Allegato 1

Istruzioni agli Incaricati del trattamento dei dati personali

In ottemperanza alle disposizioni del Codice in materia di protezione dei dati personali (D.Lgs 196/03) ed in relazione alle attività svolte nell'ambito della struttura aziendale in cui opera, Lei, in qualità di "*Incaricato",* dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che Le potrà essere fornita dal "Responsabile del trattamento".
I dati personali devono essere trattati:

a) in osservanza dei criteri di riservatezza;
b) in modo lecito e secondo correttezza;
c) er un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
d) nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure minime di sicurezza (di cui agli artt. 33 – 36 ed allegato B del citato D.Lgs 196/03) sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

1. senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);

2. con strumenti elettronici (PC ed elaboratori).

1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.
Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

1.1 Custodia

- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

1.2 Comunicazione

- L'utilizzo dei dati personali deve avvenire in base al principio del *"need to know*" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie attività lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno dell'Azienda e comunque a soggetti terzi se non previa autorizzazione.

1.3 Distruzione

- Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
- I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

1.4 Ulteriori istruzioni in caso di trattamento di dati sensibili, giudiziari e di traffico

- I documenti contenenti dati sensibili, giudiziari o relativi al traffico devono essere controllati e custoditi dagli Incaricati in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.
- L'archiviazione dei documenti cartacei contenenti dati sensibili, giudiziari o relativi a dati di traffico deve essere separata da quella relativa ai dati comuni (può essere utilizzato lo stesso armadio o cassetto chiuso a chiave ma contenitori separati).
- Per accedere agli archivi contenenti dati sensibili e giudiziari fuori orario di lavoro è necessario farsi identificare e registrare sugli appositi registri.

2. TRATTAMENTI CON STRUMENTI ELETTRONICI

2.1 Gestione delle credenziali di autenticazione

La legge prevede che l'accesso alle procedure informatiche che trattano dati personali sia consentito agli Incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. smart card) o in una caratteristica biometrica. Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni.

- Le user-id individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se Incaricati del trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Responsabile del trattamento.
- Gli strumenti di autenticazione (ad esempio le password) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Incaricati del trattamento).
- Le password devono essere sostituite, a cura del singolo Incaricato, al primo utilizzo e successivamente almeno ogni sei mesi.
- Le password devono essere composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Le password non devono contenere riferimenti agevolmente riconducibili all'Incaricato (es. nomi di familiari) e devono essere scelte nel rispetto della normativa aziendale sulla costruzione ed utilizzo delle password (vedi successivo punto **4.**).

2.2 Protezione del PC e dei dati ~

- Tutti i PC devono essere dotati di password rispondenti alle indicazioni fornite con le presenti istruzioni e, ove possibile, va impostata anche la password di BIOS. Le password devono essere custodite e gestite come previsto dalle relative normative aziendali, ivi compresa la loro sostituzione periodica.
- Le password di accesso ai PC contenenti dati personali, nonché le eventuali password per l'accesso ai singoli file contenenti tali dati devono essere consegnate in busta chiusa al responsabile gerarchico per le finalità e con le modalità di cui alla normativa aziendale "Costruzione ed utilizzo delle password".
- Tutti i PC devono essere dotati di software antivirus aziendale aggiornato costantemente e con la funzione "Monitor" attiva.
- Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dall'Azienda. Sono vietati i software scaricati da Internet o acquisiti autonomamente.
- Per evitare accessi illeciti, deve essere sempre attivato il salvaschermo con password.
- Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.
- Deve essere effettuato, con cadenza almeno settimanale un salvataggio di back-up di eventuali dati personali presenti unicamente sul PC personale (cioè non accessibili tramite i sistemi informatici aziendali). I supporti di memoria utilizzati per il back-up devono essere trattati secondo le regole definite al punto "Trattamento senza l'ausilio di strumenti elettronici".

2.3 Cancellazione dei dati dai PC

- I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.

2.4 Ulteriori istruzioni in caso di trattamento di dati sensibili, giudiziari e di traffico

- Le password di accesso alle procedure informatiche che trattano dati sensibili, giudiziari e di traffico devono essere sostituite, da parte del singolo Incaricato, almeno ogni tre mesi, salvo modalità e periodi più restrittivi di volta in volta comunicati dai Responsabili o previsti da specifiche procedure.
- L'installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi per elaboratori deve essere effettuato almeno semestralmente.

3. ISTRUZIONI DI CARATTERE GENERALE

Come scegliere e usare la password (Normativa sulla costruzione ed utilizzo delle password)

- Usare almeno 8 caratteri
- Usare lettere, numeri e almeno un carattere tra ***. ; $! @ - > <***
- Non utilizzare date di nascita, nomi o cognomi propri o di parenti
- Non sceglierla uguale alla matricola o alla userid
- Custodirla sempre in un luogo sicuro e non accessibile a terzi

- Non divulgarla a terzi
- Non condividerla con altri utenti

Come comportarsi in presenza di ospiti o di personale di servizio

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del PC premendo ctrl-alt-del e selezionando il pulsante "Lock Computer".
- Non rivelare o fare digitare le password dal personale di assistenza tecnica.
- Non rivelare le password al telefono - nessuno è autorizzato a chiederle.
- Segnalare qualsiasi anomalia o stranezza al Responsabile

Come gestire la posta elettronica

- Non aprire messaggi con allegati di cui non si conoscono l'origine, possono contenere virus in grado di cancellare i dati sul PC.
- Evitare di aprire filmati e presentazioni scherzose, possono essere pericolose per i dati contenuti sul vostro PC.
- Evitare l'inoltro automatico dalla propria casella aziendale verso caselle personali esterne.

Come usare correttamente Internet

- Evitare di scaricare software da Internet (programmi di utilità, di office automation, file multimediali, ecc.) in quanto questo può essere pericoloso per i dati e la rete aziendali. I software necessari all'attività lavorativa vanno richiesti alle competenti funzioni aziendali.
- Usare Internet entro i limiti consentiti dalle procedure/regolamenti aziendali**,** i siti web spesso nascondono insidie per i visitatori meno esperti.
- Non leggere le caselle personali esterne via webmail, provider esterni in quanto potrebbero non proteggere dai virus.

4. NORMATIVE E PROCEDURE AZIENDALI, COMPENDIO DELLA NORMATIVA SULLA PRIVACY, NOMINATIVO DEL TITOLARE E/O ELENCO DEI RESPONSABILI DEL TRATTAMENTO

Le normative e le procedure in materia di misure minime di sicurezza sono consultabili sul sito internet www.fontedir.it.

Inoltre, le presenti istruzioni, unitamente ai testi della normativa vigente in materia di privacy, al compendio della normativa sulla privacy ed al nominativo del Titolare e/o all'elenco dei Responsabili del trattamento, sono disponibili sul sito www.fontedir.it.

5. SANZIONI PER INOSSERVANZA DELLE NORME

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy, l'inosservanza delle quali può comportare sanzioni anche di natura penale.

FONTEDIR

Allegato 2

Compendio della normativa sulla privacy per l'Incaricato del trattamento dei dati personali

PREMESSA

La presente trattazione, che si colloca nell'ambito delle attività poste in essere da Fontedir per favorire al proprio interno la diffusione e la corretta applicazione della normativa vigente in materia di privacy (D.Lgs 196/03) riassume i principi e le nozioni più importanti in materia di protezione dei dati personali.

Per una più agevole consultazione, si è ritenuto utile articolare l'esposizione degli argomenti nei seguenti macro capitoli:

1. **Il quadro normativo.**
2. **Il significato di alcuni termini introdotti dalla normativa vigente.**
3. **Le figure del Titolare, del Responsabile e dell'Incaricato.**
4. **La conoscenza dei principi e delle disposizioni normative in materia di privacy quale presupposto per la loro corretta applicazione in azienda.**

1. IL QUADRO NORMATIVO

Dal 1° gennaio 2004, con l'entrata in vigore del Codice in materia di protezione dei dati personali di cui in premessa (cosiddetto Codice della privacy), tutti i precedenti provvedimenti normativi e regolamentari in materia di privacy (legge 675/96, D.Lgs 171/98, DPR 318/99, ecc.) sono stati abrogati.

Il Codice, infatti, oltre a razionalizzare, semplificare e coordinare in un "Testo Unico" tutte le precedenti disposizioni relative alla protezione dei dati personali, introduce importanti innovazioni, che tengono conto della "giurisprudenza" del Garante e della direttiva UE 2002/58 sulla riservatezza nelle comunicazioni elettroniche.

Strutturalmente il Codice è diviso in tre parti (complessivamente 186 articoli). La prima è dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato. La seconda è la parte speciale dedicata a specifici settori, quali ad esempio l'ambito sanitario, il lavoro e la previdenza sociale, le comunicazioni elettroniche (quest'ultimo di particolare interesse per le aziende di telecomunicazioni). La terza parte affronta la materia delle tutele amministrative e giurisdizionali, con delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante. Sono inoltre allegati al Codice:

- **i codici di deontologia e di buona condotta (Allegato A)** relativi **(i)** all'attività giornalistica, **(ii)** agli scopi storici, **(iii)** agli scopi statistici e di ricerca scientifica nell'ambito del sistema statistico nazionale, **(iv)** codice sulle centrali rischi (emanato successivamente all'entrata in vigore del D.Lgs 196/03);
- **il disciplinare tecnico in materia di misure minime di sicurezza** (**allegato B**);
- **i trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia** (**allegato C**).

Il Codice ha la finalità di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Tali garanzie sono estese anche ai diritti delle persone giuridiche (società private e pubbliche) e di ogni altro ente o associazione.

I testi integrali della vigente normativa sono consultabili, unitamente al presente compendio, sul sito internet di Fontedir, www.fontedir.it.

2. IL SIGNIFICATO DI ALCUNI TERMINI INTRODOTTI DALLA NORMATIVA VIGENTE

2.1 Dati personali

Sono i dati relativi alle persone fisiche e giuridiche quali ad esempio il nome, il cognome, la data di nascita, la denominazione sociale, il codice fiscale, la partita Iva, le immagini/fotografie, i suoni, le pubblicazioni, le relazioni o report, le attestazioni, ecc. Sono altresì considerati dati personali quelli relativi al traffico telefonico in generale, alle e-mail ed ai c.d. *file di log*, cioè le informazioni attraverso cui è possibile sapere quando, con chi e per quanto tempo ci si è collegati in rete (Internet, Intranet). Nella pratica, i suddetti dati sono anche definiti come "***dati comuni***" per distinguerli da quelli "***sensibili***" e "***giudiziari***".

I ***dati sensibili*** sono quelli che il Codice privacy definisce come dati personali idonei a rivelare, anche indirettamente:

- l'origine razziale ed etnica;
- le convinzioni religiose, filosofiche o di altro genere;
- le opinioni politiche;
- l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale;
- lo stato di salute e la vita sessuale.

Nella tipologia dei dati sensibili sono da considerarsi ricompresi anche le semplici indicazioni utilizzate spesso nell'ambito della gestione del personale, come ad esempio: "iscritto al sindacato", "malato", "aspettativa per malattia o maternità", fruizione di "permessi per visite mediche o per attività sindacali/politiche", "inidoneità" (psico-fisica, attitudinale, etc.). Va infine precisato che il trattamento di dati sensibili può avvenire solo ed esclusivamente a seguito del consenso iscritto dell'interessato (cioè del soggetto al quale i dati si riferiscono) e dell'autorizzazione del Garante privacy (autorizzazioni generali rinnovate di anno in anno dallo stesso Garante). Il consenso non va richiesto per la gestione del rapporto di lavoro.

I ***Dati giudiziari*** sono le informazioni rinvenibili nei provvedimenti emanati dal giudice penale per i quali è prevista la registrazione nel casellario giudiziale (art. 3 del DPR 313/02 in materia di casellario giudiziale), nonché i dati idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di procedura penale. Si citano a titolo esemplificativo: le sentenze di condanna, i provvedimenti penali divenuti irrevocabili, i provvedimenti definitivi che riguardano misure di sorveglianza. L'utilizzo di tali dati da parte di terzi è ammesso soltanto se espressamente autorizzato da leggi o provvedimenti del Garante.

2.2 Trattamento

In sintesi significa **"utilizzo"** dei dati personali. Più precisamente, il Codice della privacy lo definisce come *qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.*

2.3 Banche di dati

Sono gli archivi (cartacei o elettronici/informatici) che contengono i dati oggetto di trattamento.

2.4 Interessato

E' la persona fisica, persona giuridica, ente o associazione, dipendenti cui si riferiscono i dati personali (es, dipendenti, clienti, fornitori, visitatori).

2.5 Garante per la protezione dei dati personali (o semplicemente Garante)

Autorità posta a garanzia del rispetto delle norme sulla privacy. E' un organo collegiale costituito da quattro membri (commissari) e da un Segretario Generale. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione. Riceve, tra l'altro, le segnalazioni ed i ricorsi da parte degli interessati in relazione a presunte violazioni della normativa (dinieghi di "accesso" e/o trattamenti illeciti), emettendo al riguardo eventuali provvedimenti nei confronti del Titolare/Responsabile e trasmettendo, nei casi di violazione di norme penali, gli atti alla Procura della Repubblica competente per l'adozione dei conseguenti provvedimenti.

2.6 Comunicazione elettronica

Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico (sono escluse le informazioni trasmesse al pubblico come parte di un servizio di radiodiffusione)

2.7 Rete pubblica di telecomunicazioni

E' una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico; comprende quindi le apparecchiature di commutazione o le altre risorse necessarie per la trasmissione di segnali tra punti terminali di rete definiti, a prescindere dai tipi di mezzi utilizzati (filo, radio, ottico o altri mezzi elettromagnetici).

2.8 Servizi di comunicazione elettronica

Sono i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva.

2.9 Misure minime di sicurezza

Sono il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste dal Codice della privacy che configurano il livello minimo di protezione dei dati personali. L'adozione di tali misure è obbligatoria.

2.10 Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

3. LE FIGURE DEL TITOLARE, DEL RESPONSABILE E DELL'INCARICATO

3.1 Il Titolare del trattamento dei dati personali

Il Titolare del trattamento è il soggetto (persona fisica, società, enti pubblici o qualsiasi altro ente, associazione od organismo) che, nel raccogliere i dati personali (direttamente dall'interessato od anche attraverso la cessione da parte di altri) decide come ed in base a quali finalità (ad esempio per inviare pubblicità, per rapporto di lavoro, etc.) effettuerà il trattamento dei dati raccolti.

Il Titolare del trattamento è Fontedir, nella personana del Direttore Generale, Dott. Luca Valtolina che il Consiglio di Amministrazione ha individuato come il soggetto delegato per agire in nome e per conto del Titolare stesso nell'applicazione della normativa privacy

3.2 Il Responsabile del trattamento dei dati personali

Il Codice della privacy prevede la facoltà, per il Titolare, di nominare uno o più Responsabili del trattamento; è altresì previsto che possa essere nominato "Responsabile" non solo una persona fisica ma anche una società o altri organismi come gli enti, le associazioni, ecc. Inoltre, la designazione può riguardare più soggetti (per esempio in presenza di una struttura aziendale molto articolata possono essere nominati più Responsabili del trattamento – interni o esterni alla Società).

3.3 L'Incaricato del trattamento dei dati personali

L'Incaricato è la persona fisica alla quale, nell'ambito delle proprie attività, il Titolare o il Responsabile affidano il trattamento dei dati personali (elaborazione, archiviazione, ecc.). L'Incaricato è, dunque, colui che operativamente effettua i "trattamenti", attenendosi alle istruzioni del Titolare o del Responsabile.

Fontedir ha nominato il personale incaricato del "trattamento" in relazione alle attività (e quindi ai trattamenti) di competenza svolti nell'ambito della struttura in cui operano, impartendo loro adeguate istruzioni operative.

Per la consultazione delle istruzioni operative di cui sopra, si rinvia all'allegato 1 alla lettera di nomina ad Incaricato.

4. LA CONOSCENZA DEI PRINCIPI E DELLE DISPOSIZIONI NORMATIVE IN MATERIA DI PRIVACY QUALE PRESUPPOSTO PER LA LORO CORRETTA APPLICAZIONE IN AZIENDA

Occorre introdurre, in via preliminare, alcuni principi generali sui quali si basano le procedure e le modalità operative poste in essere dall'Azienda per una corretta applicazione della normativa vigente in materia di privacy.

In particolare:

a) i dati personali devono essere trattati

- in osservanza dei criteri di riservatezza (non devono essere resi noti a persone non interessate/autorizzate, ad esempio rispettando le norme aziendali sulla classificazione e gestione delle informazioni);
- in modo lecito e secondo correttezza (ad esempio, previa informativa e consenso dell'interessato);

- conservati in una forma che consenta l'identificazione dell'interessato (ad esempio aggiornandoli, anche in base alle indicazioni fornite dall'interessato stesso) e per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (non oltre il tempo impiegato per fornire all'interessato una certa prestazione richiesta o per svolgere una determinata attività);

b) i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi, anche accidentali, di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

4.1 Informativa all'interessato

Per informativa si intende, in sintesi, la comunicazione agli interessati delle informazioni riguardanti le finalità (ad esempio promozione o vendita di prodotti, pubblicità, ecc.) e le modalità di utilizzo (in modo automatico, tramite supporto elettronico, attraverso l'elaborazione di terzi, ecc.) dei dati personali raccolti e successivamente trattati. Nell'informativa è prevista, inoltre, l'indicazione dei diritti che l'interessato può esercitare in relazione al trattamento dei suoi dati (accesso, modifica, cancellazione, ecc.) ed il nominativo/denominazione sociale ed indirizzo del Titolare; è prevista, altresì, l'indicazione dei soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati del trattamento. L'informativa può essere fornita all'interessato sia per iscritto che verbalmente (telemarketing, promozioni telefoniche, ecc.).

4.2 Consenso dell'interessato

Il trattamento di dati personali, per finalità ulteriori rispetto all'esecuzione del contratto, è ammesso solo con il consenso espresso dell'interessato, fatti salvi i casi, tassativamente elencati dal Codice privacy all'articolo 24 (dati comuni) ed all'articolo 26 (dati sensibili), per i quali il trattamento può essere effettuato senza il consenso dell'interessato (es. in esecuzione di un contratto o per obbligo di legge). Il consenso è da intendersi validamente prestato solo se è manifestato liberamente ed in forma specifica e se sono state fornite all'interessato medesimo tutte le informazioni necessarie (informativa). Per i dati comuni, il consenso è valido anche se reso verbalmente dall'interessato, purché sia documentabile per iscritto. Al riguardo, si dovranno annotare data, ora, nominativo di chi lo ha ricevuto ed eventuali circostanze (ad esempio: vendita telefonica di un dato prodotto); sono altresì validi i consensi ottenuti tramite Web, sempreché, come già osservato, ciò sia dimostrabile in caso di eventuali contestazioni. Diversamente, per i trattamenti di dati sensibili il consenso è valido solo se espresso per iscritto. I dati sensibili possono essere trattati senza il consenso solo nei casi tassativamente previsti all'articolo 26 del Codice privacy (es. per adempiere 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).

4.3 Diritti dell'interessato

Nel linguaggio comune, con una formula molto approssimativa ma efficace, si è ormai abituati ad identificare i diritti dell'interessato con il c.d. *diritto di accesso*, diritto, si badi bene, che il legislatore ha riconosciuto solo all'interessato e non a chiunque, dando però all'interessato stesso la possibilità di delegare per iscritto altre persone fisiche o associazioni. In sintesi, l'interessato ha il diritto di ottenere a cura del Titolare o del Responsabile, senza ritardo:

- la conferma dell'esistenza o meno di dati personali che lo riguardano;
- la comunicazione dei medesimi dati e della loro origine;
- la cancellazione, la trasformazione in forma anonima (cioè in forma aggregata o con la cancellazione dei riferimenti che, direttamente o indirettamente, possano far risalire all'interessato) o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;
- di conoscere i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati del trattamento.

Inoltre, l'interessato ha il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano.

4.4 Cessazione del trattamento

Ci si riferisce alla cessazione del trattamento quando per qualsiasi motivo i dati vengono distrutti (volontariamente od anche accidentalmente), ovvero ceduti a terzi cessandone il relativo trattamento.

4.5 Sicurezza dei dati personali

"Per essere efficace, la protezione dei dati deve comprendere anche una disciplina rigorosa della sicurezza". Basandosi su questo principio il legislatore ha introdotto una prima norma generale sulla sicurezza dei dati nell'ambito dell'articolo 31 del Codice della privacy, dettagliando poi i singoli adempimenti nei successivi articoli 32-36 e nell'allegato B del Codice.

In particolare, il suddetto allegato B, intitolato "Disciplinare tecnico in materia di misure minime di sicurezza", disciplina in maniera puntuale e rigorosa le misure minime da adottare per garantire la sicurezza fisica, logica e organizzativa dei dati personali. L'intera disciplina è ispirata al principio generale sancito dal citato articolo 31, secondo il quale: *"i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".*

Le modalità operative e le informazioni di carattere tecnico in materia di misure minime di sicurezza sono disponibili nell'allegato alla lettera di nomina ad Incaricato (Allegato 1) e nelle procedure (consultabili sul sito di Fontedir www.fontedir.it).

4.6 Sanzioni

Le sanzioni previste dalla normativa vigente (di cui agli articoli da 161 a 172 del Codice privacy) a fronte di eventuali inadempimenti o di trattamenti illeciti di dati personali possono essere, a seconda del tipo di inosservanza, di natura amministrativa o penale.

FONTEDIR

Allegato 3

Informativa per dipendenti

Informativa ai sensi dell'articolo 13 del Codice in materia di protezione dei dati personali

Ai sensi dell'articolo 13 del Codice in materia di protezione dei dati personali (D.Lgs 196/03) Fontedir Le fornisce, qui di seguito, l'informativa sui trattamenti dei Suoi dati personali effettuati dallo stesso in relazione al rapporto di lavoro con Lei intercorrente a seguito del distacco da Telecom Italia presso Fontedir.

1) *Finalità del trattamento e conferimento obbligatorio dei dati*

I Suoi dati personali, ivi inclusi quelli sensibili, sono trattati per le finalità connesse al suddetto rapporto di lavoro e per adempiere gli obblighi previsti dalla legge, dai regolamenti o dalla normativa comunitaria. In particolare, Fontedir tratta i Suoi dati personali nel rispetto degli obblighi normativi e di contratto di lavoro, anche per quel che concerne i profili amministrativi, fiscali, contabili, di igiene e sicurezza sul lavoro. Il conferimento dei dati è necessario per il conseguimento delle finalità di cui sopra. Il mancato, parziale o inesatto conferimento potrebbe avere come conseguenza l'impossibilità della prosecuzione del rapporto di lavoro.

2) *Modalità e logica del trattamento*

I trattamenti dei dati sono effettuati manualmente (ad esempio, su supporto cartaceo) e/o attraverso strumenti automatizzati (ad esempio, utilizzando procedure e supporti elettronici), con logiche correlate alle finalità sopraindicate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati.

3) *Titolare, Responsabili e categorie degli Incaricati in ambito Fontedir*

Il Titolare dei trattamenti dei Suoi dati personali è Fontedir, con sede in Corso Italia, 41 – 00198 Roma, nella persona del Direttore Generale, dott. Luca Valtolina, domiciliato presso Via Gaetano Negri, 1 - 20123, Milano.

4) *Categorie di soggetti terzi ai quali i dati potrebbero essere comunicati in qualità di Titolari o che potrebbero venirne a conoscenza in qualità di Responsabili o Incaricati*

Oltre che dai dipendenti di Fontedir, alcuni trattamenti dei Suoi dati personali potranno essere effettuati anche da soggetti terzi, ivi incluse le società del Gruppo Telecom Italia, alle quali Fontedir medesima affida le attività e i servizi (o parte di essi) connessi alla gestione del rapporto di lavoro o alle sopraccitate iniziative culturali e commerciali. In tal caso gli stessi soggetti saranno individuati come autonomi Titolari oppure designati come Responsabili o Incaricati del trattamento, in conformità alle vigenti disposizioni di legge in materia di privacy. In ogni caso ai Responsabili o agli Incaricati Fontedir fornirà adeguate istruzioni operative, con particolare riferimento all'adozione delle misure minime di sicurezza, al fine di poter garantire la riservatezza e la sicurezza dei dati.

Tali soggetti, che in alcuni casi possono avere sede anche all'estero, sono ricompresi nelle seguenti categorie:

a) Consulenti (Organizzazione, Formazione, Contenzioso)

b) Società incaricate dell'amministrazione e gestione del personale, della conservazione dei dati personali dei dipendenti, dello sviluppo e/o esercizio dei sistemi informativi a ciò dedicati

c) Società incaricate per la gestione degli archivi aziendali, ivi inclusi i dati personali dei dipendenti cessati dal servizio

d) Società di Revisione/auditing

e) Soggetti pubblici e privati, Medico competente ed altri Professionisti, Enti o Associazioni che collaborano con Telecom Italia per la sicurezza e la salute dei lavoratori durante il lavoro (D.Lgs 626/94)

f) Soggetti che organizzano e gestiscono i soggiorni estivi o il perfezionamento delle lingue straniere per i figli dei dipendenti

g) Società che curano l'emissione dei buoni pasto

h) Istituti bancari per il pagamento dello stipendio

i) Assicurazioni, Associazioni e Fondi pensione

j) Società che si occupano di formazione e convegni

k) Agenzie di viaggio, Società di trasporto, Alberghi, ecc., in relazione ad eventuali trasferte

l) Istituzioni e/o Autorità Pubbliche, per adempiere specifici obblighi di legge/regolamenti in materia di Sanità, Previdenza Sociale, Fondi pensione, Antinfortunistica, ecc.

5) *Diritto di accesso ai dati personali ed altri diritti ai sensi dell'articolo 7 del Codice in materia di protezione dei dati personali (D.Lgs 196/03)*

Lei ha diritto di accedere in ogni momento ai dati che la riguardano e di esercitare gli altri diritti previsti dall'art. 7 del Codice privacy, rivolgendosi al Direttore Generale indicato al precedente punto ***3)***. Allo stesso modo può chiedere l'origine dei dati, la correzione, l'aggiornamento o l'integrazione dei dati inesatti o incompleti, ovvero la cancellazione o il blocco per quelli trattati in violazione di legge, o ancora opporsi al loro utilizzo per motivi legittimi da evidenziare nella richiesta.

FONTEDIR

Allegato 4

Comunicazione agli Incaricati del trattamento dei dati personali per la fruizione del corso on line "la sicurezza dei dati" in tema di privacy

In attuazione di quanto stabilito dal Codice Privacy e dal Garante per la protezione dei dati personali circa la necessità di prevedere per gli Incaricati del trattamento uno specifico corso di formazione in materia di sicurezza dei dati personali, Le comunichiamo che Lei è tenuto/a ad effettuare il corso in oggetto nel più breve tempo possibile. Tale corso è disponibile sul sito intranet di Telecom Italia, attraverso il seguente percorso: http://noiportal.telecomitalia.it, "per me", "formazione".

Per eventuali richieste di assistenza relative alle procedure per accedere al corso in parola Lei potrà rivolgersi al Suo diretto responsabile gerarchico.

FONTEDIR