaricato che renda indispensabile ed indifferibile l'intervento.
- informare tempestivamente l'incaricato dell'intervento di accesso realizzato.

Firma del custode Firma del Titolare/responsabile

…… ……

(*) La figura del soggetto preposto alla custodia delle chiavi è obbligatoria a norma del punto 10 del disciplinate allegato al Codice: è opportuno individuare una figura professionalmente competente nella gestione informatica delle passwords. Qualora sia stato nominato un "responsabile del trattamento" per la parte informatica, quest'unico soggetto può rivestire anche la qualifica di custode delle parole chiave.

(1) Il sistema di autenticazione informatica previsto nel modello di nomina del custode è quello più diffuso che abbina il codice identificativo (user id) ad una parola chiave riservata (password); il disciplinare tecnico prevede la possibilità di altri sistemi, quali l'autenticazione biometrica dell'incaricato, eventualmente abbinata ad una password.

LETTERA AI PRESTATORI DI SERVIZI

Le aziende si avvalgono di diversi prestatori di servizi che, nell'ambito di contratti d'opera o di appalto, forniscono servizi (ad es. elaborazione paghe) o realizzano opere. Spesso tali prestatori si trovano a trattare dati personali, regolati dal Codice sulla privacy, di cui è titolare la stessa azienda committente (ad esempio, società di elaborazione paghe, software house ...). Si ritiene opportuna la nomina dei prestatori di servizi quali "Responsabili del trattamento" esterni. In tal caso essi dovranno condividere ed attuare lo specifico sistema di misure di sicurezza predisposte dall'azienda committente.

Anche non considerando questi prestatori di servizi quali "responsabili del trattamento", appare opportuno che l'azienda si premunisca con il fornitore di servizi inserendo nell'ambito del contratto un'apposita clausola con la quale lo stesso fornitore di servizi garantisca il committente sull'adozione presso la propria organizzazione delle misure di sicurezza obbligatorie ed in genere sull'adozione delle opportune misure di sicurezza informatiche ed organizzative.

Diversa è l'ipotesi, regolata al punto 25 del disciplinare tecnico sulle misure minime di sicurezza, relativa ai prestatori di servizi e beni (ad es. software) forniti per realizzare le stesse misure minime: in questo caso il disciplinare tecnico (allegato B) impone al titolare del trattamento di farsi rilasciare dal prestatore di servizi o beni una "dichiarazione di conformità" al disciplinare tecnico per l'intervento effettuato sul sistema del cliente.

Il modello riportato di seguito è una bozza di lettera integrativa del contratto già stipulato.

Modello di clausola (o lettera) per prestatori di servizi sull'applicazione delle misure di sicurezza (artt. 33 e ss.)

Nell'espletamento dell'incarico conferitoVi, la vostra società tratta dati personali, disciplinati dal decreto legislativo n. 196/2003, di cui è titolare la nostra impresa.

Poiché tali trattamenti possono avvenire anche all'esterno della nostra organizzazione aziendale e quindi al di fuori del nostro controllo, vi chiediamo di confermarci che nell'esecuzione dell'incarico da parte vostra sono state adottate tutte le misure di sicurezza minime obbligatorie previste dal disciplinare tecnico allegato allo stesso d. lgs.vo n. 196/2003, e più in generale che la vostra società si è dotata di adeguate misure di sicurezza informatiche ed organizzative atte a garantire la sicurezza, integrità e riservatezza dei dati personali trattati per nostro conto.

Vi precisiamo che siete tenuti ad informare correttamente i Vostri incaricati e a garantire il loro rispetto delle misure minime di sicurezza.

Resta inteso che non potrete effettuare alcuna comunicazione dei dati stessi a terzi se non previa nostra autorizzazione.

CLAUSOLA "CONFORMITA'" ALLE MISURE MINIME DI SICUREZZA

Il disciplinare tecnico allegato al Codice sulla privacy dispone opportunamente, nel caso di affidamento a prestatori di opera o di servizi esterni all'azienda della realizzazione di alcune misure minime di sicurezza, che lo stesso soggetto esterno dichiari che l'intervento effettuato è conforme alle disposizioni dello stesso disciplinare.
Pertanto, è opportuno che nei contratti (di fornitura, di opera, di appalto, di consulenza…) con questi prestatori esterni si precisi, con apposita clausola, che l'intervento oggetto dell'incarico dovrà garantire l'adozione di misure di sicurezza conformi alle prescrizioni del disciplinare, e che il

corretto adempimento sia attestato al termine dell'attività con un'apposita "dichiarazione di conformità".
E' evidente che imporre contrattualmente in modo esplicito l'idoneità dell'intervento al pieno rispetto delle prescrizioni tecniche del disciplinare permette, se necessario, di contestare con maggior efficacia l'inadempimento contrattuale o la presenza di vizi o difetti riscontrati.
Si riportano un modello di clausola contrattuale e di "dichiarazione di conformità".

Modello di clausola di "conformità" alle misure di sicurezza

Poiché l'intervento (l'opera realizzata, la fornitura di beni o di servizi,…) è diretto a realizzare in azienda un sistema informatico adeguato alle prescrizioni imposte dal disciplinare tecnico allegato al decreto legislativo n. 196/2003 sulle misure minime obbligatorie di sicurezza da adottare nel trattamento di dati personali, le prestazioni eseguite (l'opera realizzata, i beni forniti,…) dovranno essere pienamente conformi ai requisiti ed alle prescrizioni dettate dallo stesso disciplinare.
In considerazione delle possibili responsabilità di carattere penale in capo al titolare del trattamento per omessa adozione delle misure minime di sicurezza,la non conformità alle prescrizioni del disciplinare costituisce inadempimento grave.
Al termine dell'intervento (in conformità al punto 25 del disciplinare), dovrà essere rilasciato a cura del prestatore una dichiarazione che attesti la piena conformità di quanto installato al sistema di misure minime di sicurezza imposte dal disciplinare , e specificatamente ai punti …….

Modello di dichiarazione di "conformità"

Il sottoscritto … nella sua qualità di (legale rappresentante, procuratore, ……) della società …….., premesso che tra l'azienda committente …… e la stessa società è stato concluso un contratto di …….. per la realizzazione di ……..;
che tale contratto ha avuto esecuzione, avendo la società realizzato ……..,
con la presente, in conformità al punto 25 del disciplinare tecnico allegato al decreto legislativo n. 196/2003 sulla protezione dei dati personali,
attesta
sotto la propria personale responsabilità che l'intervento …… è pienamente conforme al sistema di misure minime di sicurezza prescritte dal disciplinare tecnico e, specificatamente, ai punti ……..

DATA …….. **FIRMA ……**

ANNOTAZIONE RELATIVA AL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA NELLA RELAZIONE DI GESTIONE DEL BILANCIO D'ESERCIZIO

Il disciplinare tecnico allegato al Codice sulla privacy prescrive (punto 26) che, nei casi in cui è obbligatoria la redazione della relazione di gestione allegata al bilancio di esercizio (nei casi in cui è prevista: articoli 2428-2478 bis e 2435 bis del Codice civile), che il titolare del trattamento (quindi gli amministratori) riferiscano sull'adozione od aggiornamento del documento programmatico sulla sicurezza, naturalmente nei casi in cui è obbligatoria questa specifica misura di sicurezza.

Modello di annotazione sulla relazione del bilancio

Il documento programmatico sulla sicurezza è prescritto dal disciplinare tecnico allegato al decreto legislativo 30.6.2003 (testo unico in materia di protezione dei dati personali) quale misura di sicurezza minima obbligatoria nel caso di trattamento, mediante sistemi informatici, di informazioni qualificabili, in base alla stessa legislazione, dati "sensibili" o "giudiziari".
Nella società vengono trattati mediante il sistema informatico anche dati sensibili (e/o giudiziari) nell'ambito delle banche dati ……
Pertanto, in ottemperanza all'obbligo contenuto nel punto 19 del disciplinare tecnico su richiamato, la stessa società,a cura del responsabile del trattamento ……(individuare la funzione), ha provveduto alla redazione/ aggiornamento dello stesso documento entro il termine del 31 marzo …..

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il "documento programmatico sulla sicurezza" costituisce una sorta di manuale della sicurezza aziendale ai fini del trattamento dei dati personali tutelati dal Codice sulla privacy.

Questo documento rappresenta una misura opportuna per analizzare la situazione aziendale ed organizzare le procedure a garanzia della sicurezza nei trattamenti: tuttavia costituisce una misura minima da adottare obbligatoriamente e da aggiornare entro il 31 marzo di ogni anno (in base al punto 19 del disciplinare tecnico allegato al d.lgs.vo n. 196/2003), esclusivamente nel caso di trattamento di dati particolari (sensibili e giudiziari).

Linee guida per la compilazione del documento programmatico sulla sicurezza

Premessa

Il Codice sulla privacy (D.lgs.vo 196/03) impone a chiunque (anche impresa) tratta informazioni relative ad altre persone, imprese, enti od associazioni di rispettare alcuni principi fondamentali a garanzia della riservatezza dei dati stessi.

Il Codice prescrive precisi obblighi e comportamenti da attuare nel trattare dati; questi obblighi sono sanzionati anche penalmente: è necessario, pertanto, procedere all'adeguamento dell'organizzazione aziendale al fine di rispettare gli obblighi imposti dal Codice.

La finalità del "documento programmatico della sicurezza" è quella di definire i criteri e le procedure per garantire la sicurezza nel trattamento di dati personali.

Fonti normative

Le disposizioni di legge principali concernenti la corretta gestione di sistemi informatici sono:

- *R.D. 22.4.1941 n. 633 e D.Lgs. 29.12.1992 n. 518 (tutela del diritto di autore sul software);*
- *L. 23.12.1993 n. 547 (reati legati all'informatica - modifiche al Codice penale);*
- *D.lgs.vo 30.6.2003 n.196 (recante il Codice in materia di protezione dei dati personali) e suo Disciplinare Tecnico (Allegato B)*

Sommario

A - ANALISI DELLA SITUAZIONE AZIENDALE

1) Descrizione del Sistema Informatico Aziendale

Devono essere descritti gli elementi fondamentali del sistema informatico aziendale, individuando tutte le sue componenti, quali ad es.:

Hardware

- Server e sistemi multiutenti presenti in azienda con i relativi sistemi operativi utilizzati

- Reti locali ed altri sistemi di collegamento di terminali
- Elaboratori portatili
- Unità di accesso per gli utenti (terminali, personal computer, workstations, stampanti, telefax)
- Collegamenti del sistema a apparecchiature di produzione, rilevatori di presenze, od altri dispositivi di acquisizione dati
- Dispositivi di connessione verso l'esterno, per singoli utenti o condivisi tra più utenti

Software
- Sistemi operativi utilizzati
- Applicazioni di tipo gestionale
- Applicazioni di office automation
- Applicazioni tecniche o grafiche (CAD/CAM, progettazione, ecc.)
- Sistemi di posta elettronica e strumenti di navigazione in Internet
- Siti Internet interni o in hosting o housing presso provider
- Altri casi .....

2) Analisi ed elenco dei dati personali

La sezione presenta le applicazioni esistenti (programmi di utilità), e sulla base delle informazioni gestite, determina se esse trattano, anche potenzialmente dati personali secondo quanto previsto dal codice sulla Privacy.

Particolare attenzione va posta riguardo all'utilizzo dei prodotti di office automation, data la libertà d'azione che tali prodotti concedono agli utenti sia riguardo al contenuto dei documenti generati, sia riguardo alla loro gestione.

La presentazione dovrà essere il più possibile completa, illustrando anche eventuali applicazioni che, pur non riguardando dati personali, sono gestite mediante il sistema informatico aziendale.

Nella sezione dovranno essere individuate ed elencate le *"banche dati"* realizzate con le specifiche applicazioni in uso (*ad* es. *clienti/fornitori; dipendenti; curricula*...) e specificate le finalità di trattamento.

Analogamente dovrà essere effettuata l'analisi degli archivi cartacei.

3) Analisi ed elenco dei trattamenti di dati "particolari";

(il censimento degli archivi e il tipo di trattamento adottato potrà essere riportato nella tabella a) dell'allegato 1)

a) Trattamento con strumenti elettronici

La sezione evidenzia la presenza di dati personali di tipo *"particolare"* (quelli sensibili o giudiziari) all'interno del sistema informatico aziendale.

Essa riporta in particolare:
- I server e/o i sistemi su cui sono archiviati i dati sensibili
- Le applicazione utilizzate per il trattamento
- Le finalità del trattamento
- Gli specifici tipi di dati particolari (sensibili o giudiziari) esistenti nel sistema *(elencare le banche dati relative)*

b) Trattamento senza l'ausilio di strumenti elettronici
- Dislocazione fisica degli archivi
- Le finalità del trattamento
- Gli specifici tipi di dati particolari, sensibili o giudiziari) presenti negli archivi *cartacei (elencare le banche dati relative)*

4) Struttura organizzativa funzionale al trattamento dati e singole responsabilità

La sezione riporta gli elementi fondamentali della struttura organizzativa aziendale coinvolti nel trattamento dei dati personali, specificandone le singole responsabilità.

In particolare nella sezione vengono evidenziati:

- Il "titolare del trattamento" dei dati, coincidente con il legale rappresentante dell'azienda
- Il/i "responsabile/i del trattamento" dati, se nominato/i (*)
- Gli "incaricati del trattamento" *(anche individuati per mansione svolta all'interno della struttura aziendale)*
- Profili di autorizzazione (*individuati per singolo incaricato o per classi omogenee di incaricati)*
- Il custode delle credenziali
- Gli eventuali prestatori di servizi che trattano all'esterno dell'impresa dati per conto della stessa impresa *(consulenti elaborazione paghe, professionisti, società di certificazione del bilancio, società di assistenza software, ...).*

(*) *per questa figura la nomina è facoltativa*

Il documento potrà contenere, in allegato, gli atti di nomina dei responsabili, le istruzioni scritte comunicate agli incaricati (nominative o per classi omogenee) ed al custode delle credenziali. Dovranno altresì essere specificate le responsabilità connesse alle mansioni da ciascuno ricoperte all'interno della struttura aziendale.

5) Analisi dei rischi possibili e dei danni conseguenti

(i possibili tipi di rischi ed i conseguenti tipi di danni dovranno essere riportati anche nella tabella b) dell'allegato 1)

Questa sezione rappresenta il nucleo fondamentale del documento, in quanto sulla base di questa valutazione l'azienda individuerà le specifiche azioni da intraprendere.

Si devono individuare ed elencare i possibili rischi cui è esposto il sistema informatico aziendale, quali ad es.:

- Alterazione/danneggiamento accidentale o dolosa del sistema, dei programmi e/o dati
- Diffusione/comunicazione non autorizzata sia accidentale che dolosa
- Danneggiamento delle risorse informatiche per disastri naturali (incendi...)
- Accessi non autorizzati
- Sottrazione di elaboratori, programmi, supporti o dati
- Intrusioni dall'esterno nel sistema
- .....

Si devono altresì individuare i tipi di danni arrecabili ai dati personali (fermo restando che l'adozione delle misure serve anche a garantire il know-how ed in genere il patrimonio aziendale), quali ad es.:

- Distruzione dei dati
- Alterazione dei dati
- Trattamento/comunicazione/diffusione non autorizzata dei dati

B - MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

6) Procedure relative alle misure imposte dal Disciplinare tecnico (Allegato B al Codice della privacy)

Scopo della sezione è evidenziare in quale maniera le misure minime di sicurezza vengono realizzate nella realtà tecnologica ed organizzativa aziendale. In particolare andranno evidenziate:

Misure minime per i trattamenti informatici

- Definizione delle credenziali di autenticazione, individuate tra le seguenti tipologie:
    1. Codice identificativo, più parola chiave
    2. Dispositivo di autenticazione (*smart card e simili*), più eventuale parola chiave
    3. Rilevazione biometrica (*es. impronta digitale*), più eventuale parola chiave
- Modalità di attivazione, variazione e gestione delle credenziali (*tra l'altro, individuazione del custode delle credenziali*)
- Criteri di definizione dei profili di autorizzazione
- Attribuzione, revoca ed aggiornamento dei profili di autorizzazione
- Criteri di utilizzo e di aggiornamento dei programmi antivirus e dei programmi di antintrusione
- Aggiornamento dei programmi volti a prevenire vulnerabilità ed a correggerne i difetti (*software update*)

Misure minime per i trattamenti cartacei

- Procedure e modalità per l'organizzazione degli archivi cartacei ad accesso autorizzato
- Modalità di custodia dei dati particolari durante l'utilizzo
- Modalità di identificazione e registrazione degli accessi ai dati particolari dopo l'orario di chiusura

7) Criteri tecnici ed organizzativi per la protezione delle aree e dei locali e procedure di controllo per l'accesso

Potranno essere evidenziate una o più delle seguenti misure per la protezione fisica:

- Localizzazione e limitazioni all'accesso del data center (localizzazione del server)
- Dispositivi antintrusione (specifici per il data center o generali per tutto l'edificio/stabilimento)
- Dispositivi antincendio (estintori, manichette, impianti di rilevazione e/o spegnimento automatico)
- Sistemi di registrazione degli ingressi e di chiusura dei locali
- Presenza di un custode e/o di un servizio di vigilanza esterna
- Custodia in armadi o classificatori ad accesso autorizzato
- Modalità di custodia delle chiavi
- .....

8) Criteri e procedure per assicurare l'integrità e la disponibilità dei dati;

- Criteri di definizione del salvataggio dei dati
- Procedure per l'esecuzione del backup
- Definizione delle tecniche e dei criteri di backup
- Procedure per la conservazione dei backup (utilizzo di casseforti od armadi ignifughi)
- Procedure per la verifica della registrazione dei backup
- Presenza di un responsabile per l'esecuzione e la verifica dei backup
- Procedura di sostituzione ed eliminazione dei dispositivi di conservazione obsoleti (cassette, nastri magnetici, supporti ottici)

Eventuali altre misure
- Alimentazione: presenza di gruppi di continuità, sistemi collegati e tempi di funzionamento garantiti
- Climatizzazione dei locali
- Sistemi dotati di mirroring, in RAID, di tipo hot-swap, dotati di alimentazione ridondante, sistemi in cluster
- Procedure di riutilizzo controllato dei supporti di memorizzazione

9) Criteri e procedure per il ripristino dell'accesso ai dati (Piano di disaster recovery)
- Criteri di definizione per il ripristino dei dati (*a seguito di distruzione o danneggiamento dei dati stessi e/o degli strumenti elettronici*)
- Identificazione degli incidenti "eccezionali" dei sistemi informatici
- Definizione di procedure che assicurino tempi certi di ripristino dei sistemi
- Verifica periodica delle procedure attivate
- Definizione di una *policy* di business continuity

10) Criteri per garantire la predisposizione delle misure minime nel caso di trattamenti affidati all'esterno della struttura aziendale
- Definizione di una corretta applicazione delle misure minime di sicurezza da parte di fornitori esterni relativi alla gestione di dati sensibili o giudiziari (*es. gestione paghe*)
- Politica di responsabilizzazione dei soggetti esterni (*predisposizione di adeguati modelli contrattuali e/o clausole contrattuali*)

C - FORMAZIONE E ADEGUAMENTO DEL DOCUMENTO

11) Piani di formazione per gli incaricati del trattamento
- Calendario e contenuti degli incontri svolti o previsti
- Conservazione della documentazione consegnata
- Registrazione dei partecipanti agli incontri formativi

12) Programma di revisione ed adeguamento

Determinare la periodicità dei controlli sull'efficienza ed efficacia delle misure previste nel documento *(almeno una volta all'anno e comunque non oltre il 31 marzo di ciascun anno).*

Vanno individuate le modalità di effettuazione del controllo (soggetti obbligati, determinando le misure di cui ogni soggetto è tenuto a verificare l'efficacia e a provvedere ai necessari interventi di adeguamento) e della relativa annotazione sulla relazione al bilancio dell'azienda.

Allegato 1

Tabella A – Censimento Archivi - Esempio di compilazione

Rev. N° ..... del ...../...../.....

N° Denominazione Archivio/banca dati (e finalità del trattamento)	***Dati sensibili*** *(contraddistinguere con X se ricorre)*	***Trattamento elettronico*** *(indicare gli elaboratori ove vengono archiviati i dati)*	***Trattamento cartaceo*** *(indicare dove sono custoditi i documenti)*
1 Personale (fiscale, previdenziale, contributiva, retributiva, ecc.)	X	Server 1	Armadio presso ufficio personale

Tabella B – **Analisi dei rischi -** Esempio di compilazione

Rev. n° ..... del ...../...../.....

Funzioni/ Aree aziendali *(sez. 4)*	***Referenti Area/ Funzione*** *(sez.6)*	***Incaricati (interni o esterni)*** *(sez.4)*	***Applicazioni informatiche***	***Tipo di danno*** *(sez.6)*	***Cause del danno*** *(sez.6)*	***Valutazione del rischio collegato alle cause*** *(alto, medio, basso) (sez.6)*	***Misure già attivate*** *(sez. 7-12)*	***Misure da attivare*** *(sez. 7-12)*
Ufficio personale	Capo ufficio personale Medico del lavoro	Addetti Ufficio Consulente del lavoro (o società di elaborazione paghe)	Rilevazione presenze Gestionale paghe	Perdita dati Comunicazione illecita Diffusione illecita Accesso non autorizzato	Eventi accidentali: -incendi -black-out Sabotaggio (interno o esterno) Negligenza, imprudenza, imperizia	M M B M B B	Estintori Gruppo di continuità Passwords Istruzioni scritte	Credenziale d'accesso

LE REGOLE AZIENDALI PER L'UTILIZZO DEI SISTEMI INFORMATICI

Le realtà aziendali si caratterizzano per l'elevato uso della tecnologia informatica che da un lato ha consentito l'introduzione di innovative tecniche di gestione dell'impresa, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'azienda al dipendente per lo svolgimento delle proprie mansioni. In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'azienda stessa a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile.

I controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal Codice sulla privacy.

Lo schema di Regolamento aziendale di seguito riportato viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti,informandoli adeguatamente ai sensi dell'art. 13 del Codice sulla privacy ed anche ai sensi dell'art.29-1°comma del d.lgs.vo 19.3.1996 n.242 sui controlli operati mediante software; il regolamento è adeguato, in particolare, agli obblighi previsti dal disciplinare tecnico sulle misure minime di sicurezza allegato al Codice. Elaborato quindi dal coordinamento legale delle associazioni industriali del triveneto sulla base delle linee guida predisposte d'intesa con Confindustria, lo schema di regolamento potrà essere utilizzato dalle imprese adattandolo però alla propria realtà aziendale.
Va peraltro segnalato che, allo stato attuale, la giurisprudenza non si è ancora pronunciata sui profili relativi all'applicazione, in materia, di quanto previsto dall'art.4 dello Statuto dei Lavoratori sul controllo a distanza della loro attività lavorativa.

Si ricorda, comunque, che l'eventuale esercizio del potere disciplinare dovrà avvenire garantendo un'adeguata pubblicità al Regolamento (mediante la sua affissione in luogo accessibile a tutti) e, più in generale, nel rispetto delle procedure previste dall'art.7 dello Statuto dei Lavoratori.

Il regolamento aziendale può costituire, inoltre, anche uno strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software presente nello stesso sistema informatico), e quella sulla tutela del know-how aziendale, quando queste importanti informazioni di proprietà dell'impresa sono custodite nel sistema informatico.

REGOLAMENTO AZIENDALE PER L'UTILIZZO DEL SISTEMA INFORMATICO

INDICE

8. Osservanza delle disposizioni in materia di Privacy.
9. Non osservanza della normativa aziendale.
10. Aggiornamento e revisione

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone *…nome azienda…*ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, *…nome azienda…* ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'…… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)*.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell' …… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici della *…nome azienda…* L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell' …… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa dell' …… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)*.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente …… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE DI *(…NOME AZIENDA…)*

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

…… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite da …… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)*È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, d.lgs.vo n.196/2003) con contestuale comunicazione al Custode delle Parole chiave (*….inserire il nome della persona…).(n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al custode; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; **;** devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico).

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Parole chiave, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o persona dalla stessa incaricata (*Responsabile*, *responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali …*)

UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli da …… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale ***……@……..it*** *(oppure .com)* per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per *(…nome azienda….)* deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno di *(…nome azienda….)* è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all' …… (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…)*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall' …… (*individuare la figura e la sua*

qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,…).

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al d.lgs.vo n. 196/2003.

NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

data

La Direzione

RAPPORTI CON IL GARANTE (*)

(*)IL MODELLO È STATO ELABORATO DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI SULLA BASE DELLA PRECEDENTE LEGGE 675/1996

ISTANZA PER L'ESERCIZIO DEI DIRITTI DELL'ART. 13
(MODELLO DEL GARANTE)

Data .....
(indirizzo del titolare del trattamento)

OGGETTO: istanza ai sensi dell'art. 13 della Legge n. 675/1996

Il sottoscritto ... nato a ... il ... residente a .... con la presente istanza, presentata ai sensi dell'art. 13, comma 1, della Legge n. 675/1996, si rivolge a .... *(indicare la denominazione del titolare del trattamento, cioè del soggetto, persona fisica o giuridica, nei cui confronti si presenta l' istanza)*:

I. per avere conferma dell'esistenza di propri dati personali e per ottenerne la comunicazione in forma intelligibile;
II. per conoscere l'origine dei dati medesimi;
III. .....
IV…..

(indicare la o le richieste che interessano)

Si segnala che, in caso di mancato o inidoneo riscontro alla presente istanza entro 5 giorni, il sottoscritto si riserva, ai sensi dell'art. 29, comma 2, della Legge n. 675, di rivolgersi all'autorità giudiziaria o di presentare ricorso al Garante per la protezione dei dati personali.

FIRMA dell'interessato
(cioè del soggetto cui si riferiscono i dati richiesti)

AVVERTENZE:

1. Il modello di istanza di accesso ai dati personali di cui sopra può essere utilizzato, con le opportune modifiche, anche per esercitare gli altri diritti tutelati dal medesimo art. 13, comma 1, della Legge n. 675 ed in particolare:

- per chiedere l'aggiornamento, la rettificazione o l'integrazione dei propri dati personali eventualmente raccolti e trattati in modo incompleto o inesatto;

- per opporsi al trattamento dei dati svolto per fini di informazione commerciale o di invio di materiale pubblicitario.

2. Qualora il trattamento dei dati sia avvenuto o tuttora si svolga in violazione di espresse norme di legge, è altresì possibile chiedere la cancellazione dei dati trattati in modo illegittimo od opporsi alla prosecuzione di tale trattamento.

3. Per dimostrare la propria identità, si consiglia di allegare all'istanza di cui sopra una fotocopia del documento d'identità (art. 17, comma 2, del D.P.R. n. 501/1998);

4. Si consiglia di inviare l'istanza di esercizio dei diritti di cui all'art. 13 mediante raccomandata con avviso di ricevimento, allo scopo di avere prova della data di spedizione e di ricezione della stessa (specie in vista dell'eventuale presentazione di un ricorso in merito).

Le modalità per l' esercizio del diritto di accesso ai propri dati personali sono dettagliate nell'art. 17 del regolamento per il funzionamento dell'ufficio del Garante (D.P.R. n. 501/1998).