Decreto Legislativo n.196 del 30 giugno 2003

(ante Regolamento UE 2016/679, ante Dlgs. 101/2018)

Codice in materia di protezione dei dati personali

Quali sono i dati da proteggere

Dati Personali

- 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.

Quali sono i dati da proteggere

Dati Sensibili

- I dati 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, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Quali sono i dati da proteggere

Dati Giudiziari

- I dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti.

Cosa significa trattare i dati

Il Codice per la tutela della Privacy prevede che i dati siano:

1. trattati in modo lecito e secondo correttezza;
2. raccolti e registrati per scopi determinati, espliciti e legittimi;
3. esatti e, se necessario, aggiornati;
4. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
5. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi siano raccolti o successivamente trattati.

Chi può trattare i dati personali

Relativamente alla comunicazione dei dati da parte dei soggetti pubblici, il Codice prevede che:

- La comunicazione da soggetto a soggetto pubblico è ammessa se prevista da una norma di legge/di regolamento o in mancanza, ove necessaria per lo svolgimento di funzioni istituzionali;
- La comunicazione/diffusione da soggetto a privati/a enti pubblici economici, è ammessa solo ove prevista da una norma di legge/di regolamento.

Chi è il titolare del Trattamento dei dati

E’ 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 a:

- Le finalità perseguite;
- Le modalità del trattamento dei dati personali;
- Gli strumenti utilizzati;

Chi è il Referente Responsabile del Trattamento dei dati

E’ la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che siano preposti dal titolare al trattamento di dati personali.

Chi è l'incaricato del Trattamento

E' la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal referente.

La designazione è effettuata per iscritto e individua l'ambito del trattamento consentito.

Misure minime: Allegato B

- Ridurre al minimo i rischi: i dati personali devono essere custoditi con cura e controllati;
- I rischi sono: la distruzione, la dispersione, il trattamento illecito;
- L'allegato B descrive le misure minime per ridurre il rischio.

Autenticazione informatica

- E' un codice di identificazione dell'incaricato + una parola chiave riservata oppure una caratteristica biometrica + una parola chiave;
- Ogni incaricato può avere uno o più codici di autenticazione;
- L'incaricato è obbligato a custodire ed assicurare la segretezza della parola chiave (niente più post-it appiccicati sul monitor);
- L'incaricato non lascia sessioni aperte incustodite

Autenticazione informatica

La parola chiave:

a) Deve avere almeno 8 caratteri;

b)Non deve contenere riferimenti all'incaricato;

c) Una volta ricevuta l'incaricato la cambia;

d) Scade al più ogni sei mesi (consigl. 3 mesi);

e) Non può essere ceduta ad altri;

Autenticazione informatica

Assenza dell'incaricato

In caso di prolungata assenza dell'incaricato il Responsabile del trattamento preleva la parola chiave dalla busta sigillata e la consegna a colui che dovrà operare sullo strumento elettronico;

L'incaricato al suo rientro sarà costretto all'immediato cambio della parola chiave con successiva consegna al responsabile del trattamento per la custodia;

Sistema di autorizzazione

- Periodicamente (almeno annualmente) il profilo di autorizzazione va verificato nella sua sussistenza;
- Vanno eliminate le credenziali non usate da più di sei mesi;

Documento Programmatico della Sicurezza

- Entro il 31 marzo di ogni anno il Titolare ed il Responsabile del Trattamento redigono un aggiornamento del DPS;
- Cosa contiene il DPS ?

Documento Programmatico della Sicurezza

Contiene:

- L'elenco dei trattamenti di dati personali;
- La distribuzione dei compiti e delle responsabilità;
- Le misure adottate per garantire disponibilità ed integrità dei dati;
- Criteri e modalità di ripristino dei dati;
- Misure di sicurezza per dati affidati all'esterno della struttura;
- Gli interventi formativi degli incaricati

Trattamento di dati sensibili e giudiziari

I supporti di copia dei dati e i supporti rimovibili vanno protetti contro l'accesso abusivo (ad es. in cassaforte);

Il trasporto elettronico dei dati sensibili e giudiziari deve essere cifrato.

Archivi cartacei

- Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento dei dati personali;
- In caso di atti contenenti dati sensibili e giudiziari, quest'ultimi vanno controllati e custoditi dall'incaricato durante tutto il trattamento fino alla restituzione in archivio;
- Il documento delineante le funzioni relative al trattamento dei dati che l'incaricato riceve può anche essere redatto per classi omogenee di incarico.

Adempimenti periodici

1° gennaio di ogni anno :

- Aggiornare l'individuazione dell'ambito di trattamento consentito agli incaricati;
- Verificare la sussistenza delle condizioni di autorizzazione;
- Programmare gli eventi formativi per gli incaricati;
- Aggiornare il sw antivirus/firewall, "patch" dei programmi.

Adempimenti periodici

31° marzo di ogni anno :

- Aggiornare il DPS.

1° luglio di ogni anno :

- Aggiornare il sw antivirus/firewall, "patch" dei programmi.