ATAHOTELS

Istruzioni operative per gli INCARICATI del Trattamento

Adempimenti previsti dal D.Lgs. 196/2003
(*Codice in materia di protezione dei dati personali*)

2013

ATAHOTELS

INDICE

ATAHOTELS S.p.A.
Sede Legale e Amministrativa
Via Gioacchino Murat, 17
20159 Milano
Tel. +39.02.895261
Fax +39.02.89503643
www.atahotels.it
sales@atahotels.it

N. iscrizione al Registro
delle Imprese di Milano
Cod. Fiscale 00849180153
Cap. Soc. Int. Vers. € 15.000.000,00
C.C.I.A.A. Milano 726120
P. IVA 07410980150

**Società soggetta all'attività
di direzione e coordinamento di
Unipol Gruppo Finanziario S.p.A.**

ATAHOTELS

1. SCOPO DEL DOCUMENTO

Scopo del presente documento è fornire agli ***Incaricati*** del trattamento di Atahotels SpA (di seguito *"Atahotels"*) le necessarie istruzioni volte a garantire che i trattamenti di dati personali siano effettuati secondo quanto previsto dal D.Lgs. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali, in seguito "Codice"*).

Il documento è organizzato nelle seguenti sezioni:

- **Introduzione**: fornisce una breve panoramica sul Codice, focalizzandosi sul ruolo dell'***Incaricato*** del trattamento all'interno dell' articolazione organizzativa di Atahotels.

- **Trattamenti di dati personali comuni**
  - *Trattamento con strumenti elettronici*. In questa sezione sono esposte le modalità tecniche da adottare, a cura dell'*Incaricato*, in caso di trattamento effettuato con strumenti elettronici
  - *Trattamento senza l'ausilio di strumenti elettronici*. In questa sezione sono esposte le modalità tecniche da adottare, a cura dell'*Incaricato*, in caso di trattamento con strumenti diversi da quelli elettronici

- **Trattamenti di dati sensibili e giudiziari**
  - *Trattamento con strumenti elettronici*. In questa sezione sono esposte le modalità tecniche da adottare, a cura dell'*Incaricato*, in caso di trattamento di dati sensibili e giudiziari effettuato con strumenti elettronici
  - *Trattamento senza l'ausilio di strumenti elettronici*. In questa sezione sono esposte le modalità tecniche da adottare, a cura dell'*Incaricato*, in caso di trattamento di dati sensibili e giudiziari con strumenti diversi da quelli elettronici

- **Glossario**: al termine del documento è riportato un sintetico glossario dei termini più ricorrenti nell'ambito della privacy.

2. INTRODUZIONE

Dal 1 Gennaio 2004 è entrato in vigore il nuovo Codice che sostituisce la preesistente legge 675 del 1996, armonizzando tutti i decreti e i provvedimenti che nel corso dei primi sette anni della legge 675 erano stati emanati dal Legislatore o dal Garante per la protezione dei dati personali. Il Codice pertanto costituisce una fonte unitaria per tutti ciò che concerne il diritto alla privacy.

Il Codice si articola in tre parti:

- le *disposizioni generali*, contenente le regole e i principi generali, nonché le disposizioni per specifici settori, finalizzati alla corretta gestione dei trattamenti di dati personali;
- le *disposizioni relative a specifici trattamenti,* contenente i requisiti per la liceità e legittimità dei trattamenti nell'ambito, per esempio, dei rapporti di lavoro, delle comunicazioni elettroniche e del marketing diretto;
- *tutela dell'interessato e le relative sanzioni*[1].

I *soggetti* previsti dal Codice per il trattamento dei dati personali sono:

- **Titolare del Trattamento**, rappresentato dalla persona fisica o giuridica cui competono le decisioni circa le finalità e le modalità di trattamento di dati personali, ivi compresa la sicurezza dei dati (Art. 4, comma 1, lettera f);
- **Responsabile del Trattamento**, ovvero la persona fisica o giuridica che il titolare ha designato per procedere al trattamento dei dati personali (Art. 4, comma 1, lettera g);
- **Incaricato del Trattamento**, colui che compie le operazioni del trattamento di dati personali, attenendosi alle istruzioni impartite dal titolare e/o dal responsabile (Art. 4, comma 1, lettera h);
- **l'Interessato del Trattamento**, ovvero la persona fisica, cui si riferiscono i dati personali (Art. 4, comma 1, lettera i.)[2].

Di seguito verranno richiamati alcuni concetti e definizioni contenuti nel Codice, al fine di dare maggiore chiarezza ai compiti affidati all'Incaricato del trattamento.

---

[1] Per le sanzioni legali si faccia riferimento al Codice Privacy e successive modifiche ed integrazioni.

[2] Lettera così modificata dall'art. 40, comma 2, lett. b), del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214. Si riporta, per completezza, il testo originale: *""interessato", la persona fisica, la persona giuridica, l'ente o l'associazione, cui si riferiscono i dati personali;"*.

2.1 Chi è l'Incaricato del trattamento

Relativamente all'***Incaricato*** del trattamento, ai compiti assegnati e al ruolo di governo del Titolare, il Codice fornisce le seguenti indicazioni:

> ***Art. 4 – Definizioni***
>
> 1. *Ai fini del presente codice si intende per:*
>
> *[…]*
>
> *h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;*
>
> ***Art. 30 - Incaricati del trattamento***
>
> 1. *Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.*
>
> **2.** *La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.*

L'***Incaricato*** del trattamento è pertanto una persona fisica che, sotto la diretta autorità del ***Titolare*** o del ***Responsabile*** (se nominato), effettua materialmente le operazioni di trattamento dei dati personali

Il Codice ha introdotto una notevole semplificazione per la nomina degli ***Incaricati***, prevedendo che l'individuazione dell'ambito del trattamento consentito possa essere realizzata per unità organizzativa. La nomina si limita pertanto ad una mera associazione del dipendente o del collaboratore ad una determinata unità cui, con documento regolamentare interno, sono stati associati determinati trattamenti di dati personali. Il dipendente associato ad una determinata unità organizzativa "eredita" quindi i trattamenti che il ***Titolare*** ha assegnato a quella stessa unità.

Quanto detto si presta ad essere utilizzato specialmente nelle unità organizzative che hanno una elevata complessità interna o che presentano una elevata rotazione del personale.

La previsione di modalità semplificate per la nomina degli ***Incaricati*** non esclude, tuttavia, che i singoli ***Responsabili*** del trattamento, anche in ragione delle modalità di trattamento e della rischiosità dei dati, decidano di effettuare delle nomine specifiche e dettagliate per ciascun ***Incaricato*** che opera nella struttura di competenza.

Nel caso di Atahotels, la designazione degli Incaricati del Trattamento verrà effettuata attraverso la documentata preposizione ad una struttura di competenza, in linea con quanto previsto dal comma 2 dell'art. 30 del D.Lgs. 196/2003.

Nel contesto delle strutture competenti di Atahotels, l'ambito del trattamento consentito per ogni unità organizzativa è descritto in via aggregata nel "Regolamento Privacy". Il "Regolamento Privacy" costituisce quindi lo strumento regolamentare attraverso il quale il Titolare definisce gli ambiti consentiti.

2.2 Cos'è un trattamento di dati personali

Il trattamento è il nucleo del sistema di gestione della privacy: il Codice, infatti, non pone al centro del sistema di protezione la banca dati o lo strumento elettronico, ma, per l'appunto, il trattamento, ovvero un insieme logicamente correlato di operazioni aventi come oggetto dati personali, svolte per scopi e finalità legittime.
A tale proposito, il Codice fornisce le seguenti definizioni:

> ***Art. 4 – Definizioni***
>
> ***1.*** *Ai fini del presente codice si intende per:*
>
> ***a) "trattamento"****, 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'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;*
>
> ***b) "dato personale"****, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;*
>
> ***c) "dati identificativi"****, i dati personali che permettono l'identificazione diretta dell'interessato;*
>
> ***d) "dati sensibili"****, i dati personali idonei a rivelare 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*
>
> ***e) "dati giudiziari"****, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;*
>
> *[...]*
>
> ***Art. 17 - Trattamento che presenta rischi specifici***
>
> *1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.*

Un efficace governo della privacy deve quindi partire da un censimento dei trattamenti di dati personali effettuati in azienda. La conoscenza dei trattamenti e di tutti gli attributi connessi, consente di diffondere all'interno dell'organizzazione la consapevolezza dell'esistenza di precisi diritti da tutelare, e dei benefici che tale tutela può comportare, nella misura in cui si riesca a far percepire agli interessati del trattamento che i loro dati "*stanno al sicuro*" (a puro titolo esemplificativo, si pensi ai dati di videosorveglianza, che possono riguardare sia dipendenti che visitatori).

I dati personali che di norma Atahotels tratta sono riferiti a:

- dipendenti
- candidati all'assunzione
- stagisti
- visitatori (o Congressuali)
- clienti
- Organi di Controllo
- consiglieri

e possono essere contenuti in banche dati elettroniche (e.g., anagrafiche, cartelle di rete), o in archivi cartacei (e.g., contratti, schedine di registrazione, fatture, curriculum vitae).

Una particolare categoria di dati personali, meritevole di maggiore tutela, è quella dei ***dati sensibili***, ovvero i dati personali dell'interessato dai quali sia possibile desumere, ad esempio:

- lo stato di salute;
- l'appartenenza a un sindacato;
- la vita sessuale;
- l'origine razziale;
- il credo religioso, etc..

Nell'ambito delle strutture organizzative di ATAHOTELS, i trattamenti di ***dati sensibili*** sono effettuati prevalentemente dal medico competente, per quanto riguarda la sorveglianza sanitaria, e dagli incaricati della Direzione del Personale per quanto riguarda lo stato di malattia o infortunio e l'appartenenza a sindacati o ad altre associazioni di categoria dei dipendenti.

Il trattamento dei dati sensibili è inoltre effettuato nella SPA delle Strutture Ricettive; in particolare in *Petriolo SPA Resort* l'ospite esterno o il cliente del Resort vengono sottoposti ad un colloquio medico preventivo alle cure di acque termali.

Con riferimento ai ***dati giudiziari***, presso Atahotels l'unico caso in cui potrebbe verificarsi un trattamento è riconducibile all'acquisizione o la conservazione dei casellari giudiziari degli interessati, nell'ambito dell'assunzione degli addetti alla Tesoreria.

Infine, come indicato all'Art.17 del Codice, è necessario evidenziare i trattamenti di quei dati i quali, sebbene meno critici di quelli sensibili o giudiziari, presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato (di seguito "***dati rischiosi***"), e per i quali sia necessario adottare misure ed accorgimenti specifici prescritti dal Garante Privacy.
Presso Atahotels sono effettuati trattamenti di dati rischiosi, quali, ad esempio, i dati di videosorveglianza.

3. TRATTAMENTO DI DATI PERSONALI COMUNI

Le istruzioni contenute nel presente paragrafo sono indirizzate ai soggetti aziendali, nominati ***Incaricati*** del Trattamento, che effettuano trattamenti di dati personali comuni.
In particolare, la prima parte della sezione riguarda il trattamento di dati personali comuni effettuato con l'ausilio di strumenti elettronici, mentre la seconda parte illustra le regole da seguire nel caso in cui i trattamenti siano effettuati senza l'ausilio di strumenti elettronici.

3.1 Trattamenti effettuati con l'ausilio di strumenti elettronici

L'art. 34 del Codice (*Trattamenti con strumenti elettronici*) circoscrive il perimetro di applicazione delle misure minime di sicurezza per il trattamento di dati personali effettuato mediante l'ausilio di strumenti elettronici.

> ***Art. 34 (Trattamento con strumenti elettronici)***
>
> *Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:*
>
> *a) autenticazione informatica;*
> *b) adozione di procedure di gestione delle credenziali di autenticazione;*
> *c) utilizzazione di un sistema di autorizzazione;*
> *d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;*
> *e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;*
> *f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;*
> *g) tenuta di un aggiornato documento programmatico sulla sicurezza;*
> *h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.*

Le modalità tecniche da adottare a cura del ***Titolare***, del ***Responsabile*** ove designato e dell'***Incaricato***, in caso di trattamento con strumenti elettronici, sono declinate ed esposte diffusamente nel *Disciplinare Tecnico in Materia di Misure Minime di Sicurezza*, Allegato B del Codice.
Nel seguito verranno presentate e commentate solo le misure di sicurezza da adottare a cura degli ***Incaricati*** del Trattamento, chiarendo, laddove opportuno, i concetti di natura prettamente tecnica.

Sistema di autenticazione informatica

La prima parte del "Disciplinare Tecnico" (regole 1-11) riguarda le misure di sicurezza da adottare per i sistemi di autenticazione informatica.

Si definisce **autenticazione informatica** il processo tramite il quale un sistema elettronico verifica l'identità dichiarata da un utente.

Un esempio di tale processo è la comune procedura di autenticazione nota come *login*: l'accesso ad un sistema di elaborazione viene garantito solo dopo aver digitato le cosiddette *credenziali di accesso*, che tipicamente sono costituite da *username* (fase di *identificazione*, in cui l'utente risponde alla domanda "chi sei?") e *password* (in cui l'utente risponde alla domanda "dimostrami chi sei?").

> ***Regola 4***
>
> *Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.*

L'accesso ai sistemi elettronici con cui sono effettuati i trattamenti di dati personali deve essere pertanto consentito ai soli ***Incaricati*** dotati delle credenziali di accesso.
La regola 4 stabilisce che l'incaricato deve assicurare la segretezza della sola password (cosiddetta "componente riservata della credenziale"), e non della username.
Il presupposto essenziale per garantire la sicurezza dei dati è, infatti, che la parola chiave rimanga riservata.

Cosa fare per mantenere segreta la parola chiave

Per proteggere il sistema da accessi non autorizzati, ogni ***Incaricato*** è pertanto tenuto a mantenere segreta la parola chiave, mediante l'osservazione di semplici regole:

- non annotare la parola chiave nei pressi della postazione di lavoro o su documenti cartacei (e.g. post-it)
- non condividere o comunicare la password via mail o mediante altre forme di comunicazioni elettroniche
- non utilizzare le funzionalità, presenti in alcuni sistemi, di memorizzazione automatica della password
- non archiviare la password in file presenti sul proprio computer
- qualora il sistema non preveda un cambio forzato della password almeno ogni 6 mesi per dati personali comuni e almeno ogni 3 mesi per dati sensibili o giudiziari - come previsto dalla regola 5[3]- cambiare autonomamente la password al primo utilizzo, successivamente almeno ogni 3 mesi o comunque ogni qualvolta si abbia il sospetto che la propria password possa essere stata intercettata
- se per qualche ragione è stato necessario comunicare la password a qualcuno (e.g. help desk), crearne una nuova alla prima occasione
- non cedere la propria parola chiave ad un collega o ad altro ***Incaricato***

ATAHOTELS

Come scegliere una parola chiave idonea

Gli hacker utilizzano tecniche di attacco basate su "dizionari" e altri strumenti software in grado di verificare, nell'arco di poche ore, la corrispondenza di una password con milioni di password comuni presenti nei dizionari stessi.
È quindi di fondamentale importanza proteggere i propri dati utilizzando password complesse, mediante l'osservazione di semplici regole:

- utilizzare password che non abbiano un senso compiuto (e.g. nomi propri)
- utilizzare lettere maiuscole (A-Z) e minuscole (a-z), numeri (0-9) e caratteri speciali (e.g. @, #, $, %)
- non usare per la password ALCUNA PARTE della username
- non usare alcuna parola o nome reale in NESSUNA lingua
- non riutilizzare alcuna parte della password precedente
- non usare lettere o numeri consecutivi, come "abcdefg" o "234567"
- qualora il sistema non preveda una lunghezza minime per la password pari ad almeno 8 caratteri - come previsto dalla regola 5[4]- costruire una password che abbia una lunghezza di almeno 8 caratteri

Cosa fare per custodire diligentemente gli strumenti elettronici aziendali

L'***Incaricato*** è tenuto a custodire con diligenza gli strumenti aziendali a lui assegnati mediante l'osservazione di semplici regole:

- tutti gli strumenti informatici e telematici (e.g. PC, relativi accessori e periferiche, software), assegnati dall'azienda, sono da intendersi esclusivamente come strumenti di lavoro e devono essere pertanto utilizzati unicamente a fini aziendali per ottemperare agli incarichi assegnati e non per scopi personali;
- gli strumenti aziendali devono essere utilizzati con diligenza e custoditi in modo appropriato; l'incaricato deve pertanto informare tempestivamente l'azienda (in particolare la struttura di Help Desk della Direzione Sistemi Informativi) in caso di furto, danneggiamento, malfunzionamento, guasto o smarrimento di uno strumento aziendale;

3 **Regola 5**: La parola chiave […] è modificata al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
4 **Regola 5**: La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; […].

- non installare qualunque tipo di software (e.g. freeware, shareware, programmi peer-to-peer) senza preventiva autorizzazione scritta da parte della Direzione Sistemi Informativi;
- non utilizzare e/o installare strumenti hardware o software atti ad intercettare, falsificare, alterare il contenuto di documenti informatici (e.g. programmi di recovery password, cracking);
- non modificare autonomamente le configurazioni impostate sul proprio PC, né installare sugli stessi mezzi di comunicazione personali (e.g. modem);
- non utilizzare il proprio PC o la propria workstation per trasmettere, ricevere, scaricare, stampare o diffondere in qualunque altro modo contenuti di carattere indecente, osceno, razzista, sessualmente esplicito, illegale, immorale e lesivo della dignità dei soggetti interessati e dell'azienda.

Regola 9

Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

La regola 9 è una misura di sicurezza organizzativa volta alla protezione dei dati sia da eventuali manomissioni, sia dall'accesso agli stessi da parte di soggetti non autorizzati. Attivare una sessione di lavoro su un PC portatile o su una workstation e lasciare incustodito lo strumento consente, infatti, l'accesso a persone non autorizzate che possono quindi venire a conoscenza dei dati e, potenzialmente, possono alterarli.

Una volta effettuato l'accesso al sistema, fornendo il codice identificativo e la parola chiave, si può accedere, in relazione al proprio profilo di autorizzazione, ai dati personali contenuti nelle banche dati.

Cosa fare per non lasciare incustodito lo strumento elettronico

Nel caso in cui un ***Incaricato*** abbia necessità di assentarsi temporaneamente dalla postazione di lavoro, deve assicurarsi che nessuno possa accedere ai dati personali del sistema durante la sua assenza, mediante uno dei seguenti accorgimenti:

- blocco del sistema ponendolo in stato di "lock"; ad esempio, nel caso dei sistemi operativi Microsoft Windows, tale operazione può essere effettuata premendo in sequenza i tasti ctrl+alt+canc e quindi cliccando sul pulsante "blocca computer" (oppure in inglese "lock computer"); in caso di sistemi operativi diversi, rivolgersi al personale preposto alla loro gestione (e.g. help desk);
- laddove possibile e con l'eventuale supporto del personale preposto, impostare funzioni automatiche di blocco, che disattivano il sistema

dopo un breve periodo di inattività, come, ad esempio, lo "screen saver" con password; il periodo di inattività oltre il quale si attiva lo screen saver non deve superare i 15 minuti;

- spegnere il sistema.

Altre misure di sicurezza

La terza parte del "Disciplinare Tecnico" (regole 15-18) riguarda altre misure di sicurezza da adottare.

> ***Regola 18***
>
> *Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.*

La regola 18 è una misura di sicurezza tecnico-organizzativa volta alla protezione dei dati dall'eventuale rischio di perdita della loro disponibilità, dovuta ad eventi accidentali (e.g. crash di una macchina) o intenzionali (e.g. cancellazione dei file presenti su un PC di un incaricato a causa dell'accesso di un hacker al sistema).

Cosa fare per salvare i dati aziendali

Al fine di preservare i dati dal rischio di perdita di disponibilità, l'***Incaricato*** è tenuto ad osservare i seguenti accorgimenti:

- effettuare il salvataggio dei dati aziendali del proprio PC o della propria workstation con cadenza almeno settimanale e, possibilmente, giornaliera;
- salvare i dati aziendali sulle directory di rete (*share*) riservate e presenti sui server aziendali e non in locale sul proprio terminale;
- qualora sia necessario utilizzare supporti di memoria rimovibili (e.g. pen drive, CD-ROM, flop disk), questi devono essere conservati in luoghi protetti (e.g. armadi e cassettiere chiusi a chiave), cancellati quando i dati non sono più necessari o distrutti nel caso non fosse possibile cancellarli.

3.2 Trattamenti effettuati in modalità manuale

L'art. 35 del Codice (*Trattamenti senza l'ausilio di strumenti elettronici*) circoscrive il perimetro di applicazione delle misure minime di sicurezza per il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici.

> ***Art. 35 (Trattamenti senza l'ausilio di strumenti elettronici)***
>
> *Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:*
>
> *a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;*
>
> *b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;*
>
> *c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.*

Le modalità tecniche da adottare a cura del ***Titolare***, del ***Responsabile*** ove designato e dell'***Incaricato***, in caso di trattamento senza l'ausilio di strumenti elettronici, sono declinate ed esposte diffusamente nel *Disciplinare Tecnico in Materia di Misure Minime di Sicurezza*, Allegato B del Codice.

Nel seguito verranno presentate e commentate solo le misure di sicurezza da adottare a cura degli ***Incaricati*** del Trattamento, chiarendo, laddove opportuno, i concetti di natura prettamente tecnica.

Tali istruzioni riguardano, come detto, tutti coloro che effettuano trattamenti di dati personali comuni in modalità manuale, ovvero mediante l'utilizzo di archivi e documenti cartacei (e.g. ordini, fatture e documenti di trasporto, schede fornitore e schede cliente, indirizzari e rubriche, schede valutative).

> ***Regola 27***
>
> *Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. [...]*

Gli ***Incaricati*** sono tenuti a custodire diligentemente gli atti e i documenti contenenti dati personali, affinché essi siano preservati da danneggiamenti, smarrimenti e accessi non autorizzati.

Come custodire con diligenza i documenti aziendali

Gli ***Incaricati*** sono tenuti ad osservare i seguenti accorgimenti:

- custodire i documenti cartacei in archivi protetti, chiusi a chiave ed accessibili al solo personale autorizzato;
- la permanenza del documento fuori dall'archivio deve essere limitata al solo periodo necessario per il trattamento;
- riporre i documenti nei corretti archivi al termine del loro utilizzo;
- non lasciare incustoditi su tavoli e scrivanie, soprattutto se accessibili al pubblico, documenti cartacei contenenti dati personali;
- al termine dell'orario di lavoro avere cura di lasciare sgombra la propria scrivania da documenti contenenti dati personali;

- apporre etichette ai documenti per una più facile archiviazione ed individuazione del contenuto degli stessi.

4. TRATTAMENTO DI DATI SENSIBILI E GIUDIZIARI

Le istruzioni contenute nel presente paragrafo sono indirizzate ai soggetti aziendali nominati Incaricati del Trattamento che effettuano trattamenti di dati sensibili e giudiziari.

All'interno di Atahotels le Direzioni Aziendali che trattano dati sensibili sono:

- Direzione del Personale
- Direzione Sistemi Informativi
- Direzione Audit e Controllo di Gestione
- Direzione SPA delle Strutture Ricettive

La sola Direzione che potrebbe trattare dati giudiziari degli interessati è la Direzione del Personale per l'assunzione degli addetti alla Tesoreria..

La prima parte della sezione riguarda il trattamento di dati sensibili e giudiziari effettuato con l'ausilio di strumenti elettronici, mentre la seconda parte illustra le regole da seguire nel caso in cui i trattamenti siano effettuati senza l'ausilio di strumenti elettronici.

4.1 Trattamenti effettuati con l'ausilio di strumenti elettronici

Come indicato nel paragrafo 3.1, l'art. 34 del Codice (Trattamenti con strumenti elettronici) circoscrive il perimetro di applicazione delle misure minime di sicurezza per il trattamento di dati personali effettuato mediante l'ausilio di strumenti elettronici.

Le modalità tecniche da adottare a cura del ***Titolare***, del ***Responsabile*** ove designato e dell'***Incaricato***, in caso di trattamento con l'ausilio di strumenti elettronici, sono declinate ed esposte diffusamente nel *Disciplinare Tecnico in Materia di Misure Minime di Sicurezza*, Allegato B del Codice.

Nel seguito verranno presentate e commentate solo le misure di sicurezza da adottare a cura degli Incaricati del Trattamento, chiarendo, laddove opportuno, i concetti di natura prettamente tecnica.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

La quinta parte del "Disciplinare Tecnico" (regole 20-24) riguarda ulteriori misure di sicurezza da adottare in caso di trattamento di dati sensibili e giudiziari.

> ***Regola 21***
> *Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.*

Gli incaricati devono pertanto custodire e utilizzare con diligenza i supporti rimovibili su cui sono memorizzati i dati sensibili o giudiziari (e.g. flop-disk, CD-ROM, pen drive USB).

ATAHOTELS

Cosa fare per custodire con diligenza i supporti rimovibili

I supporti rimovibili contenenti dati sensibili o giudiziari devono essere opportunamente custoditi per evitare che i dati in essi memorizzati vengano distrutti, resi inutilizzabili, trafugati o diffusi a soggetti non autorizzati al loro trattamento.

Gli ***Incaricati*** sono pertanto tenuti ad osservare le seguenti disposizioni:

- non asportare i supporti dall'apparecchiatura che li ospita durante la fase di trattamento (elaborazione) dei dati;
- custodire e trasportare i supporti in custodie rigide e protette;
- non esporre i supporti a campi elettromagnetici o a temperature troppo basse o troppo alte;
- custodire i supporti in cassetti o armadi chiusi a chiave e accessibili solo all'incaricato;
- utilizzare i supporti solo per il tempo necessario al trattamento e, successivamente, riporli nei rispettivi armadi o cassetti;
- apporre etichette sui supporti utili allo loro corretta individuazione e catalogazione.

> ***Regola 22***
>
> *I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili,ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.*

Gli ***Incaricati*** devono inoltre rendere inutilizzabili o distruggere tutti i supporti rimovibili su cui sono memorizzati i dati sensibili o giudiziari, qualora questi non siano utilizzati ovvero possano essere riutilizzati da altri incaricati.

Cosa fare per cancellare i dati registrati su supporti non utilizzati

I dati personali sensibili o giudiziari devono essere cancellati dai dispositivi di memorizzazione non più utilizzati dall'***Incaricato***.
Si richiede pertanto che:

- i dati sensibili e giudiziari siano cancellati[5] da tutti i supporti rimovibili non utilizzati o destinati ad altro uso, tramite un'operazione di formattazione;
- qualora non sia tecnicamente possibile cancellare i dati dai supporti rimovibili, procedere alla distruzioni fisica del supporto.

5 In certi casi potrebbe non essere banale eliminare da un supporto rimovibile i dati (e.g. dati contenuti all'interno di ambienti oppure di applicazioni specifiche); in tutti questi casi rivolgersi al personale della Direzione Sistemi Informativi per avere la certezza di aver distrutto le informazioni.

4.2 Trattamenti effettuati in modalità manuale

Come indicato nel paragrafo 3.2, l'art. 35 del Codice (*Trattamenti senza l'ausilio di strumenti elettronici*) circoscrive il perimetro di applicazione delle misure minime di sicurezza per il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici.

Le modalità tecniche da adottare a cura del ***Titolare***, del ***Responsabile*** ove designato e dell'***Incaricato***, in caso di trattamento con l'ausilio di strumenti elettronici, sono declinate ed esposte diffusamente nel *Disciplinare Tecnico in Materia di Misure Minime di Sicurezza*, Allegato B del Codice.

Tali istruzioni riguardano, come detto, tutti coloro che effettuano trattamenti di dati sensibili e giudiziari in modalità manuale, ovvero mediante l'utilizzo di archivi e documenti cartacei (e.g. curriculum vitae, elenchi di appartenenza al sindacato, certificati di idoneità al lavoro, certificati di infortunio o malattia).

> ***Regola 28***
>
> *Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.*

Gli ***Incaricati*** sono pertanto tenuti ad evitare che vi siano accessi di personale non autorizzato ai dati sensibili o giudiziari.

Come evitare accessi non autorizzati ai dati sensibili e giudiziari

Gli ***Incaricati*** sono tenuti a:

- riporre i documenti e gli atti contenenti dati sensibili e giudiziari in armadi o cassetti chiusi a chiave;
- custodire la chiave con diligenza;
- non lasciare in nessun caso i documenti incustoditi;
- al termine di ogni trattamento riporre i documenti nell'archivio appropriato.

ATAHOTELS

5. GLOSSARIO

A

Autorizzazione
Un provvedimento adottato dal Garante con cui il titolare (ente, azienda, libero professionista) viene autorizzato a trattare determinati dati sensibili o giudiziari o a trasferire dati personali all'estero. In tema di dati sensibili e giudiziari, il Garante ha emanato sette autorizzazioni generali che consentono a varie categorie di ***Titolari*** di trattare dati per gli scopi specificati senza dover chiedere singolarmente un'apposita autorizzazione al Garante.

Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

B

Banca Dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Blocco
La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

C

Codice in materia di protezione dei dati personali (D.Lgs. 196/2003)
Testo unico in materia di protezione di dati personali, entrato in vigore dal 1 Gennaio 2004 che sostituisce la precedente *Legge 675/96* e integra in numerosi decreti e provvedimenti emanati dal 1997 al 2003.

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 tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Comunicazione
Il dare conoscenza dei dati personali a uno o più soggetti determinati, diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal ***Responsabile*** e dagli ***Incaricati***, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

Consenso
La libera manifestazione della volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, sul quale è stato preventivamente informato da chi gestisce i dati (v.d. titolare). E' sufficiente che il consenso sia documentato in forma scritta (ossia, annotato, trascritto, riportato dal Titolare o dal ***Responsabile*** o da un ***Incaricato*** del trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati sensibili; in questo caso occorre il consenso esplicito rilasciato per iscritto dall'interessato (ad es., con la sua sottoscrizione).

ATAHOTELS

D

Dato Anonimo

Dati che in origine, o a seguito di trattamento, non possono essere associati ad un interessato identificato o identificabile (*lettera n, comma 1, art. 4*).

Dato Giudiziario

I dati personali idonei a rivelare provvedimenti di cui all'*articolo 3, comma 1, lettere* da *(a)* a *(o)* e da *(r)* a *(u),* del *D.P.R. 14 novembre 2002, n. 313*, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli *articoli 60 e 61 del codice di procedura penale*.

Dato Personale

Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (*lettera b, comma 1, art. 4*). In particolare, i dati personali che permettono l'identificazione diretta dell'interessato, sono detti "dati identificativi" (*lettera c, comma 1, art. 4*).

Dato sensibile

Un dato personale che, per la sua delicatezza, richiede particolari cautele: sono dati sensibili quelli che possono rivelare la razza, l'appartenenza etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale (*lettera d, comma 1, art. 4*).

Dato personale rischioso

Un dato personale che, pur non essendo un dato sensibile, presenta dei rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare (ad esempio i nominativi presenti nelle centrali rischi utilizzate nel settore creditizio).

G

Garante

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla legge sulla privacy (legge n. 675 del 31 dicembre 1996). L'istituzione di analoghe autorità prevista in tutti gli altri Paesi membri dell'Unione Europea (direttiva comunitaria 95/46/CE). Il Garante ha il compito di assicurare la tutela dei diritti e delle libertà fondamentali nel trattamento dei dati personali, ed il rispetto della dignità della persona. Il Garante si compone di quattro membri eletti dal Parlamento, ha sede a Roma (piazza di Monte Citorio, 121). Alle sue dipendenze è posto un Ufficio con un organico di cento unità. Esamina segnalazioni dei cittadini e vigila sul rispetto delle norme che tutelano la vita privata. Decide sui ricorsi presentati dai cittadini e può compiere ispezioni.

I

Informativa

Le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi: su quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i

diritti riconosciuti all'interessato; chi sono il titolare e il responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax ecc.).

M

Misure di sicurezza

Sono tutti gli accorgimenti e i dispositivi utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti. Rispetto alle più ampie misure che il titolare deve applicare a tutela dei dati, un regolamento ha indicato le misure di sicurezza che è obbligatorio adottare a rischio di responsabilità penale per garantire un livello minimo di protezione. Nel regolamento sono fissati una serie di criteri e accorgimenti (es. password, codice identificativo, antivirus) che i titolari devono adottare a seconda che il trattamento riguardi dati sensibili e sia effettuato manualmente (archivi e documenti cartacei) o con elaboratori (distinguendo tra elaboratori accessibili in rete o meno). E' previsto che tali misure siano adeguate periodicamente, per tenere conto degli sviluppi tecnologici e dell'esperienza maturata.

N

Notificazione

La notificazione è una comunicazione che il titolare del trattamento deve effettuare una tantum utilizzando un apposito modulo da inviare al Garante, in cui vengono descritte le principali caratteristiche del trattamento.

P

Privacy

E' un termine inglese che evoca significati a volte mutevoli, accostabile ai concetti di riservatezza, privatezza. Ad esempio, oggi la privacy non significa soltanto diritto di essere lasciati in pace o di proteggere la propria sfera privata, ma anche il diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione. Il diritto alla privacy e, in particolare, alla protezione dei dati personali costituisce un diritto fondamentale delle persone, direttamente collegato alla tutela della dignità umana, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea.

Profilo di autorizzazione

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

R

Registro dei trattamenti (o Censimento)

Il registro dei trattamenti è un documento rappresentativo dei trattamenti effettuati in azienda. È costituito da schede singole in cui sono riportati tutti gli attributi rilevanti dei trattamenti.

S

Strumenti elettronici

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

T

Trattamento (di dati personali)

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.