Dispense
INCONTRO
"Privacy, che fare?"

A cura di: Luciana Beccaria
Associazione "help For You"

1) Le norme a tutela dei dati personali

Le norme principali di riferimento per il trattamento dati personali sono:

- **Codice Privacy (D. Lgs. 1956/2003)**, recentemente "novellato" (non è un semplice aggiornamento, ma variano parti importanti del testo) dal **D. Lgs 101/2018**
- **Regolamento UE 679/2016 o GDPR (General Data Protection Regulation)**; obbligatorio uniformarsi al GDPR dal **25.5.2018.**
- **Disposizioni** e provvedimenti del **Garante** + eventuali **"Codici di Condotta"** di categoria

2) Cosa si intende per "DATO PERSONALE"

Dati personali

«Dato personale» è **qualunque informazione che consenta l'identificazione dei soggetti interessati**; quindi è "dato" anche se deriva da suoni o da immagini - come potrebbe essere una registrazione sonora, una foto od un filmato - da un'intervista o un colloquio, così come qualsiasi altra dichiarazione, opinione o manifestazione del pensiero proveniente dall'interessato (uno scritto, un saggio, un articolo, ecc.), costituiscono senz'altro informazioni che riguardano la sua persona e come tali «dati personali», essendo del tutto irrilevante la forma in cui esse sono trattate oppure gli eventuali supporti che le contengono. Sono dati anche gli indirizzi IP, per esempio, i dati di spostamento (geolocalizzazione), l'indirizzo di posta elettronica.

Dati "particolari"

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** od organizzazioni a **carattere religioso, filosofico, politico o sindacale,** nonché i dati personali idonei a rivelare lo **stato di salute e la vita sessuale.**

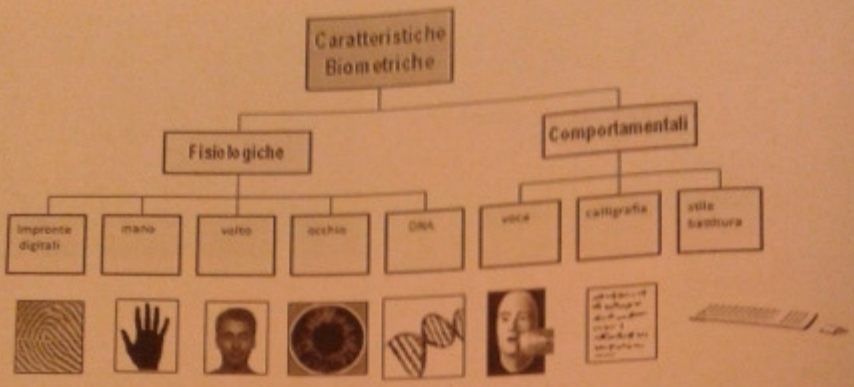
Dati giudiziari

I dati personali idonei a rivelare provvedimenti giudiziari, fra cui anche il casellario giudiziale, l'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.

Dati "biometrici"

I dati che vengono utilizzati per identificare o autenticarsi 8es. per accessi) usando un elemento "biometrico" considerato:

- **universale**: l'elemento è presente in tutte le persone;
- **unico**: l'elemento biometrico è diverso per ogni persona e la "distingue" da tutte le altre (es impronta digitale)
- **permanente**: ogni persona conserva il proprio elemento biometrico nel corso del tempo.



Tecniche per trattare dati biometrici possono essere :

- di tipo **fisico o fisiologico**: misurano le caratteristiche fisiologiche di una persona. Esse comprendono: la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, l'analisi della retina, il riconoscimento del volto, la geometria della mano, il riconoscimento della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi della struttura del DNA, l'analisi dei pori della pelle ecc..
- Di **tipo comportamentale**: misurano il comportamento di una persona. Esse comprendono, ad esempio, la verifica della firma manoscritta, l'analisi della battitura su tastiera, l'analisi dell'andatura.

3) Cosa si intende per "TRATTAMENTO"

Trattamento è l'utilizzo, la raccolta, la conservazione, la distruzione, e comunque **qualunque azione riferita al dato** (es. anche solo "leggere" il dato).

Modalità del trattamento e requisiti dei dati

I dati personali devono essere:

a) trattati in **modo lecito** e con correttezza;

b) raccolti e registrati per **scopi determinati, espliciti e legittimi**, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) **esatti** e, se necessario, aggiornati;

d) **pertinenti, completi e non eccedenti** rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) **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.

I dati trattati in violazione della normativa in materia non possono essere utilizzati.

Come trattare i dati in modo "lecito?

Significa che per trattare il dato ci deve essere una **"base giuridica"** cioè qualche forma di "autorizzazione" a farlo.

Questo può essere, ad esempio:

- un contratto
- una norma di legge
- un'autorizzazione generica o specifica del Garante

- la tutela della salute dell'interessato (es. trattamenti sanitari)
- la tutela dell'ordine pubblici e della sicurezza
- un interesse legittimo del titolare (es. videosorveglianza, tesa a proteggere i beni aziendali o le persone: questo comunque va bene individuato, definito e analizzato prima di procedere; es. videosorveglianza, e se ne deve dare apposito avviso con vetrofanie, informative specifiche ecc.).
- la difesa dei diritti (devo potermi ad. es. difendere in giudizio).

In assenza di una queste basi, per trattare i dati devo avere il **CONSENSO delle persone interessate**; se i dati riguardano un minore, si devono adottare maggiori cautele, e **comunque raccogliere il "consenso" dei genitori**.

Principi specifici per le PA (pubbliche amministrazioni)

Principi generali

- Il trattamento dati è consentito solo per lo svolgimento delle funzioni e dei fini istituzionali (principio funzionale).
- Non necessita del consenso, ma vanno osservati i limiti stabiliti dal codice privacy, da leggi e regolamenti.

Principi applicati ai dati personali diversi da quelli sensibili e giudiziari

- Il trattamento da parte di un **soggetto pubblico** riguardante dati diversi da quelli sensibili e giudiziari è consentito **anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente**.
- La comunicazione ad **altri soggetti pubblici** è **ammessa** se prevista da una **norma di legge** o di regolamento o se **necessaria per lo svolgimento di funzioni istituzionali**; La comunicazione da parte di ente PA a **privati o a enti pubblici economici** e la diffusione da parte di un soggetto pubblico sono ammesse **unicamente** quando sono previste da una **norma di legge o di regolamento**.
- Le notizie concernenti lo **svolgimento delle prestazioni di chiunque sia addetto a una funzione pubblica e la relativa valutazione sono rese accessibili dall'amministrazione di appartenenza**. Non sono invece rese accessibili, se non nei casi previsti dalla legge, le notizie su natura infermità e impedimenti personali/familiari che causino l'astensione dal lavoro e le componenti della valutazione o le notizie sul rapporto di lavoro che rivelino informazioni "sensibili".

Il trattamento dei dati sensibili da parte di soggetti pubblici

- I **dati sensibili** possono essere trattati **solo se autorizzati da espressa disposizione** di legge che specifichi: tipi di dati trattati / operazioni eseguibili / **finalità di rilevante interesse pubblico perseguite**.
- Va previsto l'utilizzo di tecniche di cifratura e codici identificativi
- Vanno conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
- **I dati idonei a rivelare lo stato di salute non possono essere diffusi**.

4) L'informativa e il consenso

Perché si dà "l' Informativa"

Il Titolare DEVE **informare l'interessato sui suoi diritti e su come i dati verranno raccolti, conservati e trattati**.
Per farlo di solito usa un documento chiamato "INFORMATIVA". Ve ne possono essere di diverso tipo, a seconda del tipo e del fine del trattamento (es. clienti, dipendenti, videosorveglianza, il web, ecc.
Gli articoli 13 e 14 del GDPR prevedono che l' informativa per il trattamento dei dati personali contenga alcuni dati in più rispetto a quanto già previsto dal precedente Codice Privacy. In particolare, nell'informativa si **deve indicare**:

- l'identità e i dati di contatto del titolare e, se nominato, i dati di contatto del DPO,
- la base giuridica del trattamento,
- il proprio interesse legittimo (se questo è base del trattamento, es. videosorveglianza)
- il periodo di conservazione dei dati personali
- se trasferisce i dati personali in Paesi terzi e attraverso quali strumenti
- informare l'interessato della possibilità di avvalersi dei suoi diritti (anche quello di presentare reclamo al Garante)
- informare dell'eventuale adozione di processi decisionali automatizzati.
- indicare se è obbligatorio o no fornire tali dati, e le conseguenze se non lo si fa.

L'informativa deve avere **un linguaggio semplice, comprensibile e trasparente** per l'interessato e deve essere **fornita prima di effettuare il trattamento, quindi prima della raccolta dei dati**. Se i dati non sono raccolti direttamente dall'interessato, ma

arrivano da altre fonti, l'informativa va data entro un mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati a terzi o all'interessato.

Nel caso si faccia profilazione (analisi delle preferenze, gusti, inclinazione delle persone, luogo in cui si trovano ecc. , cioè quel che fanno di norma tutte le APP), l'informativa deve specificarlo così come deve indicare anche la logica del processo di decisione (es. nel caso si faccia analisi automatica di un curriculum, come succede in IKEA, in cui l'analisi non la fa una persona ma un processo automatico) e le conseguenze previste per l'interessato se nega il consenso.

Il Consenso

Data l'informativa, occorre, a meno che non vi siano basi giuridiche che autorizzano a trattare il dato, richiedere il **"consenso" della persona cui si riferiscono**, cioè lui mi deve aver dato la SUA autorizzazione a farlo. Il Consenso deve essere:

- libero, (es. no a caselle pre-compilate)
- specifico (si deve indicare per quale fine si chiede)
- informato (prima si dà informativa, poi si chiede il consenso)
- manifestato con dichiarazione o un'azione positiva inequivocabile (flag, crocetta, ecc.)
- revocabile (si deve poter "cambiare idea" e revocare consenso dato in precedenza)

Non necessariamente il consenso deve essere "scritto", anche se questa è la modalità più idonea, perché il titolare deve poter sempre dimostrare che l'interessato ha prestato il consenso ad un determinato trattamento.

Il GDPR richiede, inoltre, un esplicito e specifico **consenso** per il trattamento di c.d. **"dati sensibili"** e per acconsentire che i dati vengano trattati in **maniera automatizzata (compresa la profilazione)**. *Sono esentati dal richiedere il consenso, per finalità di cure sanitarie per il pubblico interesse, ed anche il medico singolo, o farmacista (professionisti tenuti al segreto professionale).* I

I consenso raccolto precedentemente rimane valido se ha tutte le caratteristiche sopra descritte.

Vi sono anche forme di **consenso "implicito"**: *Ad esempio, per le foto consenso è considerato consenso "implicito" se facendo foto di gruppo uno mi ha guardato nell'obiettivo e si è messo in posa; se non lo voleva poteva non mettersi lì; poi però se la foto voglio metterla su un giornale, devo farci attenzione, ed essere sicuro di non violare i suoi diritti, ad esempio non posso pubblicare la foto con il sottotitolo "gruppo alcolisti anonimi"*

Legame tra informativa e consenso:

Il consenso può ritenersi validamente prestato **solo ove fondato su un'informativa adeguata**, quindi eventuali vizi attinenti alla mancanza, all'incompletezza o all'inesattezza dell'informativa si riflettono inevitabilmente sul consenso, rendendolo NON valido(Garante, 13 gennaio 2000).

5) La "Responsabilizzazione" del Titolare

Si tratta di una grande novità per la protezione dei dati in quanto viene **affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali**, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel GDPR.

Uno dei compiti che ha il titolare per dimostrare la propria "responsabilizzazione", è quello di **adottare un'efficace ed efficiente struttura organizzativa** articolata in un insieme di ruoli, ciascuno dei quali responsabile di uno specifico ambito in funzione delle proprie competenze.

6) Le "figure" della Privacy

L' "Interessato": E' la persona cui si riferiscono i dati.

Il "Titolare": L'azienda, cioè chi decide in materia di Privacy e nomina le altre figure (responsabili e incaricati, DPO)

di idonee e preventive misure di sicurezza, **i rischi di distruzione o perdita**, anche accidentale, dei dati stessi, **di accesso non autorizzato o di trattamento non consentito o non conforme** alle finalità della raccolta.

- **Va prevista una tutela generale per tutti i dati oggetto** di trattamento da parte sia di aziende private che di pubbliche amministrazioni.
- **Le precauzioni, di carattere generale, investono tutte le tipologie di dati trattati** per i quali è sempre richiesta l'adozione di idonee e preventive misure di sicurezza.

Il registro dei trattamenti (art. 30 GDPR)

Tutti i titolari che per il tipo, il numero, le finalità dei dati che trattano sarebbero tenuti alla nomina di un DPO ed i loro Responsabili (esterni) devono anche tenere un **REGISTRO DELLE OPERAZIONI DI TRATTAMENTO** (di seguito "Registro").

Il registro è un documento che raccoglie l'elenco e analisi dei tipi di dati trattati, la valutazione dei rischi, indica le misure adeguate per proteggere i dati e il loro periodo di conservazione.

E' uno strumento importante che in caso di ispezione va messo a disposizione dell'autorità di controllo.

Il registro ha una pagina iniziale con i dati di titolare, responsabili seguita dall' "elenco" dei trattamenti, con tante schede quanti sono i trattamenti fatti, catalogati secondo le varie finalità (es. "gestione personale", "fornitori", "clienti", "videosorveglianza", "marketing", "associati", attività specifiche, ecc).

Il Registro è un documento che va aggiornato man mano che variano i singoli trattamenti nel tempo, ad esempio, quando si usano nuove soluzioni tecnologiche o vengono introdotti prodotti o servizi.

Sarebbe uno strumento da adottare, perché molto utile, anche per chi NON ne ha l'obbligo: predisporlo, anche in un formato semplice quale potrebbe essere un foglio di lavoro tipo excel aiuterebbe il titolare a riflettere sui dati che tratta, a fare il punto sulle modalità ed i fini per cui li raccoglie e tratta, e di fare qualche ragionamento su chi e come li segue in azienda.

Trattamenti effettuati con strumenti elettronici

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate **misure di sicurezza adeguate.** Nel codice – **ora superato** - era stato previsto un disciplinare tecnico (Allegato B) a cui eventualmente si poteva fare riferimento; ora è prevista la **RESPONSABILIZZAZIONE DEL TITOLARE** ("accountability"), che dovrà tener conto che le **misure vanno individuate dal titolare e devono essere adeguate al rischio:**

Eccone alcune misure di protezione a titolo di esempio, perché - come detto - **spetta al titolare individuare le più adatte**:

- autenticazione informatica;
- prevedere "procedure di gestione" delle credenziali di autenticazione ed autorizzazioni specifiche;
- aggiornare periodicamente l'ambito del trattamento consentito ai singoli incaricati, l'elenco degli incaricati e dei responsabili, e l'elenco degli addetti alla gestione o alla manutenzione degli strumenti elettronici;
- proteggere gli strumenti elettronici e i dati dai da trattamenti illeciti e accessi non consentiti;
- adottare procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- se si trattano dati particolarmente delicati o comunque se il trattamento ha impatto sulle persone per il numero di trattamenti e di persone interessate, fare analisi preventiva di "impatto" (DPIA)
- adottare 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.

Autenticazione informatica: le Credenziali (dispositivi usati entrare in un PC o sistema) possono essere di tre tipi:

1) codice per l'identificazione dell'incaricato associato a una parola chiave (password);
2) dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato (badge, pass);
3) una caratteristica biometrica dell'incaricato (impronte digitali, impronta retinica, ecc.).

- Quando non vengono utilizzate per almeno 6 mesi vanno disattivate.
- Vanno disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati.
- Il codice per l'identificazione, se utilizzato, non può essere assegnato ad altri, neppure in tempi diversi.
- Gli incaricati devono mantenere segreta la password e custodire in modo diligente i dispositivi.
- NON va lasciato incustodito lo strumento durante un' interruzione anche temporanea della sessione di lavoro.

Parola chiave: La parola chiave deve rispettare le seguenti caratteristiche:

- deve essere composta da almeno 8 caratteri e va modificata al PRIMO utilizzo dall'incaricato;
- non deve contenere riferimenti riconducibili all'incaricato (nome proprio o di familiari, data di nascita...);
- va modificata almeno ogni 6 mesi (per i sistemi che gestiscono dati sensibili e giudiziari almeno ogni 3 mesi).

Sistemi di autorizzazione

Il "Responsabile":

Secondo il GDPR europeo è inteso come esterno", nel senso che è chi gestisce, raccoglie conserva, cioè "tratta" per CONTO del TITOLARE (ES può essere il commercialista, chi tiene le paghe, il reisponsabile sistemi informatici esterno, ecc.).

La norma italiana previde che vi possano anche essere figure di responsabile "interne", cioè delegate a presidiare delle funzioni interne (es. in grandi aziende potrebbero essere responsabili di Area/Uffici, Responsabile IT, Resp. l'Area Personale, ecc.). Questa figura invece nel regolamento europeo non viene formalmente citata, si parla solo di "deleghe" o personale "autorizzato".

In ogni caso la **nomina va fatta per iscritto** e **il titolare deve dare istruzioni scritte al responsabile** su come deve gestire il dato

Gli incaricati

Sono di norma i lavoratori, che devono essere autorizzati per iscritto, in qualità di "incaricato" o "delegato", alle operazioni di trattamento e **vanno istruiti** (formazione, regolamenti interni o ordini di servizio, ecc.) su quanto devono fare con riferimento ad accesso e utilizzo delle informazioni personali di cui possono venire a conoscenza nello svolgimento della propria prestazione lavorativa.

La designazione degli incaricati può essere effettuata su singolo nome o, specie nell'ambito di strutture organizzative complesse, mediante atti legati a "unità organizzative" (es. cassieri, reponsabili di ufficio, ecc.) per le quali deve comunque anche essere individuato, per iscritto, l'ambito del trattamento consentito (art. 30 CP).

Il "DPO", cioè la figura che "protegge" i dati

Un nuovo RUOLO è stato invece introdotto dal GDPR ed è quello del DPO o "Data Protection Officer cioè il "responsabile della protezione dei dati"; una persona esperta che **dà consulenza al titolare, effettua controlli sulla corretta esecuzione della norma e tiene i contatti con il Garante** in caso di necessità o di ispezioni, verifica che si faccia formazione ai dipendenti ecc..

Lo devono nominare :

a) tutte le amministrazioni ed enti **pubblici**(fanno eccezione le autorità giudiziarie)

b) chi effettua, come **attività principale, trattamenti che richiedono il monitoraggio** regolare e sistematico degli interessati su larga scala (es chi "profila" abitudini acquisto o fa geolocalizzazione, le banche ed assicurazioni ecc.)

c) chi ha come attività principale il **trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici** (es. una farmacia non è tenuta a nominarlo, come non è tenuto a farlo un medico di base, perché non trattano i dati sensibili su "larga scala".

Chi ha l' OBBLIGO di nominare un DPO deve prima della nomina:

- Verificare che siano rispettati requisiti di indipendenza richiesti dal GDPR;
- verificare che il soggetto abbia competenze specifiche in materia di privacy;

Poi occorre predisporre un Accordo per disciplinare le attività legate all'incarico di DPO e una lettera di designazione contenente i riferimenti del DPO nominato. Inoltre si deve comunicare nominativo e dati di contatto del DPO al Garante per la protezione dei dati personali, tramite procedura telematica predisposta da quest'ultimo. Infine i dati di contatto del DPO dovranno essere pubblicati sul sito internet dell'azienda e sulla documentazione da questa adottata (informative e consensi lo devono sempre indicare).

7) La Sicurezza dei dati e dei sistemi

Le misure di sicurezza hanno una importanza fondamentale nella tutela dei dati personali. Il titolare del trattamento quindi deve **mettere in atto misure adeguate** e poter **dimostrare che il trattamento è stato effettuato secondo le norme** Privacy. Le misure di sicurezza devono essere graduate a seconda del tipo e del fine del trattamento, e dei rischi che comporta rischi per i diritti e le libertà delle persone fisiche. **A rischi maggiori devono corrispondere maggiori misure a protezione dei dati.**

Obblighi di sicurezza

Titolare e responsabile devono **selezionare e modulare le misure** di protezione disponibili, in modo da renderle **efficaci**:

- **I dati personali oggetto di trattamento sono custoditi e controllati**, anche in relazione al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, **in modo da ridurre al minimo**, mediante l'adozione

Quando per gli incaricati ci sono profili di autorizzazione diversi v previsto un sistema di autorizzazione:

- Prevedere un sistema di gestione delle autorizzazioni.
- I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati prima dell'inizio del trattamento, così da limitare l'accesso ai soli dati necessari per effettuare le operazioni dovute.
- Periodicamente (almeno ogni anno), si verificano le condizioni per mantenere i profili di autorizzazione.

Protezione degli strumenti informatici e dei dati

I dati personali sono protetti contro il rischio di intrusione mediante:

1. attivazione di strumenti elettronici da aggiornare con cadenza almeno semestrale (i programmi antivirus);
2. aggiornamento periodico dei programmi per prevenire vulnerabilità e correggere i difetti (i c.d. patch);
3. per i dati sensibili e giudiziari va anche protetto il sistema da accessi abusivi (i c.d. firewall).

Back up e ripristino della disponibilità dei dati

- Il salvataggio dei dati deve avvenire con frequenza almeno settimanale.
- Vanno previste ed implementate procedure per il ripristino della configurazione di sistema.
- Deve essere previsto un piano di *disaster recovery* obbligatorio, se si trattano dati sensibili e giudiziari.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

- I dati sensibili o giudiziari vanno protetti contro l'accesso abusivo mediante l'utilizzo di idonei strumenti elettronici.
- L'uso e la custodia di supporti rimovibili su cui sono memorizzati dati va limitato a casi di effettiva necessità e la gestione dei supporti deve essere effettuata evitando accessi non autorizzati e trattamenti non consentiti.
- I supporti rimovibili contenenti dati sensibili o giudiziari ,se non utilizzati, sono distrutti o resi inutilizzabili.
- Vanno adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
- I dati genetici sono trattati solo in locali protetti (accessibili ai soli soggetti specificatamente autorizzati); il trasporto dei dati all'esterno dei locali prevede contenitori con serratura; il trasferimento elettronica è cifrato.

Trattamenti senza ausilio di strumenti elettronici

Il trattamento senza strumenti elettronici dovrebbe prevedere ALMENO le seguenti misure:

- a) aggiornamento periodico (almeno annuale) dell'elenco di incaricati a cui il trattamento è consentito;
- b) gli incaricati devono tenere chiusi a chiave i dati, non possono lasciarli incustoditi sulle scrivanie in caso di assenza anche temporanea, e possono gestirli nello stretto limite previsto da contratto o da obbligo di legge;
- c) gli atti vanno conservati in armadi o archivi ad accesso selezionato, identificando chi vi ha accesso.

Protezione dati "by default and by design"

Il primo criterio a cui il titolare si deve attenere è comunque riferito alla protezione dati definita "by default and by design" (art. 25 GDPR): **cioè si devono adottare misure (tecniche e organizzative) che garantiscano l'effettiva protezione** dei dati personali **fin dalla progettazione del trattamento e per impostazione predefinita**.

- **Privacy by Design**: fin da quando si progetta un trattamento vanno previste misure sicurezza idonee
- **Privacy by Default**: per impostazione predefinita (es. telefonino non deve "tracciare" con geolocalizzazione, almeno se lo impostio l'utente)

Le misure da adottare a questo fine potrebbero ad esempio consistere nel:

- ridurre al minimo il trattamento dei dati personali, raccogliendo solo i dati necessari per ogni specifica finalità del trattamento, limitando il periodo di conservazione, la portata e l'accessibilità.
- pseudonimizzare (rendere anonimi) i dati personali il più possibile, o "spezzarli" in più archivi
- offrire trasparenza per quanto riguarda il trattamento di dati personali e consentire controllo all'interessato.

8) Diritti degli interessati

Il GDPR prevede che l'interessato **possa tutelare i propri dati personali esercitando i diritti** previsti dagli articoli da 15 a 22 del GDPR presentando una richiesta (scritta) al titolare. Il titolare deve dare riscontro al massimo entro 1 mese dalla ricezione della richiesta, eventualmente prorogabile di 2 mesi. Se non è possibile farlo nei termini, si informa l'interessato sui motivi. Il titolare del trattamento deve, in ogni caso, ad adottare misure appropriate per fornire all'interessato le informazioni (artt. 13 e 14) e le comunicazioni (artt. da 15 a 22) previste dal GDPR, nonché agevolare l'esercizio dei suoi diritti. L'esercizio dei diritti dell'interessato è gratuito (art. 12 GDPR) se non si tratta di richieste infondate o eccessive.

Elenco dei diritti degli interessati:

• diritto di **accesso** (art. 15); diritto di rettifica (art. 16); • diritto alla **cancellazione** (oblio; art. 17 se i dati non sono più necessari, o si revoca il consenso o ci si oppone, se i dati sono trattati in modo non lecito o vanno cancellati per un obbligo legale; il diritto non si applica se trattare i dati è necessario per un obbligo legale o pubblico interesse o per esercizio di un diritto in sede giudiziale); • diritto di limitazione dei (art. 18) non esatti, se trattati in modo non lecito, se ci si oppone alla cancellazione chiedendo di limitare invece l'utilizzo, se i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; • diritto alla portabilità dei dati (art. 20); • diritto di opposizione (art. 21); • diritto a non essere sottoposto a un processo decisionale automatizzato (art. 22); • diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali; • diritto di revocare il consenso prestato in ogni occasione e con la stessa facilità con cui è stato fornito.

9) Violazioni di dati personali (data breach)

Per **violazione di dati personali** si intende la distruzione, perdita, modifica, divulgazione non autorizzata l'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (art.33 comma 2).
L'articolo 4 del GDPR, ha introdotto l'obbligo di gestire e, se necessario **segnalare a Garante e interessati la VIOLAZIONE DEI DATI PERSONALI.**
La notifica deve effettuata essere entro 72 ore dal momento in cui il titolare del trattamento è venuto a conoscenza della violazione. Se la notifica all'autorità di controllo (Garante) non viene effettuata entro 72 ore vanno indicati i motivi del ritardo. La notifica al garante non va fatta se il titolare ritiene che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Se la violazione presenta una probabilità elevata di rischio per i diritti degli interessati, il Titolare inoltre, senza ingiustificato ritardo, **INFORMA DELLA VIOLAZIONE ANCHE GLI INTERESSATI**

10) Le sanzioni

Sanzioni amministrative (GDPR)

Il GDPR (art.83) prevede sanzioni severe ma graduate, a discrezione del Garante, in modo da essere "dissuasive". Le sanzioni previste sono il Richiamo, l'Ammonizione, la Sospensione dal trattamento dei dati, sanzioni pecuniarie fino a 20 milioni di euro oppure il 4% del fatturato totale annuale. Alcuni casi sanzionabili sono:

- Omessa o inidonea informativa all'interessato
- Sanzioni in materia di conservazione dei dati di traffico
- Omessa o incompleta notificazione al Garante e Omessa informazione o esibizione al Garante
- Pubblicazione del provvedimento del Garante (*sanzione accessoria: può essere applicato la sanzione amministrativa accessoria della pubblicazione per intero o per estratto, in uno o più giornali*).

Sanzioni penali (ex Codice Privacy, novellato dal D Lgs 101/2018)

Nel D Lgs 101/2018 di recente pubblicazione, si specificano alcuni punti relativi a sanzioni penali, che includono, ad esempio:

- Trattamento illecito di dati
- Falsità nelle dichiarazioni e notificazioni al Garante Inosservanza di provvedimenti del Garante.
- Mancata adozione misure di sicurezza

Responsabilità civile

Il titolare è civilmente responsabile qualora ometta di adottare le misure di sicurezza idonee e preventive che riducono al minimo i rischi; il Codice infatti prevede chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c.

Nota: Questo materiale è una sintesi, molto semplificata, di un argomento in realtà complesso, su cui si innestano norme di legge, provvedimenti del Garante, diritto del lavoro e altro; la materia va approfondita, caso per caso, col supporto di un esperto o consultando il sito *www.garanteprivacy.it*

ASSOCIAZIONI CRISTIANE LAVORATORI ITALIANI - CUNEO -

Per chiarimenti potrete contattare:
ACLI CUNEO Pzza. Virginio Vincenzo 13 Cuneo tel. 0171/452611
BECCARIA LUCIANA, DPO Cert. Bureau Veritas, tel. 347/4841225