Principali novità e misure per la tutela dei dati personali D. Lgs. 30 giugno 2003 n. 196 e Regolamento Europeo 2016/679

Relatore: Avv. Sabrina Primavera

D.lgs 30 giugno 2003 n. 196

- In un unico testo, di natura legislativa, vengono raccolte e coordinate le disposizioni precedentemente contenute in vari provvedimenti, legislativi e di natura regolamentare, conseguentemente abrogati;
- Sono apportate integrazioni e modifiche;
- Il testo mira alla massima chiarezza;
- Vigenza: dal 1 gennaio 2004;

Principali norme abrogate e nuovi riferimenti

- Legge n. 675 del 31 dicembre 1996 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali);
- D.Lgs. 28 dicembre 2001, n. 467;
- D.P.R. 318 del 28 luglio 1999: Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge n. 675 del 31 dicembre 1996;

comma 2 dell'articolo 184: *"quando leggi, regolamenti e altre disposizioni fanno riferimento a disposizioni comprese nella legge 31 dicembre 1996, n. 675, e ad altre disposizioni abrogate dal presente codice, il riferimento si intende effettuato alle corrispondenti disposizioni del presente codice, secondo la tavola di corrispondenza riportata in allegato"*.

Dalla forma alla sostanza

- Prevalenza della sostanza sulla forma, infatti nella relazione di accompagnamento del codice si legge che:

  "*sul piano sistematico, si è ritenuto doveroso porre in maggiore evidenza, nella parte iniziale del codice, le disposizioni generali riguardanti i diritti e le libertà fondamentali, le principali garanzie e le connesse sfere di responsabilità. Ciò tenendo conto dell'erronea tendenza registratasi in passato, volta ad enfatizzare e, talvolta, a drammatizzare i profili legati a taluni adempimenti a carico del titolare del trattamento*";

Composizione del nuovo codice

- **Tre parti:**

– Disposizioni generali (artt. 1 – 45);

– Disposizioni particolari (artt. 46 – 140);

– Azioni di tutela dell'interessato e sistema sanzionatorio (artt. 141 – 172) + Norme finali transitorie (artt. 173 – 186);

- **Tre allegat**i:

– Codici di deontologia (**allegato A**);

– Disciplinare tecnico in materia di misure minime di sicurezza (**allegato B**)

– Elenco trattamenti non occasionali in ambito giudiziario o per fini di polizia (**allegato C**)

Le disposizioni generali

Articoli da 1 a 45:

- Regole sostanziali della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti;
- Regole specifiche per i trattamenti effettuati da soggetti pubblici;
- Regole che trovano applicazione per i trattamenti effettuati da soggetti privati e da enti pubblici economici.

Diritto alla protezione dei dati personali (art. 1)

Art. 1: “Chiunque ha diritto alla protezione dei dati personali che lo riguardano”:

- Diritto all’autodeterminazione informativa: il singolo ha il diritto di decidere autonomamente i tempi ed i limiti di utilizzo delle informazioni che lo riguardano;
- Si cerca di contemperare le esigenze di **riservatezza** dell’individuo con le necessità della società dell’**informazione**.

Finalità ed obiettivi (art. 2)

- I trattamenti dei dati personali si devono svolgere nel rispetto dei diritti e delle **libertà fondamentali**, nonché della **dignità dell'interessato**;
- Rispetto alla L. 675/96 viene estesa la portata della protezione ("*interessato*") a persone giuridiche, enti ed associazioni; detta estensione è stata abrogata con il Decreto Monti del 2012 volto alla semplificazione in materia di Privacy.
- Principio di "semplificazione nell'elevata tutela" (passaggio dalla forma alla sostanza)

Il principio di necessità nel trattamento dei dati (art. 3)

- L'articolo 3, di nuova introduzione, dispone che i sistemi informativi ed i software debbano essere configurati in modo da **minimizzare il ricorso ai dati personali ed identificativi**;
- Vanno utilizzati dati anonimi o pseudonimi ogniqualvolta le finalità dei trattamenti non ne risentano;
- L'interessato deve **essere identificabile solo in caso di necessità** (v. ad es. le prescrizioni di medicinali);
- Il principio di necessità rappresenta un potenziamento dei principi di pertinenza e non eccedenza dei dati rispetto alle finalità del trattamento ex L. 675/96.

Alcune definizioni (art. 4) 1/2

- **Trattamento**: operazioni sui dati, anche senza ausilio di strumenti elettronici (v. fascicoli e rubriche cartacei), anche se non registrati in una banca dati (novità: basta la "*consultazione*" dei dati perché si configuri trattamento);

- **Dato personale**: qualunque informazione relativa a persone fisiche, giuridiche o associazioni, identificata o identificabile;

- **Dati sensibili**: dati personali idonei a rivelare l'origine razziale o etnica, convinzioni religiose o politiche, adesione a partiti, sindacati, associazioni o organizzazioni di carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Alcune definizioni (art. 4) 2/2

- **Interessato**: la persona fisica o giuridica, ente o associazione cui si riferiscono i dati personali;
- **Comunicazione**: dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall'interessato;
- **Diffusione**: dare conoscenza dei dati personali a soggetti indeterminati;
- **Banca di dati**: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Cosa sono i dati personali?

- Informazioni su soggetti identificati o identificabili;
  – Sia quando risultino oggettivamente caratterizzate;
  – Sia quando riguardino giudizi, descrizioni o profili soggettivi;
- Suoni ed immagini (v. direttiva 95/46/CE) qualora permettano di identificare i soggetti, anche in via indiretta (ad esempio, videosorveglianza).
- Associazioni di informazioni:
  – “Abramo Levi, nato a Tel Aviv il 12 febbraio 1958” (potrebbe rivelare religione ed etnia);
- Risulta importante il contesto nel quale i dati sono inseriti!

Quando un dato è sensibile?

- Alcune situazioni rivelano oggettivamente dati sensibili. Ad esempio, un archivio che contenga nominativi e religioni di appartenenza;
- Altre informazioni non sono di per sé “sensibili”, ma possono diventarlo in base al contesto in cui vengono utilizzate;
- Quello che può rendere un dato sensibile è quindi l’uso che il titolare del trattamento ne fa, in relazione alle finalità per cui il dato viene trattato.

Oggetto ed ambito di applicazione (art. 5)

- Il codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque nel territorio dello Stato o in un luogo soggetto alla sovranità dello Stato (diritto nazionale applicabile: princìpio di stabilimento del titolare del trattamento);

- Il trattamento effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. In ogni caso si applicano le disposizioni in tema diresponsabilità (art. 15) e di sicurezza (art. 31).

I diritti dell'interessato (art. 7)

- **Diritto di conoscere**

– Titolare e responsabili dei trattamenti;

– I soggetti ai quali i dati possono essere comunicati;

- **Diritto di certificare e controllare**

– Aggiornamento e rettifica dei dati inesatti (dati oggettivi, ma non anche dati di tipo valutativo soggettivo: v. art.8);

– Integrazione dei dati, se vi ha interesse;

– Cancellazione

– Trasformazione

– Blocco

- **Diritto di opporsi al trattamento per motivi legittimi**

Esercizio dei diritti da parte dell'interessato

I diritti da parte dell'interessato sono esercitati tramite:

- **RICHIESTA**: Lettera raccomandata, telefax, posta elettronica od anche orale, rivolta al titolare o al responsabile del trattamento.

  La richiesta deve essere riscontrata in maniera tempestiva, la norma dice "senza ritardo".

  Pertanto, ricevuta la richiesta, il titolare del trattamento deve:
- AGEVOLARE l'accesso ai dati personali da parte dell'interessato;
- SEMPLIFICARE le modalità di accesso e
- RIDURRE i tempi dando RISCONTRO completo e intellegibile (comprendere tutti i dati personali dell'interessato trattati dal titolare).

Modalità del trattamento e requisiti dei dati (art. 11)

- Correttezza (lealtà del trattamento);

- Liceità del trattamento

– **Norme imperative** (es. illecito il trattamento che abbia ad oggetto le persone disposte a donare organi);

– **Ordine pubblico** (es. illecito il trattamento che abbia ad oggetto i nomi di persone disposte a scendere armate in piazza);

– **Buon costume** (il Garante ha dichiarato illegittimo il trattamento effettuato da una casa di appuntamenti relativo ai dati personali dei propri clienti);

- Pertinenza, completezza e non eccedenza

I Codici Deontologici (art. 12)

- Il legislatore Italiano ha scelto una “terza via” tra il metodo legislativo puro e quello autodisciplinare;
- E’ prevista una speciale procedura di formazione del codice mediante verifica di conformità ai princìpi generali della legge operata dal Garante, che riconosce ai codici deontologici il valore di “criterio di riferimento” per la determinazione di legittimità del trattamento;
- In tal modo il codice deontologico assume valenza di norma, seppure di grado secondario rispetto alla Legge, potendo però approfondire meglio e più tecnicamente i singoli settori di riferimento.

I danni cagionati per effetto del trattamento (art. 15)

- Il Legislatore considera il trattamento di dati personali come attività pericolosa (vedi art. 2050 Codice Civile).

- Chi ritenga di essere stato leso da un trattamento dati che lo riguardano può ottenere il risarcimento danni senza dover provare la colpa del Titolare. Deve provare solo gli eventuali danni derivati dal trattamento. Il nesso di causalità è pertanto che:
  - Il danno si sia realizzato;
  - Dipenda dall'attività di trattamento dati;

- Chi ha effettuato il trattamento, per sottrarsi all'obbligo di risarcimento, ha l'onere di provare di aver adottato tutte le misure idonee ad evitare il danno (*inversione dell'onere della prova*).

I danni risarcibili

- L’area dei danni risarcibili per la violazione del diritto alla riservatezza è estesa anche al danno non patrimoniale (art. 15 comma 2) nel caso in cui il titolare vìoli i princìpi generali sulla privacy dettati all’art. 11 (modalità e requisiti);

- La quantificazione del danno non patrimoniale si basa su una valutazione di equità, ai sensi degli artt. 1226 e 2056 del Codice Civile.

L’informativa (art. 13)

L’interessato deve essere **previamente informato** circa:

– Finalità e modalità del trattamento dati;
– Natura obbligatoria o facoltativa del conferimento dati;
– Le conseguenze di eventuali rifiuti di rispondere;
– I soggetti (o categorie) cui potranno essere comunicati i dati, o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l’ambito di diffusione dei dati medesimi;
– I diritti di cui all’articolo 7;
– Gli estremi identificativi del titolare;

Il Consenso (artt. 23-26) – 1/2

- E’ una libera ed esplicita manifestazione di volontà dell’interessato in relazione all’utilizzo dei propri dati personali da parte di terzi che, in qualità di titolari del trattamento dei dati, ne decidono finalità e modalità;

- **Momento** di richiesta del consenso: va richiesto all’interessato prima della raccolta dei dati (salvo particolari situazioni);

- E’ condizione di liceità del trattamento dati posto in essere da parte di privati ed enti pubblici economici (non Pubblica Amministrazione, v. art.18 c. 4);

Il Consenso (artt. 23-26) – 2/2

- **Forma**: il consenso deve essere manifestato in forma scritta nel caso in cui il trattamento abbia ad oggetto dati sensibili;
- Per i dati non sensibili basta che il consenso sia documentato per iscritto;
- Deve essere fornito in riferimento ad un trattamento chiaramente individuato;
- Unica eccezione: per i dati sulla salute (quindi “sensibili”) ai fini sanitari è ammessa la formula del consenso verbale documentato per iscritto (semplificazione);

Trattamento dati da parte di soggetti pubblici (Con esclusione di Enti Pubblici Economici)

Dati di qualsiasi genere e dati diversi da quelli sensibili e giudiziari:

- è consentito soltanto per lo svolgimento delle funzioni istituzionali.
- in conformità ai presupposti e nei limiti previsti dal codice, leggi e regolamenti.
- Non è necessario acquisire il consenso salvo che si tratti di dati acquisiti da esercenti professioni sanitari e organismi sanitari pubblici.
- nel rispetto dei divieti di comunicazione e diffusione (art.25 codice)

Trattamento dati sensibili e giudiziari

- solo se autorizzato da espressa disposizione di legge che specifichi o provvedimento del Garante;
- solo se svolto con modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato;
- in ogni caso solo per i dati necessari ed indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa;
- nell'informativa (art.13) devono essere specificate le norme che prevedono i compiti e gli obblighi del trattamento;

Trattamento dati da parte di enti pubblici economici e privati

- deve essere autorizzato per legge con specificazione della tipologia dei dati oggetto del trattamento e delle finalità pubbliche perseguite.
- con il consenso scritto dell'interessato e previa autorizzazione del Garante.
- in ogni caso, con osservanza delle cautele volte a prevenire lesioni di diritti e di interessi degli individui.

Trattamento dati sensibili

- è ammesso solo con il consenso espresso dell'interessato e previa autorizzazione da parte del garante. Se il garante non si pronuncia entra 45 gg equivale a rigetto. Con il provvedimento di autorizzazione, o anche successivamente, il Garante può prescrivere, al titolare del trattamento, misure e accorgimenti a garanzia dell'interessato.
- In casi specificatamente previsti è ammesso anche senza consenso previa autorizzazione da parte del Garante, con esclusione della diffusione.

Trattamento dati giudiziari

- è consentito: se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino:

I Ruoli privacy (artt. 28 – 30)

- Il Titolare
- I Responsabili
- Gli Incaricati

Il Titolare (art. 28)

- E’ il soggetto che esercita autonomo potere decisionale sulle finalità e modalità del trattamento dati.
- Può essere una persona fisica, giuridica o un ente.
- Princìpio di effettività della delega di esercizio: una delega è efficace quando il delegato riceve anche i poteri che gli consentano di esercitare in modo effettivo i compiti attribuitigli.

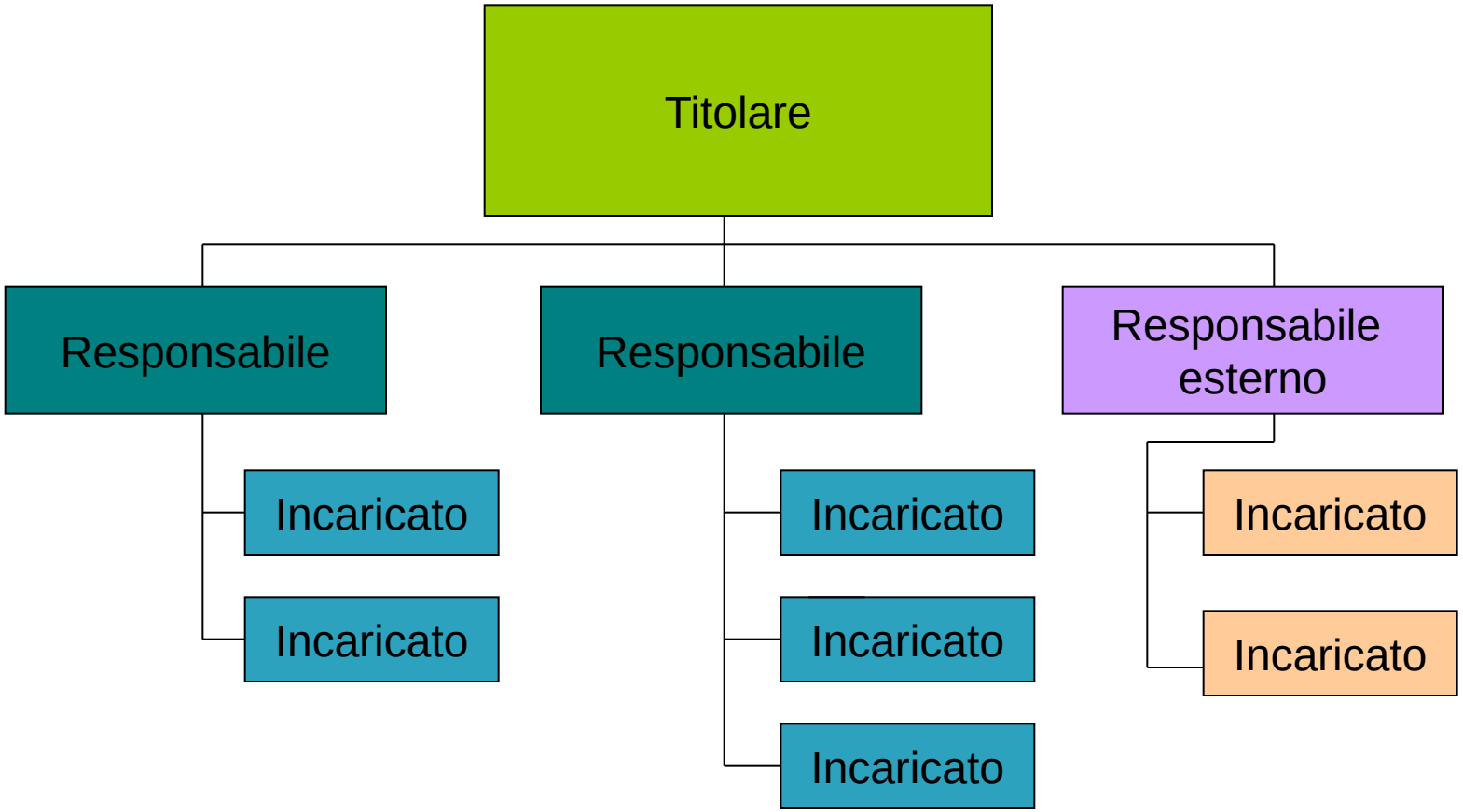
Il Responsabile (art. 29)

- E’ la persona fisica o giuridica che può essere designata da parte del titolare del trattamento;
- Deve obbligatoriamente essere nominato per iscritto, e deve essere indicato il potere di controllo del titolare sul suo operato;
- E’ possibile nominare più di un responsabile;
- Deve essere scelto tra persone che per esperienza o capacità forniscano idonee garanzie circa il pieno rispetto delle norme vigenti in materia di trattamento dati, compreso il profilo della sicurezza.

L’Incaricato (art. 30)

- Chiunque compia operazioni di trattamento dei dati è individuato come incaricato;
- Possono essere individuati come incaricati solo le persone fisiche (non anche le persone giuridiche);
- Modalità di nomina: la designazione si deve ritenere valida anche qualora sussista la documentata preposizione della persona fisica ad una unità per la quale sia individuato, per iscritto, l’ambito del trattamento consentito agli addetti dell’unità medesima

Rapporti tra i ruoli privacy



Sicurezza nei flussi di dati (artt. 31 – 33 e 36)

- Gli obblighi di sicurezza (idonee e preventive) cui sono tenuti i titolari sono enunciati nell'art. 31;
- Obblighi aggiuntivi sono enunciati per i titolari che forniscono servizi di comunicazione elettronica accessibili al pubblico (art. 32);
- Le misure minime di sicurezza obbligatorie sono introdotte all'art. 33;
- I prerequisiti per le misure minime di sicurezza sono disciplinate negli artt. 34 e 35, e le modalità tecniche sono rinviate al "*disciplinare tecnico*" (all. B);
- Le modalità di aggiornamento del disciplinare sono previste all'art. 36;

Misure minime (art. 33)

- Ci si trova nel contesto dell'art. 31 (obblighi di sicurezza) che tratta il più generale contesto delle misure idonee e preventive per la sicurezza;
- L'art. 33 stabilisce che i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate, volte ad assicurare un livello minimo di protezione dei dati personali;
- Le modalità di implementazione sono definite nell' Allegato B – il Disciplinare Tecnico.

Trattamenti con strumenti elettronici (art. 34)

- Il trattamento dati personali effettuato con strumenti elettronici è consentito solo se sono adottate le seguenti misure minime:

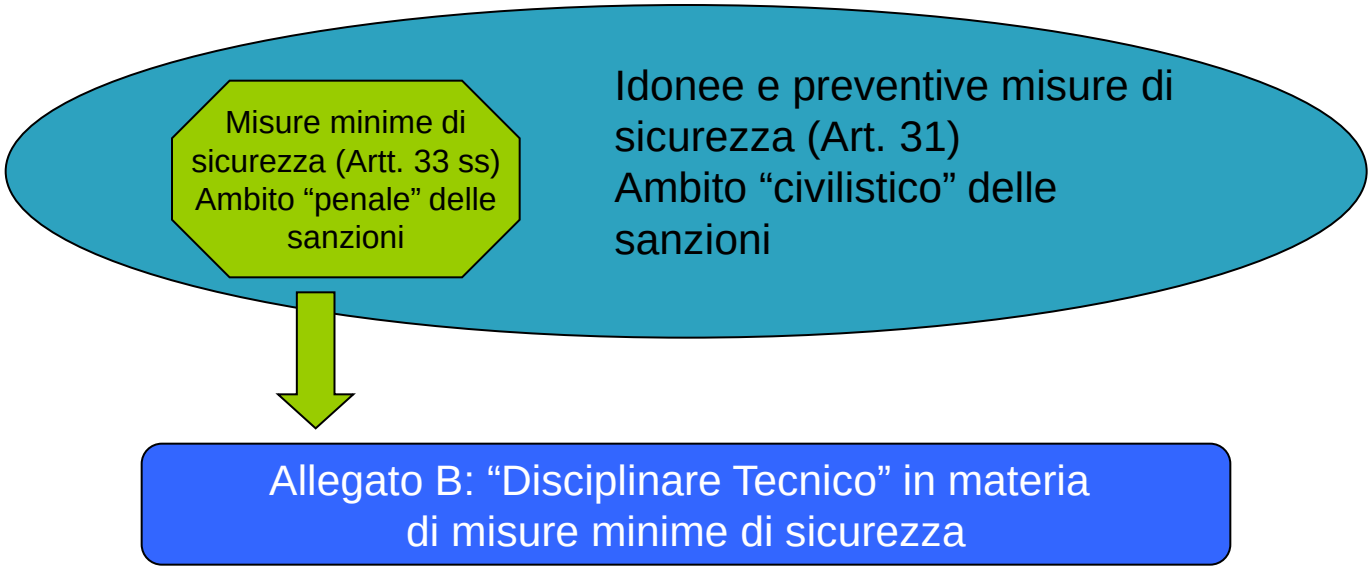
– Autenticazione informatica;
– Adozione di procedure di gestione delle credenziali di autenticazione;
– Organizzazione di un sistema di autorizzazione;
– Aggiornamento periodico dell'individuazione dei singoli incaricati e manutentori;
– Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti ed accessi non consentiti;
– Procedure per la custodia di copie di sicurezza e ripristino;
– Tenuta di un *aggiornato documento programmatico sulla sicurezza*;
– Adozione di tecniche di cifratura o codici identificativi per determinati trattamenti dati (stato di salute e vita sessuale) effettuati da organismi sanitari.

Trattamenti senza l'ausilio di strumenti elettronici (art. 35)

- E' consentito solo se sono adottate le seguenti misure minime:

– Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
– Previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
– 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.

Misure idonee e misure minime di sicurezza



La Notificazione (artt. 37-41)

- E’ lo strumento usato per rendere note al Garante le caratteristiche principali del trattamento;

- Importante novità: si passa da una previgente normativa che prevedeva un sistema “*in positivo*”, in cui vigeva un obbligo generale di notificazione salvo eccezioni espressamente previste, ad un sistema “*in negativo*”, in cui l’obbligo non sussiste più, salvo che il trattamento sia connotato da specifici elementi espressamente previsti dal Legislatore.

L’obbligo di notificazione

- Quando: l’obbligo va adempiuto in via *preliminare* rispetto al trattamento che richiede l’adempimento stesso;

- Va ripetuto, sempre in via preventiva, solo quando muti taluna delle informazioni rese;

- Va preventivamente notificata anche la cessazione del trattamento;

In quali casi notificare

- E’ necessario procedere alla notifica in quelle situazioni in cui le particolari modalità di trattamento o la natura dei dati personali facciano ritenere che sussistano potenziali rischi per la riservatezza e la dignità dell’individuo.

Attualmente i casi sono:

– Raccolta di dati biometrici;

– Prestazione di servizi sanitari in via telematica;

– Definizione di profili con strumenti elettronici;

– Gestione di dati sensibili da parte di agenzie di ricerca di personale per conto terzi;

– Gestione di banche dati per rischi creditizi o antifrode.

- In base al Codice il Garante ha potere di modificare (per eccesso o per difetto) l’elencazione attualmente contenuta nella Legge, tramite proprio provvedimento.

Modalità di notificazione (art. 38)

- La notificazione è una dichiarazione per la quale è prevista dal Legislatore una determinata forma e specifiche modalità di trasmissione:
  - Deve essere rilasciata secondo il modello messo a disposizione dal Garante e contenere le informazioni in esso richieste;
  - Deve essere trasmessa per via telematica, previa apposizione della firma digitale da parte del dichiarante;
  - Secondo le prescrizioni impartite dall'Autorità.

L’autorizzazione

- E’ condizione di liceità del trattamento dei dati sensibili (e, in alcuni ambiti, giudiziari);
- Provvedimento del Garante che acconsente al trattamento dati solo dopo aver verificato che questo non comporti particolari rischi di danni o di pericoli per i diritti, le libertà fondamentali e la dignità delle persone;
- E’ una deroga al generale sistema della libertà di trattamento per i dati “comuni”, posto che il trattamento dei dati sensibili o giudiziari è vietato, a meno che non sia consentito da una preventiva autorizzazione dell’Autorità;
- Rappresenta condizione di legittimità del trattamento operato nel settore privato, in quanto privati ed enti pubblici economici che intendano utilizzare dati sensibili devono soddisfare i seguenti requisiti (art. 26):

– Che l’interessato abbia acconsentito per iscritto;
– Che sia stata ottenuta l’autorizzazione del Garante.

Le autorizzazioni generali (art. 40)

- L’autorità acconsente ad operazioni di trattamento dati sensibili o giudiziari a determinate condizioni e per determinati fini;

- Il Garante ha rilasciato delle autorizzazioni generali per tipologia di trattamenti;

Le autorizzazioni generali“vigenti”

- Autorizzazione n. 1 del 2004:
  trattamento dei dati sensibili nei rapporti di lavoro;
- Autorizzazione n. 2 del 2004:
  trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale;
- Autorizzazione n. 3 del 2004:
  trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni;
- Autorizzazione n. 4 del 2004:
  trattamento dei dati sensibili da parte dei liberi professionisti;
- Autorizzazione n. 5 del 2004:
  trattamento dei dati sensibili da parte di diverse categorie di titolari;
- Autorizzazione n. 6 del 2004:
  trattamento di dati sensibili da parte degli investigatori privati;
- Autorizzazione n. 7 del 2004:
  trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici;

Richieste di autorizzazione (art. 41)

- Qualora il trattamento non sia già stato regolamentato, o le modalità di trattamento differiscano da quelle prospettate nella relativa autorizzazione generale, il Titolare deve sottoporre all'Autorità specifica richiesta di autorizzazione;
- La richiesta dev'essere preventiva rispetto al trattamento che si intende effettuare;
- Il Garante comunica la decisione entro 45 giorni dal ricevimento della richiesta;
- La mancata pronuncia entro il termine equivale a rigetto.

Le misure minime del disciplinare (All. B)

- Indica le modalità tecniche e organizzative da adottare a cura del Titolare, dei Responsabili ove designati e dell'Incaricato, in caso di trattamento con strumenti elettronici;

- E' strutturato in 7 sezioni:
  – Sistema di autenticazione informatica;
  – Sistema di autorizzazione informatica;
  – Altre misure di sicurezza;
  – Documento Programmatico Sulla Sicurezza;
  – Ulteriori misure in caso di trattamento di dati sensibili o giudiziari;
  – Misure di tutela e garanzia;
  – Trattamenti senza l'ausilio di strumenti elettronici;

Il DPSS

- Redatto ed aggiornato entro il 31 Marzo di ogni anno;
- Il Documento Programmatico Sulla Sicurezza descrive, tra l'altro, come e quali misure di sicurezza *organizzativa*, *fisica* e *tecnologica* l'azienda:
  – Abbia implementato;
  – Abbia deciso di implementare nel corso dell'anno;
  – Abbia deliberato di implementare in futuro (programmazione);
- Il DPSS è il documento sulla base del quale è possibile dimostrare quanto fatto in azienda a protezione dei dati personali trattati.
- Dal 2011 ne è stata sospesa la obbligatorietà a fronte della crisi.
- Nel 2012 il DPSS non è più obbligatorio in conseguenza della abrogazione dell'obbligo contenuto nel Decreto Monti.

Informazioni nel DPSS - 1/2

- L’elenco dei trattamenti dei dati personali;
- La distribuzione di compiti e responsabilità nell’ambito delle strutture preposte al trattamento del titolare;
- L’analisi dei rischi che incombono sui dati;
- Le misure da adottare per garantire l’integrità e la disponibilità dei dati rilevanti ai fini della loro custodia e accessibilità;
- Le misure da adottare a protezione delle aree e dei locali;
- La descrizione dei criteri da adottare per il ripristino della disponibilità dei dati a seguito di danneggiamento e/o distruzione;
- La previsione della formazione sugli incaricati;
- La descrizione dei criteri da adottare per garantire l’attuazione delle misure di sicurezza in caso di trattamenti svolti all’esterno;
- L’individuazione dei criteri da adottare per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e/o la vita sessusale (medici e organismi sanitari);

Ulteriori Informazioni nel DPSS - 2/2
Per dati sensibili e giudiziari

- Adozione di idonei strumenti elettronici per proteggere i dati personali contro accessi abusivi di cui all'art. 615ter c.p. (accesso abusivo a sistema informatico o telematico);

- Distruzione o inutilizzabilità di supporti rimovibili contenenti dati personali;

- Ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici (politiche di backup);

- Cifratura od adozione di codici identificativi dei dati idonei a rivelare lo stato di salute e/o la vita sessuale (obbligo per gli organismi sanitari o per i medici);

Tutela dei diritti dell'interessato

Dinanzi al Garante:

- SEGNALAZIONE (per sollecitare un controllo quando non si hanno dati per effettuare un reclamo)
- RECLAMO CIRCOSTANZIATO (per denunciare la violazione di regole di trattamento)
- RICORSO (per esercitare i diritti dell'interessato ed ottenere la immediata sospensione del trattamento e la cessazione del comportamento illegittimo)

In sede giudiziaria: dinanzi a Giudice Ordinario

Alternativo al ricorso al Garante (no ambedue, la proposizione dell'uno esclude l'altro)

- RICORSO per esercitare i diritti dell'interessato ed ottenere la immediata sospensione del trattamento e la cessazione del comportamento illegittimo ed il risarcimento del danno. La sentenza è Inappellabile: ammesso solo Ricorso per Cassazione.

Violazioni e sanzioni

Illeciti Penali che comportano l'applicazione di pene:

- trattamento illecito di dati
- falsità nelle notificazioni
- mancata osservanza alle prescrizioni del Garante
- omessa adozione delle misure minime di sicurezza.

Violazioni amministrative (ammenda):

- omessa informativa all'interessato
- indebita cessione dei dati
- omessa informativa al Garante
- omessa, incompleta o tardiva notificazione

IL NUOVO REGOLAMENTO EUROPEO UE 2016/679 - GDPR

- Il Regolamento (UE) 2016/679 mira ad introdurre una legislazione – in materia di protezione dati – uniforme e valida in tutta Europa, affrontando temi innovativi come il diritto all'oblio e alla portabilità dei dati e stabilendo anche criteri che, da una parte, responsabilizzano maggiormente imprese ed enti rispetto alla protezione dei dati personali e, dall'altra, introducono notevoli semplificazioni e sgravi degli adempimenti per chi si conforma alle regole.

IL NUOVO REGOLAMENTO EUROPEO UE 2016/679

- E’ stato pubblicato il **4 maggio 2016** sulla Gazzetta Ufficiale dell’Unione Europea /GUUE e sarà definitivamente e direttamente applicabile in tutti i Paesi UE a partire dal **25 maggio 2018**, data per la quale dovrà essere garantito l’allineamento della normativa nazionale con le disposizioni del Regolamento.

Oggetto e finalità

- Stabilire un complesso normativo volto alla protezione del trattamento dei dati personali delle persone fisiche, nonché a disciplinare le regole sulla libera circolazione dei dati personali.

Definizioni

- “dato personale”: qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”)
- “trattamento” del dato: qualsiasi operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o ad insieme di dati personali.

Ambito di applicazione materiale

- Il Regolamento si applicherà sia al **trattamento interamente o parzialmente automatizzato** di dati personali, sia al **trattamento non automatizzato** di dati personali contenuti in un archivio o destinati a figurarvi (ART. 2). Lo stesso articolo stabilisce espressamente i casi sottratti alla portata di questa disposizione, tra cui i trattamenti effettuati dalle autorità di pubblica sicurezza.

Ambito di applicazione territoriale

- Dal punto di vista “geografico”, la nuova disposizione europea rovescia il tradizionale principio di stabilimento, sancendo l’applicabilità della disciplina dettata “*indipendentemente dal fatto che il trattamento sia effettuato o meno nell’Unione*” e stabilendo l’applicazione delle sue regole **anche nei confronti dei Titolari e Responsabili non stabiliti nell’UE, quando** le attività di trattamento riguardano:

Ambito di applicazione territoriale

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)

L'art. 25 del Regolamento introduce due differenti principi:

- "***PRIVACY BY DESIGN***",
- "***PRIVACY BY DEFAULT***"

Privacy by design

- il titolare del trattamento deve adottare ed attuare misure tecniche ed organizzative, adeguate sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati;

Privacy by default

- il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento

Segue: Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)

- L'utente diventa quindi il punto di partenza per sviluppare il progetto in base alla legge sulla *privacy*, tramite un approccio ***user-centric*.** Pertanto, ogni volta che un progetto inizia deve prendere in considerazione, prima di tutto, il ruolo dell'utente, progettando tutto attorno alla persona fisica.

Data breach

- Sulla base della normativa europea, il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori **l'obbligo di comunicare eventuali violazioni di dati personali** ("*data breach*") all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

Data breach

- Mentre per la **notifica all'autorità** di controllo è richiesto "*un **rischio per i diritti e le libertà degli individui***", per la **notifica al diretto interessato** è necessario che il **rischio** sia "***elevato***": in quest'ultimo caso, è richiesta una soglia di pericolo maggiore anche per evitare inutili allarmismi da parte dei soggetti interessati.

Registro delle attività di trattamento

- Altra novità di rilievo è l'introduzione dell'**obbligo per ogni azienda titolare del trattamento** dei dati di tenere un "**registro delle attività" di trattamento**, svolte sotto la propria responsabilità, nonché quello di effettuare una "**valutazione di impatto sulla protezione dei dati**".

Valutazione d’impatto sulla protezione dei dati

E’ richiesto in relazione

a) ai trattamenti automatizzati, ivi compresa la profilazione,

b) ai trattamenti su larga scala di categorie particolari di dati (sensibili), nonché relativamente ai dati ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico.

Valutazione d’impatto sulla protezione dei dati

Sarà ad ogni modo il Garante Privacy (per quanto riguarda l'Italia), a redigere e rendere pubblico l'elenco delle tipologie di trattamenti soggetti al requisito della "valutazione di impatto sulla protezione dei dati”.

Data Protection Officer (artt. 37 e ss.)

- Tra i nuovi adempimenti è prevista l'adozione di una nuova figura professionale obbligatoria: **il Responsabile per la protezione dei dati personali** (*Data Protection Officer o "DPO"*).
- Il *DPO* è un supervisore indipendente che sarà designato da soggetti apicali sia dalle pubbliche amministrazioni che in ambito privato.

Data Protection Officer (artt. 37 e ss.)

Sarà obbligatorio all'interno di tutte:

a) le **aziende pubbliche** nonché in tutte quelle ove i trattamenti presentino specifici rischi;

b) le aziende nelle quali sia richiesto un **monitoraggio regolare e sistematico degli "interessati"** su larga scala,

c) le aziende che trattano i c.d. "**dati sensibili**".

Data Protection Officer (artt. 37 e ss.)

Il Responsabile per la protezione dei dati personali è tenuto a:

- **informare e consigliare** il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento;
- **verificare** l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi auditors;

Data Protection Officer (artt. 37 e ss.)

- **fornire**, se richiesto, **pareri** in merito alla valutazione d'impatto sulla protezione dei dati e a sorvegliare i relativi adempimenti;
- fungere da **punto di contatto per gli "interessati",** in merito a qualunque problematica connessa al trattamento dei loro dati nonché all'esercizio dei loro diritti;
- fungere da **punto di contatto per il Garante** per la protezione dei dati personali oppure, eventualmente, per consultare il Garante di propria iniziativa.

Data Protection Officer (artt. 37 e ss.)

- **Attenzione:** la figura del DPO non va confusa con quella di un responsabile *privacy ex* art. 29 del nostro Codice Privacy.
- Elemento cruciale che differenzia le due figure: mentre il primo deve essere indipendente ed autonomo, il secondo deve agire seguendo soltanto le istruzioni del titolare del trattamento

Diritti dell'interessato: il diritto all'oblio (art. 17)

- Una delle principali novità portata dal Regolamento riguarda il **diritto all'oblio**, ovvero la **possibilità per l'interessato di decidere che siano cancellati e non sottoposti ulteriormente al trattamento** i propri dati personali non più necessari per le finalità per le quali sono stati raccolti *ab origine*.

Diritti dell'interessato: il diritto all'oblio (art. 17)

- Lo stesso articolo riconosce espressamente il "diritto all'oblio" anche nel caso di **revoca del consenso** o quando l'interessato si sia **opposto al trattamento** dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali **non sia altrimenti conforme al Regolamento**.

Diritti dell'interessato: il diritto all'oblio (art. 17)

Tale diritto è oggetto di tre considerando nel preambolo del Regolamento:

- *n.65* "Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che la riguardano e il diritto all'oblio se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento […]";

Diritti dell’interessato: il diritto all’oblio (art. 17)

- *n. 66* "Per rafforzare il diritto all'oblio nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali";

Diritti dell’interessato: il diritto all’oblio (art. 17)

- *n. 156* "[…] Gli Stati membri dovrebbero essere autorizzati a fornire, a specifiche condizioni e fatte salve adeguate garanzie per gli interessati, specifiche e deroghe relative ai requisiti in materia di informazione e ai diritti alla rettifica, alla cancellazione, all'oblio, alla limitazione del trattamento, alla portabilità dei dati personali, nonché al diritto di opporsi in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche […]"

Diritti dell'interessato: il diritto all'oblio (art. 17)

- In ambito nazionale il Garante della Privacy ha chiarito tramite una propria pronuncia come lo stesso **diritto all'oblio debba essere bilanciato con il diritto di cronaca**; difatti, gli utenti non possono ottenere da Google la cancellazione dai risultati di ricerca di una notizia che li riguarda se si tratta di un fatto recente e di rilevante interesse pubblico

Diritti dell'interessato: il diritto alla "portabilità dei dati" (art. 20)

- si intende il riconoscimento sia del diritto dell'interessato a **trasferire i propri dati** (es. quelli relativi al proprio "profilo utente") da un sistema di trattamento elettronico (es. Social Network) ad un altro senza che il Titolare possa impedirlo, sia del diritto **di ottenere gli stessi in un formato elettronico strutturato e di uso comune** che consenta di farne ulteriore uso.

Sanzioni (artt. 83 e 84).

- Il nuovo Regolamento prevede che ogni autorità di controllo abbia il potere di imporre sanzioni amministrative. Le stesse verranno inflitte in funzione delle circostanze di ogni singolo caso, tenendo quindi conto della natura, della gravità e della durata della violazione, nonché del carattere doloso o colposo della violazione nonché degli altri fattori puntualmente elencati dallo stesso art. 83.

Sanzioni (artt. 83 e 84).

- Le sanzioni oltre a dover essere proporzionate alla violazione posta in essere devono essere dissuasive, così da evitare che lo stesso soggetto reiteri il proprio comportamento.
- Pure se le autorità di controllo potranno stabilire autonomamente il *quantum* della sanzione tenendo conto degli indici sanciti dallo stesso Regolamento, tuttavia è la stessa disposizione europea che ne fissa l'importo pecuniario massimo che può essere applicato.

Sanzioni (artt. 83 e 84).

- In effetti, a seconda del trasgressore (persona fisica o impresa) ed a seconda della violazione commessa, la sanzione potrà raggiungere un massimo di:
- *10.000.000,00 di euro*, o per le imprese, *fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente*27; alternativamente
- *20.000.000,00 di euro*, o per le imprese, *fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.*

Norma UNI 11697:2017

- **Titolo**: Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza
- **Data entrata in vigore:** 30 novembre 2017

Norma UNI 11697:2017

- La norma definisce i profili professionali relativi al trattamento e alla protezione dei dati personali coerentemente con le definizioni fornite dall'EQF e utilizzando gli strumenti messi a disposizione dalla UNI 11621-1 "Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 1: Metodologia per la costruzione di profili professionali basati sul sistema e-CF".

Norma UNI 11697:2017

- La norma fa riferimento ai profili professionali relativi al trattamento ed alla protezione dei dati personali ed è stata sviluppata secondo l'ormai ben noto schema europeo chiamato EQF-European Qualification framework, che rappresenta la linea guida per sviluppare norme applicabili ad attività professionali non regolamentate e non ordinistiche.
- Le **figure professionali** delineate dalla norma UNI sono le seguenti:

Data Protection Officer (DPO)

- supporta il titolare o il responsabile del trattamento nell'applicazione e nell'osservanza del Regolamento (UE) 2016/679 ("Regolamento"), in conformità all' art. 37 (Designazione del Responsabile della protezione dei dati) ha il compito principale di garantire, in maniera indipendente, l'applicazione interna delle disposizioni del Regolamento da parte del Titolare del trattamento.

Data Protection Officer (DPO)

- Il DPO è inoltre tenuto a tenere un registro di tutte le operazioni di trattamento che coinvolgono dati personali effettuato da parte dell'istituzione. Il registro, che deve contenere le informazioni circa lo scopo e le condizioni delle operazioni di trattamento, dovrebbe essere accessibile a tutti gli interessati.

Manager Privacy

- assiste il titolare nelle attività di coordinamento di tutti i soggetti che – nell'organizzazione – sono coinvolti nel trattamento di dati personali (responsabili, incaricati, amministratori di sistema, ecc.), garantendo il rispetto delle norme in materia di privacy e il mantenimento di un adeguato livello di protezione dei dati personali.

Specialista Privacy

- figura di supporto appositamente formato egli collabora con il Manager Privacy e cura la corretta attuazione del trattamento dei dati personali all'interno dell'organizzazione, svolgendo le attività operative che, di volta in volta, si rendono necessarie durante tutto il ciclo di vita di un trattamento di dati personali. Tale figura è richiesta soprattutto all'interno di grandi organizzazioni aziendali (che incide su più uffici e/o stabilimenti con una diversa collocazione territoriale) ove si rende necessario creare più "presidi" privacy;

Valutatore Privacy

- figura dotata di una apposita formazione che si caratterizza per la sua terzietà sia nei confronti del Manager che dello Specialista Privacy; egli esercita una attività di monitoraggio (audit) andando ad esaminare periodicamente il trattamento dei dati personali e valutando il rispetto delle normative di settore emanate a livello nazionale, comunitario e internazionale. Egli, inoltre, approva le misure necessarie per l'eliminazione di eventuali non conformità alla disciplina prescritta.

GRAZIE DELL'ATTENZIONE

Avv. Sabrina Primavera
Via Nomentana 909
00137 Roma
Tel. 068276766
www.pride29.it