LA PRIVACY DALLA PARTE DELL'IMPRESA

Relatore: Avv. Sabrina Primavera

LA TUTELA DELLA PRIVACY

prevista dal nostro ordinamento dal **D.Lgs. n. 196/2003 del 30.06.2003** (che ha abrogato la prima normativa italiana in materia di privacy: Legge n. 675/96 in attuazione delle Direttive 95/46/CE, 97/66/CE, 2002/58/CE) è un diritto fondamentale della persona e una necessità imprescindibile della società moderna ma in ambito imprenditoriale viene spesso vissuta come obbligo burocratico che rallenta o rende più macchinoso il raggiungimento degli obiettivi d'impresa.

In realtà la corretta adozione di semplici misure a protezione dei dati personali può contribuire a rendere più efficiente l'organizzazione dell'impresa e a ridurre sensibilmente i potenziali rischi a cui la stessa si espone sul mercato.

LA TUTELA DELLA PRIVACY

Per questo il Garante della privacy ha voluto aiutare le imprese con una selezione di dieci “best practice” per migliorare

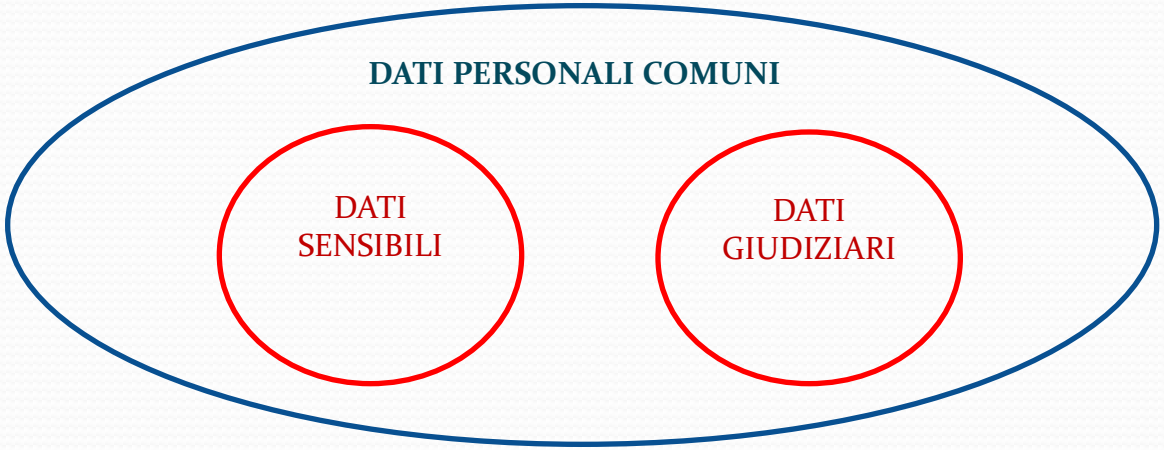
A. l’immagine dell’impresa (soggetto attento al principio di “responsabilità sociale”),
B. la capacità di business (a parità di costi sostenuti, aumentando la fiducia di utenti e consumatori nella serietà e affidabilità dell’impresa).

PRIMA REGOLA: IL VALORE DEI DATI

I “dati” rappresentano uno dei beni più preziosi posseduti da un’impresa, sia essa di grandi o piccole dimensioni.

Ma le potenzialità economiche dei dati sono direttamente proporzionali alla liceità del loro trattamento: raccoglierli nel rispetto della privacy, e poterne quindi liberamente usufruire, significa creare valore per l’azienda.

Bisogna quindi conoscere la differenza esistente tra i vari tipi di dati e la loro utilizzabilità



PRIMA REGOLA: IL VALORE DEI DATI

I dati personali sono:

- tutte le informazioni relative a una persona fisica, identificata o identificabile, anche indirettamente, incluso l'eventuale numero di identificazione personale (indirizzo e-mail, immagine fotografica di una persona, codice fiscale, numero telefonico, indirizzo IP, targa automobilistica).

Solo per persone fisiche infatti non sono più considerati come dati personali i dati riferibili alle persone giuridiche.

PRIMA REGOLA: IL VALORE DEI DATI

I dati sensibili sono:

- quei dati idonei a rivelare l'origine razziale ed etnica di una persona, le sue convinzioni religiose, filosofiche o di altro genere,
- quelli che indicano l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,
- i dati idonei a rivelare lo stato di salute e la vita sessuale.

Sono tutte informazioni delicate che possono incidere sulla riservatezza e la dignità dell'individuo.

PRIMA REGOLA: IL VALORE DEI DATI

I dati giudiziari sono:

- le informazioni contenute nel casellario giudiziale e quelle connesse alla posizione di imputato o indagato in procedimenti penali (carichi pendenti).

I dati sensibili e giudiziari devono essere trattati con maggiore attenzione e particolari cautele.

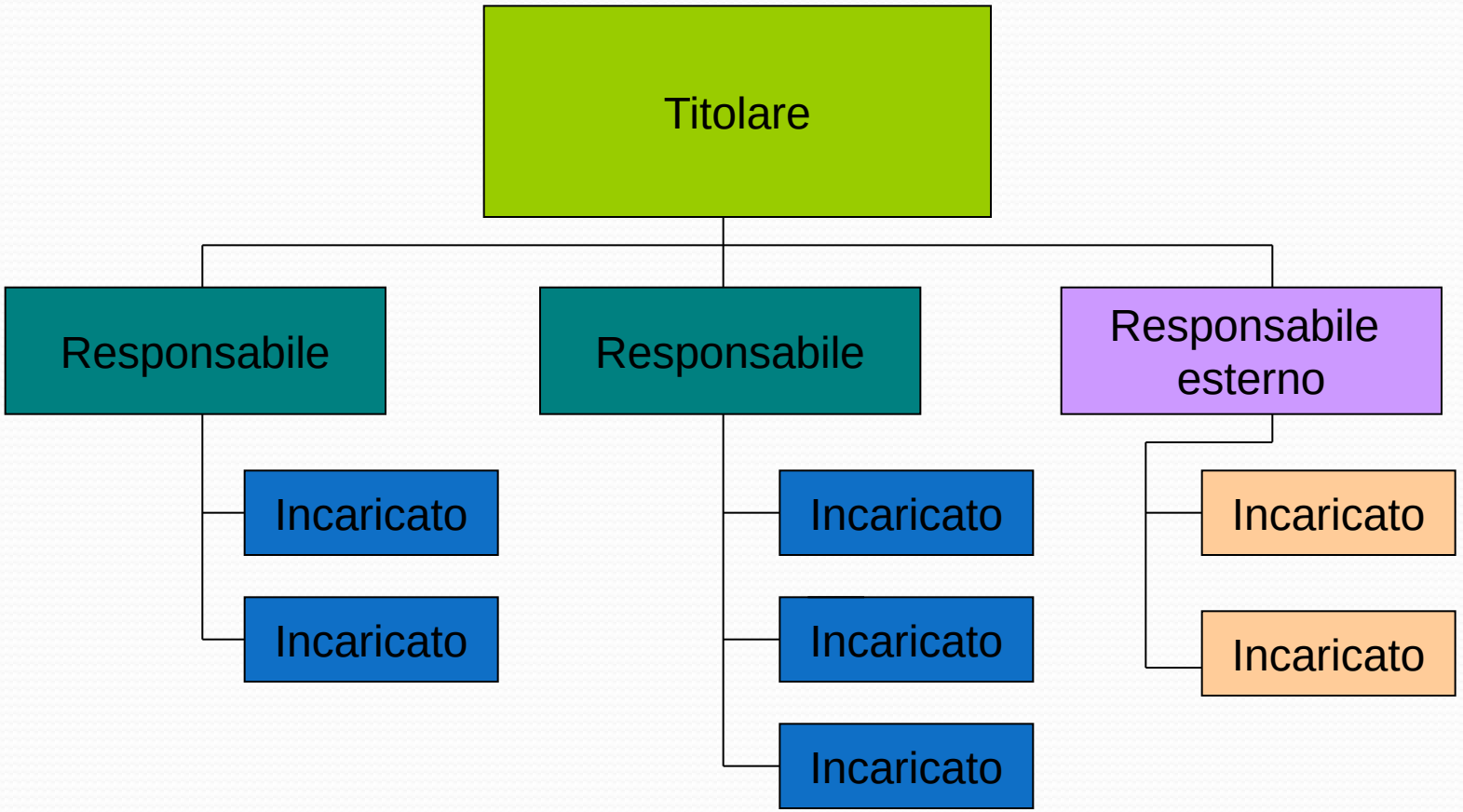
SECONDA REGOLA: AD OGNUNO LE PROPRIE RESPONSABILITÀ

Anche quando i beni usati sono i dati personali è necessario che sia chiaro "**chi fa cosa**" e con quali scadenze.

Il Codice della privacy impone di definire bene quali figure hanno la possibilità di trattare dati personali:

- **Il titolare del trattamento** (data controller) è il soggetto che esercita un potere decisionale, del tutto autonomo, sulle finalità e sulle modalità del trattamento. La qualità di titolare discende direttamente dai poteri che si esercitano sui dati.
- **Il responsabile del trattamento** (data processor): persona fisica o giuridica nominata dal titolare per la gestione dei dati nel rispetto delle regole dettate dal titolare del trattamento.
- **Gli incaricati del trattamento** sono le persone fisiche che effettuano materialmente le operazioni di trattamento dei dati personali e operano sotto la diretta autorità del titolare (o del responsabile se è stato nominato) secondo precise istruzioni.

Rapporti tra i ruoli privacy



TERZA REGOLA: TRASPARENZA E CORRETTEZZA NEL BUSINESS

È sempre necessario informare il legittimo proprietario e chiedere il suo permesso prima di utilizzare un bene che gli appartiene.

Quando i beni sono dati personali il proprietario è l'interessato al quale il titolare dovrà fornire l'informativa e dal quale dovrà ricevere il consenso.

PRIMA DI UTILIZZARE I DATI

TITOLARE  INTERESSATO

TERZA REGOLA: TRASPARENZA E CORRETTEZZA NEL BUSINESS

INFORMATIVA

Un'impresa che tratti dati personali deve spiegare agli interessati con un'informativa completa e chiara, le caratteristiche essenziali dei trattamenti effettuati: dove sono stati presi i dati, le finalità e le modalità del trattamento, se i dati debbano o possano essere forniti a terzi, i soggetti o le eventuali categorie ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza, nonché il nome di almeno un responsabile del trattamento, qualora designato.

Il Garante ha consentito e suggerito forme semplificate di informativa, adatte alle specifiche esigenze espresse da singoli imprenditori o dalle associazioni di categoria (Ad esempio per informare le persone dell'esistenza di un sistema di videosorveglianza in un supermercato è sufficiente esporre dei cartelli che segnalino le telecamere e che indichino le finalità della ripresa e il nome del responsabile del trattamento a cui rivolgersi per eventuali informazioni aggiuntive).

TERZA REGOLA: TRASPARENZA E CORRETTEZZA NEL BUSINESS

PRIMA DI UTILIZZARE I DATI

TITOLARE → INTERESSATO

CONSENSO

L'impresa, dopo aver informato l'interessato, deve chiedergli il consenso per utilizzare i suoi dati personali: consenso "informato". Tale consenso deve essere:

- liberamente espresso, evitando quindi di adottare condizionamenti o pressioni per ottenerlo
- documentato per iscritto

TERZA REGOLA: TRASPARENZA E CORRETTEZZA NEL BUSINESS

Casi in cui non è richiesto il consenso dell'interessato:

- quando il trattamento è previsto da un obbligo di legge (es. quello che impone agli alberghi di comunicare le generalità delle persone alloggiate alle autorità di pubblica sicurezza) da un regolamento o dalla normativa comunitaria
- quando i dati vengono trattati per adempiere, prima della conclusione di un contratto, a specifiche richieste dell'interessato (ad es. come avviene per i dati necessari per la concessione di un mutuo bancario)
- per il trattamento dei dati necessari per l'esecuzione di un contratto già in essere (come quelli per la fatturazione di un prodotto o servizio)
- i dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque. Va comunque rispettato rigorosamente il vincolo di finalità (ad es. i dati del PRA si possono usare senza consenso per finalità attinenti la sicurezza stradale - ad esempio per ricordare l'obbligo di revisione periodica dell'autoveicolo - ma non per l'invio di pubblicità come quelle su pezzi di ricambio e accessori
- alcune attività svolte all'interno di gruppi di imprese come nel caso in cui sia necessario comunicare i dati per finalità meramente amministrativo-contabili
- il trattamento dei dati è necessario ai fini dello svolgimento di investigazioni difensive o comunque per far valere un diritto in sede giudiziaria.

TERZA REGOLA: TRASPARENZA E CORRETTEZZA NEL BUSINESS

Consenso e dati sensibili

I dati sensibili necessitano di tutele rafforzate, quindi per poterli utilizzare l'impresa avrà bisogno di:

- consenso scritto della persona interessata
- l'autorizzazione del Garante

autorizzazioni generali Garante: un esempio l'autorizzazione generale per il trattamento dei dati sensibili o giudiziari nell'ambito del rapporto di lavoro o per il trattamento effettuato da liberi professionisti o da organismi di tipo associativo o dalle fondazioni.

QUARTA REGOLA: CURRICULUM & CO. SEMPLIFICAZIONE

1. Non è necessario richiedere al candidato il consenso al trattamento dei dati personali contenuti nel curriculum, per finalità di selezione del personale a meno che:
   - non abbiano natura sensibile (come l'appartenenza a categorie protette)
   - non siano destinati alla comunicazione a terzi.
2. L'impresa che avvia una selezione del personale deve fornire al candidato, a voce o per iscritto, prima di acquisire il suo cv, l'informativa sul trattamento dei dati personali.

In caso di autocandidatura l'azienda che riceve i curriculum non ha l'obbligo di offrire l'informativa o di chiedere al candidato il consenso per il trattamento dei dati personali (inclusi quelli sensibili) contenuti nella documentazione pervenuta. L'informativa dovrà essere data nel momento in cui l'azienda decida di prendere in considerazione il curriculum e di contattare il candidato.

QUINTA REGOLA: TRATTAMENTI A RISCHIO

Al fine di garantire maggiore trasparenza e tutele nel caso in cui vengano effettuati trattamenti di dati di particolare delicatezza e di potenziale pericolosità, il Codice della privacy ha previsto che, in casi specifici, le imprese comunichino preventivamente al Garante informazioni generali sull'attività di raccolta e di utilizzazione dei dati personali tramite la:

NOTIFICAZIONE

comunicazione telematica obbligatoria quando si effettuano determinati tipi di trattamento:

- trattamenti di dati genetici, biometrici o di dati che indicano la posizione geografica di persone o di oggetti a loro riferibili (come i sistemi di geolocalizzazione) acquisiti, ad esempio, con rilevamenti radio;
- i trattamenti di dati per le attività di profilazione, e così pure la raccolta di informazioni in apposite banche dati relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni (vi rientrano ad esempio gli archivi dei cosiddetti sistemi di informazioni creditizie) e a comportamenti illeciti o fraudolenti.

Una volta effettuata la "notifica" del trattamento, non è necessario che l'azienda invii altre comunicazioni al Garante, a meno che il trattamento non sia modificato o interrotto.

SESTA REGOLA: TECNOLOGIA PER L'IMPRESA

Gli interessi imprenditoriali possono essere perseguiti con molteplici soluzioni tecnologiche e organizzative, alcune delle quali possono comportare il trattamento di dati personali e possono confliggere con la dignità e la riservatezza delle persone coinvolte, per questo è previsto l'intervento del Garante per valutare e "bilanciare" i diritti e gli interessi esistenti

Controllo sul lavoro:

L'imprenditore deve ponderare con attenzione quali strumenti adottare al fine di evitare trattamenti di dati non necessari che, tra l'altro, possono risultare eccessivi o anche discriminatori, per cui:

SESTA REGOLA: TECNOLOGIA PER L'IMPRESA

- **SI** alla installazione di un sistema di videosorveglianza per esigenze organizzative e produttive,

- **NO** alla raccolta di immagini che può consentire anche il controllo a distanza e la verifica dell'attività dei lavoratori, occorre tenere in considerazione non solo le norme previste dal Codice della privacy, ma anche quelle indicate nello Statuto dei lavoratori (tenendo presente che l'installazione di tecnologie per l'esclusiva finalità di controllo a distanza dei lavoratori è comunque vietata).

- **NO** all'utilizzano software che, al fine di migliorare le prestazioni della rete internet aziendale, potrebbero consentire il monitoraggio della navigazione o della posta elettronica dei dipendenti.

- **SI ma con le dovute** valutazioni di tutte le circostanze del caso e la proporzionalità del suo utilizzo, all'impiego di tecnologie che consentono la precisa localizzazione del lavoratore come, ad esempio, il Gps dell'autoveicolo o dello smartphone in dotazione, o l'Rfid (Identificazione a radio frequenza) del documento di riconoscimento.

SESTA REGOLA: TECNOLOGIA PER L'IMPRESA

In ogni caso

Verifica preliminare

il Garante deve essere contattato preventivamente, chiedendo una verifica preliminare, nel caso in cui la società intenda avviare un trattamento di dati personali (diversi da quelli sensibili e giudiziari) che possa presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato (ad esempio, quando si intendono attivare sistemi di videosorveglianza "intelligente")

La verifica preliminare è richiesta anche quando, per particolari esigenze, si vogliano allungare i tempi di conservazione delle immagini registrate oltre il termine massimo di sette giorni.

In sintesi: La normativa non vieta in assoluto l'adozione di misure tecnologiche a tutela delle attività aziendali, ma cerca un bilanciamento con altri diritti fondamentali della persona, attraverso la preventiva autorizzazione da parte del Garante.

SESTA REGOLA: TECNOLOGIA PER L'IMPRESA

CONTROLLO A DISTANZA DOPO IL JOBS ACT
(nuovo Art. 4 Statuto Lavoratori)

- Non vi è più il divieto generale di controllo a distanza dell'attività dei lavoratori;
- E' prevista la possibilità di impiegare impianti audiovisivi e altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori "esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale" previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali o autorizzazione della Direzione Territoriale del lavoro;
- nel caso di imprese con unità produttive site in diverse province della stessa regione o in diverse regioni, è consentito stipulare gli accordi sindacali per l'installazione degli impianti audiovisivi e degli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dei lavoratori, anziché con le rappresentanze sindacali aziendali o le rappresentanze sindacali unitarie, con le associazioni sindacali comparativamente più rappresentative sul piano nazionale e, in difetto di accordo, è previsto che l'autorizzazione ministeriale sia concessa dal Ministero del lavoro e delle politiche sociali;
- è espressamente esclusa la necessità di accordo sindacale o autorizzazione ministeriale per gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa (pc, tablet, telefoni cellulari, ecc), pur se dagli stessi derivi anche la possibilità di un controllo a distanza del lavoratore;
- è prevista la possibilità di utilizzare le informazioni e i dati raccolti tramite gli impianti audiovisivi (previamente autorizzati) e gli strumenti di lavoro (per cui non occorre autorizzazione) per "tutti i fini connessi al rapporto di lavoro" a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196

SETTIMA REGOLA: DIFESA DEL PATRIMONIO DATI

All'interno della vasta gamma di misure idonee si trovano quelle che devono essere obbligatoriamente adottate:

Misure minime

Il Codice prevede che per il trattamento dei dati è necessario che i titolari adottino misure minime di sicurezza che garantiscano:

SETTIMA REGOLA: DIFESA DEL PATRIMONIO DATI

In caso di trattamento elettronico:

- la verifica e la convalida dell'identità di chi accede al sistema (identificativi personalizzati, password sicure…),
- l'adozione di un apposito sistema di autorizzazione che consenta solo specifiche attività predefinite,
- l'utilizzo di strumenti (come antivirus aggiornati e altri software e sistemi di protezione) per impedire accessi illeciti o abusivi che mettano a rischio l'integrità e la confidenzialità del dato personale.
- Idonea procedura di gestione di situazioni di crisi, ad esempio predisponendo "copie di backup", in modo da poter rendere nuovamente disponibili dati e sistemi.
- Definizione di misure di protezione particolari per i dati sensibili, magari adottando tecniche crittografiche che non li rendano immediatamente leggibili in caso di accessi illeciti.
- Formazione continua del personale addetto al trattamento dei dati personali
- Aggiornamento delle misure adottate, affinchè non perdano di efficacia, nel tempo.

SETTIMA REGOLA: DIFESA DEL PATRIMONIO DATI

In caso di trattamento senza l'ausilio di strumenti elettronici

- 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.

SETTIMA REGOLA: DIFESA DEL PATRIMONIO DATI

DPS

Documento Programmatico della Sicurezza

Il DPSS è il documento sulla base del quale è possibile dimostrare quanto fatto in azienda a protezione dei dati personali trattati.

Non è più obbligatorio (decreto Monti 2012) predisporre un "documento programmatico sulla sicurezza" che elenchi le misure adottate.

Le imprese potranno comunque trarre beneficio da un monitoraggio frequente della propria privacy policy e delle misure adottate per proteggere i dati, mantenendo così sotto controllo la situazione.

Ciò anche perché l'imprenditore (il titolare e i responsabili del trattamento), nel caso in cui a seguito di violazioni dei dati sia chiamato in causa per un'azione risarcitoria in sede civile, dovrà affrontare le difficoltà derivanti dall'inversione dell'onere della prova, e dovrà essere in grado di dimostrare di aver adottato tutte le misure idonee, in base allo stato dell'arte, a ridurre - per quanto possibile - i rischi connessi al non corretto utilizzo dei dati.

OTTAVA REGOLA: CONTROLLO DEL "CONTROLLORE INFORMATICO".

Quasi in tutte le imprese esiste una figura particolare che si occupa della gestione dei sistemi informatici e della sicurezza:

l'amministratore di sistema

Per la peculiarità delle sue funzioni, questo professionista può avere accesso ai dati più riservati di un'azienda perciò il Garante ha prescritto che anche il suo operato sia trasparente e posto sotto il controllo del titolare del trattamento.

- Attenta valutazione l'esperienza, la capacità, e l'affidabilità delle persone chiamate a ricoprire tale ruolo;
- Utilizzo di sistemi di controllo (presenti in tutti i moderni sistemi operativi oggi in uso) che consentano la tracciabilità degli accessi effettuati dagli amministratori di sistema agli archivi elettronici e ai sistemi di elaborazione, e la registrazione dei relativi dati per un tempo non inferiore ai sei mesi;
- Il titolare del trattamento dovrà poi provvedere a una verifica, con cadenza almeno annuale, sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.

NONA REGOLA:L"EXPORT" DEI DATI.

La normativa comunitaria prevede che i dati personali possono circolare liberamente entro l'Unione europea. Per trasferire dati al di fuori dell'Unione europea devono invece essere garantiti standard di protezione adeguati a quelli europei: in caso contrario è vietato trasferire dati personali.

Il Garante pubblica sul proprio sito internet un elenco aggiornato degli Stati "terzi" che sono già ritenuti affidabili a livello europeo e per i quali non è necessario alcun "passaporto" per l'esportazione.

Se il paese scelto non è in questa lista, l'eventuale trasferimento dei dati può essere consentito sulla base di altre garanzie adeguate. Per quanto riguarda gli Stati Uniti, si può controllare se i dati sono trasferiti ad imprese presenti sul territorio americano che aderiscono ad un accordo bilaterale UE-USA detto Safe Harbor (letteralmente "porto sicuro"), il quale definisce regole sicure e condivise per il trasferimento dei dati personali.

In ogni caso: **è consentito il trasferimento** se:

- vi è l'apposito consenso dell'interessato
- il trasferimento risulta necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato.

DECIMA REGOLA: VERSO UNA"CUSTOMER CARE" DEI DATI.

Il patrimonio informativo di un'azienda è un valore da tutelare e promuovere alla stregua di ogni altro asset, e può trasformarsi in una risorsa competitiva e di immagine, per cui anche nella gestione dei dati l'azienda deve fornire assistenza agli interessati, tenendo presente:

Diritti della persona interessata

- La normativa sulla privacy, garantisce alla persona interessata specifici diritti:
- quello di conoscere quali siano i dati che lo riguardano in possesso dell'impresa e per quale motivo siano stati raccolti e come siano elaborati;
- richiesta di estrapolazione e la messa a disposizione in modo intelligibile dei dati personali che lo riguardano;
- il loro aggiornamento, la rettifica o l'integrazione;
- in caso di violazione di legge, può anche esigere il blocco, la cancellazione o la trasformazione in forma anonima di queste informazioni.

DECIMA REGOLA: VERSO UNA"CUSTOMER CARE" DEI DATI.

Conservazione dei dati

In linea generale, un dato personale non deve essere conservato per sempre, ma solo fin quando è necessario per lo scopo per il quale i dati sono stati raccolti.

Qualora non sia indicato per legge un preciso termine di conservazione, occorre comunque prevederlo.

Distruzione o perdita di dati personali

Le imprese dovrebbero reagire con prontezza e trasparenza ogni volta in cui dovessero accorgersi di violazioni dei dati personali trattati. In questi casi, al di là delle opportune valutazioni in termini di responsabilità civile e penale, sarebbe sempre opportuno avvisare gli interessati del problema riscontrato, anche per consentire loro di adottare misure che limitino i possibili pregiudizi alla persona che possono derivare, ad esempio, da un furto di identità o il danno alla reputazione che può discendere dall'utilizzo di dati inesatti o non aggiornati.