

La tutela della Privacy

Autore: Marco Schiavi

Mail: marco.schiavi@alice.it

Contenuti

- Quadro normativo: il codice privacy
- L'adeguamento organizzativo: i ruoli
- Il trattamento dei dati

Quadro normativo: il codice privacy

**Il decreto legislativo 196 del 30/06/2003 è
il nuovo codice per la privacy**

È un “ testo unico ”

Cos'è la “ Privacy ” ?

**È un termine di origine inglese traducibile
come “ diritto alla riservatezza ”**

*[...] dignita' dell'interessato, con particolare riferimento
alla riservatezza, all'identita' personale e al diritto
alla protezione
dei dati personali [...]*

Il diritto alla Privacy

il D.Lgs 196 enuncia che :

“ Il trattamento dei dati personali e' effettuato assicurando un elevato livello di tutela dei diritti e delle libert  [...] nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalit  previste per il loro esercizio da parte degli interessati, nonch  per l'adempimento degli obblighi da parte dei titolari del trattamento”.

L'adeguamento organizzativo: i ruoli

I ruoli

L'organizzazione che il codice impone risulta riconducibile a quattro ruoli principali:

- Il **titolare** del trattamento
- Il **responsabile** del trattamento
- Gli **incaricati** al trattamento
- L'**interessato** al trattamento

Titolare del trattamento

*“ la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui **competono**, anche unitamente ad altro titolare, **le decisioni** in ordine alle **finalità**, alle **modalità** del trattamento di dati personali e agli **strumenti** utilizzati, ivi compreso **il profilo della sicurezza** ”*

Responsabile del trattamento

*“ la persona fisica, la persona giuridica,
la pubblica amministrazione e
qualsiasi altro ente, associazione od
organismo **preposti dal titolare**
al trattamento di dati personali ”*

Responsabile del trattamento

Il responsabile deve sovrintendere o effettuare i trattamenti dei dati personali rispettando ed attenendosi alle istruzioni impartite dal titolare il quale deve, anche con verifiche periodiche, vigilare sull'osservanza delle disposizioni impartite

Incaricato al trattamento

*“ la persona fisica
autorizzata a compiere
operazioni di trattamento
dal titolare o dal responsabile”*

Incaricato al trattamento

Gli incaricati possono materialmente effettuare le operazioni di trattamento dei dati personali. La loro designazione deve contenere la precisa ed analitica individuazione **dell'ambito del trattamento** consentito e delle **istruzioni** cui dovranno attenersi nello svolgimento dello stesso

Interessato al trattamento

*“ la persona fisica,
la persona giuridica,
l'ente o l'associazione
cui si riferiscono i dati personali ”*

I diritti dell'interessato

Chiunque ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati

I diritti dell'interessato

L'interessato ha diritto di ricevere
la comunicazione dei propri dati personali
in forma chiara ed intelligibile

Il diritto può essere esercitato con una **semplice
richiesta** rivolta al titolare o al
responsabile del trattamento.

I diritti dell'interessato

L'interessato ha **diritto di ottenere l'indicazione** :

- a) **dell'origine** dei dati personali;
- b) delle **finalità e modalità** del trattamento;
- c) della **logica applicata** in caso di trattamento effettuato con l'ausilio di **strumenti elettronici**;
- d) degli **estremi identificativi del titolare**, dei **responsabili** e del rappresentante designato ai sensi dell'articolo 5, comma 2;
- e) dei **soggetti** o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

I diritti dell'interessato

L'interessato ha **diritto di ottenere:**

- a) **l'aggiornamento**, la **rettificazione** ovvero, quando vi ha interesse, **l'integrazione** dei dati;
- b) la **cancellazione**, la **trasformazione in forma anonima** o il **blocco** dei dati trattati in violazione di legge, compresi quelli di cui non e' necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- c) **l'attestazione** che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

Il trattamento dei dati

Dati personali

“Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale ”

I dati personali si dividono in tre categorie:

- Dati identificativi o comuni
 - Dati sensibili
 - Dati giudiziari

Dati identificativi (Comuni)

***“ dati che permettono la
identificazione
diretta dell'interessato ”***

Dati sensibili

***“ 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”***

Dati giudiziari

***“ dati personali idonei a rivelare provvedimenti
iscrivibili nel casellario giudiziale (articolo 3, comma
1, lettere da a) a o) e da r) a u), del d.P.R. 14
novembre 2002, n. 313)***

o la qualità di imputato

***o di indagato ai sensi degli articoli 60 e 61 del codice
di procedura penale ”***

Adempimenti preliminari per il trattamento dei dati

- **La designazione del responsabile**
 - **L'informativa**
 - **Il consenso**
- **L'adozione di idonee misure di sicurezza**

Informativa

L'interessato deve essere **informato preventivamente del trattamento**

Contenuto dell'informativa

- **finalità e modalità del trattamento cui sono destinati i dati;**
- **natura obbligatoria o facoltativa del conferimento dei dati;**
- **conseguenze di un eventuale rifiuto di rispondere;**
- **soggetti o categorie di soggetti ai quali possono essere comunicati i dati personali o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;**
- **diritto di accesso ai dati;**
- **titolare del trattamento cui rivolgersi.**

Consenso informato al trattamento

Il trattamento **e' ammesso solo con il consenso espresso dell'interessato.**

Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

Il consenso e' valido solo se riferito ad un trattamento chiaramente individuato, se e' documentato per iscritto, e se all'interessato è stata resa la **informativa**

Il consenso al trattamento **é manifestato in forma scritta se riguarda dati sensibili.**

Misure di sicurezza

I titolari del trattamento
sono sempre tenuti ad adottare
le misure di sicurezza
individuate nel codice in modo
da assicurare un livello minimo di
protezione dei dati personali.

Misure di sicurezza

Le misure di sicurezza attengono :

alla protezione dei dati
trattati con strumenti tradizionali

alla protezione dei dati
trattati con strumenti elettronici

Trattamenti **SENZA** **strumenti elettronici**

Il trattamento di dati personali effettuato
senza l'ausilio di strumenti elettronici
e' consentito solo se sono adottate le
misure previste dal disciplinare
tecnico

(allegato B al codice)

Trattamenti **SENZA** **strumenti elettronici**

A) aggiornamento della definizione
periodica dell'**ambito del trattamento**
consentito ai singoli
incaricati e addetti alla unità
organizzative

Trattamenti **SENZA** **strumenti elettronici**

B) previsione di procedure per un'**idonea custodia di atti e documenti affidati** agli incaricati per lo svolgimento dei relativi compiti

Trattamenti **SENZA** **strumenti elettronici**

- C1) previsione di **procedure per la
conservazione di determinati atti
in archivi ad accesso selezionato**

- C2) **disciplina delle modalità di
accesso finalizzata all'identificazione
degli incaricati.**

Trattamenti **CON** **strumenti elettronici**

- A) **autenticazione informatica**
- B) adozione di **procedure di gestione delle credenziali di autenticazione**
- C) utilizzazione di un **sistema di autorizzazione**

Trattamenti **CON** **strumenti elettronici**

D) aggiornamento della definizione
periodica dell'**ambito del**
trattamento consentito ai singoli
incaricati e addetti alla gestione o alla
manutenzione degli strumenti elettronici

Trattamenti **CON** **strumenti elettronici**

- E) **protezione degli strumenti elettronici**
e dei dati rispetto a trattamenti illeciti di
e/o 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

Trattamenti **CON** **strumenti elettronici**

G) tenuta di un **aggiornato** documento
programmatico sulla sicurezza (**DPS**)

Adempimenti

Devono poi essere oggetto di aggiornamento annuale:

- L'ambito dei trattamenti consentiti agli incaricati
- La verifica di istruzioni tecniche e organizzative per il salvataggio settimanale dei dati
- La programmazione della formazione per gli incaricati
- L'aggiornamento delle patch dei programmi dei computer per trattamento dei dati comuni

Adempimenti

Devono poi essere oggetto di aggiornamento semestrale:

- L'aggiornamento dell'antivirus
- L'aggiornamento delle patch dei programmi dei computer per trattamento dei dati sensibili
- Il cambio password per i dati comuni

Altri adempimenti: Dati sensibili

- Il cambio password per i dati sensibili avviene ogni tre mesi
- Almeno ogni settimana occorre effettuare il salvataggio dei dati
- Entro 7 giorni deve essere possibile ripristinare l'accesso ai dati in caso di danneggiamento

Disciplinare tecnico

Il disciplinare tecnico (Allegato B), relativo alle misure minime di sicurezza, **sarà periodicamente aggiornato entro il 31 Marzo di ogni anno**

(con apposito decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore).

Disciplinare tecnico

Contenuti rilevanti:

- Credenziali di autenticazione: user id e password
- Password di almeno 8 caratteri non riconducibile direttamente all'interessato
- Credenziali non utilizzate da almeno 6 mesi vanno eliminate
- Istruzioni che non lascino incostudito il pc (saver screen con password)
- Definire uno o più incaricati deputati alla custodia di copia delle credenziali

Disciplinare tecnico

Contenuti rilevanti:

- Individuare per gli incaricati i relativi profili di autorizzazione
- Definire classi omogenee per i profili di autorizzazione per limitare l'accesso ai soli dati necessari
- Proteggere i dati da intrusione con idonei strumenti (antivirus, firewall)
- Aggiornare periodicamente i programmi del pc
- Salvataggio dei dati almeno settimanale

Il Documento programmatico sulla sicurezza (**DPS**)

Fra le misure minime di sicurezza
che il codice impone di adottare rientra
il DPS

il DPS

Il DPS fotografa tutte le misure di sicurezza logiche, tecniche ed organizzative che l'azienda :

- ha adottato da subito**
- ha deciso di adottare a breve**
- adotterà nel medio e lungo termine**

il DPS

- 19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige un documento programmatico sulla sicurezza o procede al suo aggiornamento**

Contenuto del DPS

- 19.1 l'elenco dei trattamenti di dati;**
- 19.2 la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;**
- 19.3. l'analisi dei rischi che incombono sui dati;**

Contenuto del DPS

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

Contenuto del DPS

19.5 la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

(Devono essere rispettati i tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni)

Contenuto del DPS

19.6 la previsione di **interventi formativi** degli incaricati del trattamento

(piano della formazione per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali)

Grazie per l'attenzione