LINEE GUIDA E ADEMPIMENTI IN MATERIA DI TUTELA DEI DATI PERSONALI

DEFINIZIONI

- Per **trattamento** si intende qualunque operazione o complesso di operazioni 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. Tale trattamento può avvenire con o senza l'ausilio di strumenti elettronici.
- Per **dato personale** si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili anche indirettamente mediante riferimento a qualsiasi altra informazione, come numeri di identificazione personale. Esempi di dati personali sono: il nome e il cognome, l'indirizzo, il codice fiscale, la Partita IVA e i recapiti telefonici.
- Per **dati identificativi** si intendono i dati personali che permettono l'identificazione diretta dell'interessato.
- Per **dati particolari/sensibili** si intendono 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.
- Per **dati giudiziari** si intendono i dati personali idonei a rivelare informazioni relative al casellario giudiziale, alle sanzioni amministrative, ai carichi pendenti, alla qualità di imputato o di indagato.
- Per **banca di dati** si intende qualsiasi complesso organizzato di dati personali, ripartito in una o più unità.
- Per **misure minime** si intende il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza volte a garantire un livello minimo di protezione dai rischi ai quali i dati sono sottoposti, come ad esempio la distruzione o la perdita, l'accesso non autorizzato e il trattamento non consentito o non conforme alle finalità della raccolta.
- Per Titolare del trattamento si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Per fare un esempio, nelle aziende private tale soggetto coincide in genere con l'amministratore o altro rappresentante legale;
- Il Titolare può nominare uno o più **Responsabili del trattamento**. Per responsabile si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti al trattamento di dati personali dal titolare. In genere si tratta di una persona di fiducia al quale il Titolare del trattamento demanda tutti i compiti legati alla corretta organizzazione del lavoro di raccolta dati nonché della loro custodia e trattamento nel pieno rispetto del dettato normativo;
- I Responsabili o il Titolare possono infine nominare i cosiddetti **Addetti**, coloro i quali compieranno materialmente le operazioni di trattamento. Agli incaricati possono essere assegnati compiti come l'inserimento, la modifica, la cancellazione e la stampa dei dati attenendosi sempre alle istruzioni loro impartite;
- Il titolare può decidere di nominare anche un **responsabile esterno** alla struttura. In tal caso sarà quest'ultimo a nominare gli incaricati al trattamento e vigilare sul loro operato e sul rispetto delle misure di sicurezza. Accettando l'incarico il Responsabile esterno svolgerà le sue mansioni nella piena consapevolezza degli obblighi assunti e delle responsabilità che ne derivano.

Oltre a questi soggetti, espressamente previsti dalla normativa, il Titolare del trattamento può prevedere altre figure necessarie ai fini del corretto trattamento dei dati e della loro sicurezza, come ad esempio:

- **L'amministratore di sistema** il quale si occuperà di gestire tutte le esigenze informatiche legate al trattamento dei dati con strumenti elettronici. Alcuni esempi sono l'installazione di programmi antivirus e l'utilizzo di software che limitano i rischi di intrusioni informatiche nei PC utilizzati per il trattamento dei dati;

- **Il custode delle password** che provvederà a conservare in luogo sicuro, senza divulgarle, tutte le parole chiave o qualsiasi altra credenziale di autenticazione ai sistemi informatici fornita ad ogni incaricato al trattamento;
- **Custode o vigilante** per la sorveglianza dei locali nei quali avviene il trattamento dei dati o dove vengono custodite le copie di sicurezza delle banche dati.

Nulla vieta che tutti questi ruoli possano essere ricoperti dallo stesso soggetto e, pertanto, tutte le figure previste dal legislatore saranno racchiuse nella persona del Titolare del Trattamento. Se da un lato esistono soggetti tenuti ad adottare misure di sicurezza idonee a garantire la riservatezza dei dati e il loro trattamento secondo legge, dall'altro lato vi è l'**Interessato** che è la persona fisica, persona giuridica, ente o associazione cui si riferiscono i dati personali oggetto del trattamento. L'interessato, ad esempio, è il soggetto privato che fornisce i propri dati ad una pubblica amministrazione o ad un'azienda per l'ottenimento di un determinato servizio. L'Interessato ha il diritto di chiedere al titolare, tra le altre cose citate all'articolo7 del codice sulla privacy:

- le finalità e le modalità del trattamento dei dati che lo riguardano;
- l'indicazione dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati;
- la rettifica, l'integrazione o la cancellazione dei dati quando vi ha interesse;

Inoltre l'interessato ha il diritto di opporsi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta o all'invio di materiale pubblicitario.

Infine, l'organo al quale è demandato il compito di vigilare sul corretto utilizzo delle banche dati e sul rispetto della normativa vigente è il cosiddetto **Garante della privacy** costituito da quattro componenti, eletti due alla Camera dei deputati e due dal Senato della Repubblica. I compiti del Garante sono molteplici. Fra i più rilevanti citiamo:

- Rilasciare le autorizzazioni per il trattamento dei dati personali;
- Esaminare i reclami ricevuti dai soggetti interessati;
- Vietare il trattamento non corretto o illecito dei dati;
- Disporre ispezioni nei luoghi dove avviene il trattamento dei dati.

Per eseguire questi controlli il Garante può avvalersi della collaborazione di altri organi dello Stato come la Guardia di Finanza.

ADEMPIMENTI OBBLIGATORI

La normativa prevede specifici adempimenti in capo al Titolare del trattamento regolamentando sia la fase che precede la raccolta di dati, che successivamente le modalità di trattamento.

In particolare, il Titolare deve fornire, oralmente o per iscritto, idonea **informativa** ogniqualvolta proceda alla raccolta di dati. Tale informativa deve contenere:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati;
- gli estremi del titolare e del responsabile del trattamento;
- i diritti riconosciuti all'interessato.

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il **consenso espresso** dell'interessato, escluse le precise eccezioni individuate dal Garante Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili e/o giudiziari.

Una volta acquisiti i dati, il Titolare del trattamento deve approntare tutte le misure operative e di sicurezza idonee a garantire il trattamento dei dati secondo legge. In particolare deve sincerarsi che i dati siano:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti, legittimi ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;

• pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; • 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 sono stati raccolti o successivamente trattati.

Infine, in caso di cessazione di un trattamento, i dati possono essere:
• distrutti;
• ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
• conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
• conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta.

MISURE DI SICUREZZA DA ADOTTARE

Il legislatore ha previsto due tipologie di trattamento di dati:
• Trattamenti con l'ausilio di strumenti elettronici
• Trattamenti senza l'ausilio di strumenti elettronici

Nel caso di **Trattamento con l'ausilio di strumenti elettronici,** il titolare deve provvedere, anche per tramite di una persona appositamente incaricata, ad approntare tutte quelle soluzioni informatiche idonee a ridurre al minimo il rischio di infezioni da programmi virus, intrusioni nella rete informatica da parte di soggetti non autorizzati o perdita dei dati.
Il codice della privacy elenca specifiche misure di sicurezza fra le quali:

• **Adozione di credenziali di autenticazione:** come recita il Disciplinare Tecnico in materia di misure minime di sicurezza, "*il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di **credenziali di autenticazione** che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti*".
Pertanto ogni soggetto incaricato al trattamento di dati deve avere un nome utente e una **Password**, quest'ultima impostata dallo stesso incaricato al primo utilizzo del PC col quale effettua il trattamento dei dati. La password è composta da almeno otto caratteri, non deve contenere riferimenti facilmente riconducibili all'incaricato e andrà modificata almeno ogni sei mesi, se trattasi di dati comuni, o ogni tre mesi in caso di trattamento di dati sensibili o giudiziari. La password deve essere conosciuta solo dall'incaricato. Il titolare o il responsabile del trattamento devono prevedere le modalità di accesso al sistema protetto da password in caso di prolungata assenza dell'incaricato.

• **Protezione degli strumenti elettronici:** gli elaboratori utilizzati per il trattamento dei dati devono essere protetti dai rischi informatici legati all'azione di virus o intrusioni non autorizzate nella rete. Gli antivirus dovranno essere aggiornati con cadenza almeno semestrale anche se il proliferare di virus informatici ne consiglierebbe l'aggiornamento con frequenza maggiore.
Anche i sistemi operativi e i programmi installati nei PC utilizzati per il trattamento dei dati devono essere aggiornati per prevenirne la vulnerabilità e correggerne i difetti. In genere tali aggiornamenti sono messi a disposizione periodicamente dalle stesse case produttrici dei software e sono solitamente scaricabili anche da internet. Gli aggiornamenti devono avere una cadenza almeno annuale; in caso di dati sensibili o giudiziari l'aggiornamento deve essere eseguito semestralmente.

• **Creazione di copie di sicurezza:** a garanzia della salvaguardia dei dati oggetto di trattamento, il nuovo codice prescrive l'adozione di idonee procedure per la creazione di copie di salvataggio. Tali copie dovranno essere ripristinate in caso di distruzione o danneggiamento dei dati in tempi compatibili con i diritti degli interessati e non superiori a sette giorni. Le copie di salvataggio, se non più utilizzate, sono distrutte o rese inutilizzabili in modo tale da rendere illeggibile il loro contenuto. Sempre in tempi compatibili con i diritti degli interessati devono essere riportati al normale stato d'uso gli strumenti elettronici danneggiati utilizzati per l'accesso alle banche dati.

• **Cifratura di dati sanitari:** gli organismi sanitari sono tenuti ad adottare tecniche informatiche di cifratura di dati per garantire la segretezza delle informazioni idonee a rivelare lo stato di salute o la vita sessuale degli interessati.

Tutte le soluzioni informatiche adottate devono essere periodicamente analizzate ed eventualmente aggiornate in base al progresso tecnologico o alle mutate esigenze dell'azienda. Per chi invece effettua **trattamenti di dati senza l'ausilio di strumenti elettronici** è prevista l'adozione di una serie di misure minime di sicurezza volte anch'esse a garantire l'integrità dei dati e la loro sicurezza. Tali misure sono:

• **Impartire istruzioni scritte agli incaricati** per lo svolgimento delle operazioni di trattamento degli atti e dei documenti contenenti dati personali.

• Per gli incaricati, **custodire gli atti e controllare i documenti contenenti dati sensibili o giudiziari** per tutta la durata del loro utilizzo fino alla restituzione, evitando che vi possano accedere persone prive di autorizzazione.

• **Controllare gli accessi agli archivi contenenti dati particolari o giudiziari.** Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate. A tale scopo il Titolare può ricorrere alla nomina di personale appositamente preposto alla vigilanza dei locali.

Tutte le misure adottate devono essere anche in questo caso aggiornate periodicamente per adeguarle alle nuove esigenze organizzative o a un mutato livello di rischio.