PRIVACY

LA PROTEZIONE DEI DATI NELL'UNIONE EUROPEA E...NON SOLO

Il progresso tecnologico e la capillare diffusione di computer, tablet, smart-phone, non solo influenza la nostra vita quotidiana, ma definisce dei veri e propri stili di vita.

A livello quotidiano, quasi tutti sono ormai in grado di utilizzare un computer, collegarsi ad internet, magari in wi-fi, e operare online per acquistare, ad esempio, un biglietto del treno e del teatro.

Ma cosa c'è dietro a questi sistemi di comunicazione elettronica?

Dove inizia e dove finisce la nostra sfera privata? E quali strumenti abbiamo per tutelarci, o eventualmente anche opporci, da interferenze nella nostra vita privata da parte di enti pubblici o privati?

Scopo di questa breve dissertazione è di fornire elementi attraverso cui capire le motivazioni che hanno portato all'elaborazione della Direttiva 95/46/EC concernente la tutela delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali ed attualmente in corso di riesame, per migliorarla e renderla più coerente con gli obiettivi di armonizzazione delle legislazioni nazionali e di realizzazione del mercato unico europeo.

Le leggi di recepimento della direttiva all'interno degli stati membri dell'Unione europea non mostrano ancora un quadro europeo uniforme, per questo sono state elaborate schede analitiche su concetti chiave che cercano di mettere in luce similitudini e differenze.

Inoltre, poiché la tecnologia non conosce confini, la ricerca si conclude con una veloce occhiata su come 32 paesi del resto del mondo si approcciano al concetto di privacy.

Buona lettura!

Stefania Fenati

INDICE

PREMESSA

Quando nasce l'esigenza di tutelare la sfera privata dell'individuo?

Nell'era moderna, con il progresso tecnologico: la stampa, la macchina fotografica, i sistemi di registrazione di suoni e immagini. E' evidente come l'esigenza di tutela della privacy oltre ad essere mutevole nel tempo, sia legata in modo diretto alla diffusione delle nuove tecnologie informatiche la cui diffusione nel corso del secolo scorso è stata esponenziale.

Quando e dove nasce il concetto giuridico di privacy?

Il concetto giuridico di privacy nasce negli Stati Uniti nel 1890. Due ricercatori, S. D. Warren e L. D. Brandeis, pubblicarono sulla Harvard Law Review un articolo dal titolo "The right to privacy" in cui si ritrova la prima definizione di privacy: "the right to be let alone".

Già allora, il progresso tecnologico (stampa e macchina fotografica) limitava la libertà individuale e il diritto alla riservatezza e Warren & Brandeis sottolinearono l'esigenza di rafforzare il confine tra vita privata e ambito pubblico per tutelare giuridicamente "thoughts, sentiments and emotions".

Evoluzione del diritto alla privacy

Dal 1890 in poi l'evoluzione del concetto di "right to privacy" non ha conosciuto soste, inizialmente soprattutto grazie all'interpretazione giurisprudenziale, attraverso cui il concetto di privacy viene applicato a situazioni profondamente differenti. Si parla di informational privacy, riferendosi al diritto del singolo di tutelare i propri dati personali, e di decisional privacy per riferirsi alla libertà di ogni individuo di autodeterminarsi rispetto alle proprie scelte personali.

Cosa succede in Italia?

Mentre nei sistemi di common-law è stato agevole identificare e disciplinare il diritto alla privacy per la peculiare funzione esercitata in quei sistemi dalla giurisprudenza, in Italia il percorso è stato molto più lento e accidentato.

Fino al 1955 in Italia si negava addirittura l'esistenza del diritto alla riservatezza e solo nel 1975, vent'anni dopo, la Suprema Corte di Cassazione prende una posizione netta e riconosce l'esistenza nel nostro ordinamento di tale diritto. La pietra miliare è la sentenza n. 2129 del 27 maggio 1975, che si riferisce alla controversia sollevata da Soraya Esfandiari, ex moglie dell'ultimo scià di Persia (oggi Iran), in cui si legge che la divulgazione di immagini o avvenimenti non direttamente rilevanti per l'opinione pubblica, anche se effettuata con mezzi leciti e per fini non esclusivamente speculativi, costituisce lesione della privacy.

I riferimenti in Italia

La nostra Costituzione

Art. 2 "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità...", da cui la Corte, ponendo l'accento sulla norma che riconosce all'uomo il rispetto della propria personalità, fa discendere il diritto erga omnes alla libertà di autodeterminazione;

Art 3 "Tutti i cittadini hanno pari dignità sociale. ...", dignità che la legge deve garantire anche attraverso il riconoscimento di una specifica sfera di autonomia che impedisca indebite ingerenze altrui, in questo senso l'art. 2 diventa il riferimento legislativo attraverso cui adeguare la normativa alle mutevoli esigenze di tutela della personalità;

Art. 13 "La libertà personale è inviolabile....", la Corte ha inteso l'inviolabilità della persona nella sua accezione più ampia, quindi non solo fisica.

D. Lgs. 30 giugno 2003 n. 196

Il nostro paese adotta un'apposita norma solo nel 1996 con la Legge 675 alla quale hanno fatto seguito altri testi normativi. Successivamente è stato necessario riordinare la materia ed è stato pubblicato il Codice in materia di protezione dei dati personali adottato con il D. lgs. 30 giugno 2003 n. 196.

I riferimenti in Europa

- Convenzione del Consiglio d'Europa n. 108 su "Protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale" firmata il 28 gennaio 1981 a Strasburgo

- Carta dei diritti fondamentali dell'Unione Europea proclamata ufficialmente a Nizza nel dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione che riunisce in un unico documento i diritti che prima erano contenuti in vari strumenti legislativi, tra cui i principi generali sanciti dalla Convenzione europea dei diritti dell'uomo del 1950, da convenzioni internazionali del Consiglio d'Europa, delle Nazioni Unite (ONU) e dell'Organizzazione internazionale del lavoro (OIL).

In particolare, la Convenzione 108 è l'unico strumento internazionale giuridicamente vincolante e applicabile nel mondo intero. Essa stabilisce una serie di principi fondamentali a protezione della privacy e attualmente rappresenta un riferimento per 44 stati che hanno firmato e ratificato la convenzione . Qualunque paese, purché disponga della normativa richiesta in ordine alla protezione dei dati, può diventarne parte.

Curiosità

Già nel 1981 in Italia esistevano più di 60.000 banche dati private che potevano raccogliere e trattare dati anche in assenza di una specifica regolamentazione.

L'evoluzione del progresso tecnologico unitamente all'enorme diffusione dei computer ha in pochi anni non solo moltiplicato in maniera esponenziale il numero delle banche dati, ma anche modificato il comportamento degli utenti-consumatori che sempre più frequentemente svolgono transazioni on-line.

Una società democratica, nel promuovere lo sviluppo tecnologico ed economico, deve riconoscere, garantire e soprattutto tutelare le libertà fondamentali tra cui anche il diritto alla riservatezza, sensibi-

lizzando i cittadini a comportamenti consapevoli.

E' per questo che nel 2007 il Consiglio Europeo, la Commissione europea e tutte le Autorità europee per la protezione dei dati personali, hanno istituito la "Giornata europea della protezione dei dati personali", celebrata annualmente in tutta Europa il 28 gennaio, data della firma della Convenzione 108.

INTRODUZIONE

Diritto alla privacy, diritto alla riservatezza, diritto alla protezione dei dati personali ... Quante volte abbiamo sentito, letto o magari utilizzato queste allocuzioni? Ma possono essere utilizzate indifferentemente o vi sono delle differenze?

Il diritto alla privacy è il risultato dell'evoluzione del diritto alla riservatezza che è un diritto separato, ma strettamente ed intimamente collegato al diritto alla protezione dei dati personali, tanto che nell'uso comune le due espressioni sono utilizzate senza alcuna distinzione.

In verità con diritto alla riservatezza si intende il diritto di ogni persona a vedere protetta la propria vita privata dall'ingerenza delle autorità pubbliche, salvo specifici casi previsti dalla legge, e dalla curiosità altrui. Tale diritto è stato stabilito dal Consiglio d'Europa con l'adozione della "Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali" (CEDU) firmata a Roma il 4 novembre 1950.

Il diritto alla protezione dei dati è invece più recente. La sua introduzione risale, infatti, agli anni Ottanta in seguito allo sviluppo delle nuove tecnologie con l'approvazione da parte del Consiglio d'Europa della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale. Con la Convenzione sono stati fissati principi e regole in base ai quali è legittimo raccogliere e trattare dati personali. La sua applicazione è bidirezionale, essa da una lato obbliga i titolari del trattamento a rispettare una serie di regole, e dall'altro riconosce agli interessati una serie di nuovi diritti, oltre alle modalità e agli ambiti per la loro tutela.

Fino a metà degli anni Novanta, la protezione dei dati personali in Europa era regolata da singole leggi nazionali non armonizzate tra loro. Sebbene fossero tutte ispirate ai principi fondamentali stabiliti dalla Convenzione n. 108 sulla protezione dei dati, approvata nel 1981 dal Consiglio d'Europa, queste leggi erano profondamente

diverse nei contenuti e tali differenze incidevano negativamente sulla competitività e il corretto funzionamento del mercato unico europeo. La necessità di un quadro normativo unico si faceva sempre più urgente per eliminare questi ostacoli.

Nel 1995 l'Unione Europea adotta la Direttiva 95/46/EC al fine di armonizzare al proprio interno la normativa concernente la tutela delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

In verità, le Relazioni presentate dalla Commissione al Parlamento Europeo sull'applicazione della Direttiva, pur rilevando uno sviluppo positivo del diritto alla privacy e nella circolazione dei dati all'interno dell'Unione, hanno evidenziato una situazione non ancora sufficientemente armonizzata fra gli Stati membri.

Inoltre, negli ultimi anni, abbiamo assistito ad eventi di ordine politico ed economico che hanno investito la comunità internazionale incidendo profondamente sul suo sviluppo. La necessità di far fronte ai pericoli terroristici e di infiltrazione della criminalità organizzata, ha determinato un rafforzamento della cooperazione giudiziaria e di polizia in materia penale a livello europeo che deve, nello stesso tempo, garantire la protezione del diritto alla privacy e consentire alle autorità delegate alla difesa di trattare e trasmette dati per proteggere e salvaguardare l'ordine interno dell'Unione. Oltre a ciò, la forte crisi economica degli ultimi anni unitamente al progresso delle tecnologie dell'informazione e della comunicazione ha spinto le aziende a ricercare sistemi condivisi per il trattamento, la protezione e la circolazione dei dati al fine di liberare risorse necessarie per rilanciare lo sviluppo, soprattutto dell'economia digitale europea.

Per questi motivi la Commissione ha ritenuto indispensabile ed urgente pensare ad una modifica della regolamentazione ora in vigore e ha avviato una fase di riforma ora in corso.

Questa pubblicazione, pur non volendo avere un carattere esaustivo, nella prima parte si pone l'obiettivo di evidenziare gli aspetti

comuni agli Stati membri così come definiti dalla direttiva europea 95/46/EC, oltre ad introdurre gli elementi principali del processo di riforma in corso. Nella seconda, invece, attraverso schede costruite per ogni Stato membro, si possono rilevare i riferimenti legislativi nazionali, oltre a differenze e peculiarità di ciascuno stato. Infine nella terza parte, la ricerca offre un quadro molto essenziale della situazione in alcuni paesi extraeuropei.

In tutto i paesi presi in considerazione sono 60.

1. LA PROTEZIONE DEI DATI PERSONALI NELL'UNIONE EUROPEA

Ogni volta che ci iscriviamo ad un social network o a una newsletter, che prenotiamo un volo o una vacanza on-line o che apriamo un conto in banca, trasmettiamo informazioni personali essenziali.

Dove vanno a finire questi dati?

Chi li può utilizzare e in che modo?

Non abbiamo più nessun controllo su di loro?

Quali diritti ci spettano?

Per chi vive in uno dei paesi dell'Unione europea, il diritto alla privacy è protetto, oltre che dalle norme internazionali e dalla Convenzione Europea per i Diritti dell'Uomo (CEDU), anche dalla direttiva europea 95/46/CE del 24 ottobre 1995.

Questa direttiva è la pietra miliare se si vuole capire in che modo l'Unione europea tutela la nostra privacy e, allo stesso tempo, riesce a fare in modo che questa tutela non sia un limite per la libera circolazione delle informazioni tra gli Stati membri, essendo questo uno degli elementi fondamentali del mercato unico. Ogni giorno, infatti, imprese, enti pubblici e singoli cittadini trasmettono grandi quantità di dati personali attraverso i confini nazionali all'interno dell'UE. Un eventuale conflitto di norme nazionali sulla protezione di dati presenti in vari paesi interromperebbe gli scambi internazionali, frenando il mercato e il processo di integrazione economica e sociale: è anche per questo motivo, quindi, che sono state emanate norme UE comuni volte a garantire che i dati personali delle persone fisiche godano di un livello elevato di protezione ovunque all'interno dell'UE.

Inoltre, la direttiva 95/46/CE sul trattamento dei dati personali contempla delle disposizioni specifiche per il trasferimento di dati personali anche fuori dall'Unione Europea, al fine di garantirne la migliore protezione possibile.

La direttiva, che è stata ratificata da tutti gli Stati membri dell'Unione Europea, viene applicata anche in Islanda, Liechtenstein e Norvegia.

Oggi più che mai bisogna rendersi conto che la protezione dei dati personali è un vero e proprio diritto fondamentale che riguarda le azioni quotidiane di tutti noi e che, nel contempo, la libera circolazione dei dati personali è indispensabile affinché i cittadini europei possano agire ed operare liberamente all'interno di uno spazio comune.

LA DIRETTIVA UE

La direttiva 95/46/EC del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati rappresenta la base normativa di riferimento in materia di protezione dei dati personali.

La direttiva è impostata in modo tale da riuscire a creare un equilibrio tra due tendenze fondamentali dell'Unione europea:

- da un lato l'istituzione di relazioni sempre più strette tra gli Stati membri e l'eliminazione delle barriere che impediscono l'instaurazione e il funzionamento del mercato interno in cui è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali: un mercato che esige che i dati personali possano circolare liberamente da uno Stato membro all'altro;

- dall'altro lato l'aumento e l'equiparazione tra gli Stati membri dei livelli di protezione dei diritti fondamentali sanciti dalle costituzioni nazionali e dalle leggi degli Stati membri, nonché dalla Convenzione Europea di Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali (in particolare all'art.8 "Diritto alla vita privata").

In questo modo la direttiva, grazie al ravvicinamento delle legislazioni, permette la libera circolazione di dati personali tra gli Stati membri, senza che questi ultimi possano ostacolarla.

L'azione degli Stati viene, infatti, limitata entro un margine di manovra ben definito.

APPLICAZIONE DELLA DIRETTIVA

La direttiva si applica al trattamento di dati personali interamente o parzialmente automatizzato, nonché al trattamento non automatizzato di dati personali contenuti o destinati ad archivi.

Un'applicazione limitata è prevista per il trattamento di suoni e immagini finalizzato all'attività giornalistica o all'espressione letteraria o artistica.

La direttiva, invece, non si applica nel caso in cui:

- il trattamento di dati personali venga effettuato da una persona fisica nell'esercizio di attività a carattere esclusivamente personale o domestico (ad esempio la corrispondenza privata, un'agenda elettronica personale o un file con dati riferiti alla famiglia o agli amici);

- il trattamento dei dati personali venga effettuato per l'esercizio di attività attinenti alla pubblica sicurezza, alla difesa, alla sicurezza dello Stato e alle attività dello Stato in materia di diritto penale (art. 3) che non rientrano nel campo di applicazione del diritto comunitario. In questo caso gli Stati membri possono limitare il diritto alla privacy, fermo restando il rispetto dei diritti e delle libertà fondamentali delle persone fisiche previsti dalle convenzioni internazionali e dal diritto europeo (come ad esempio la Carta dei diritti fondamentali dell'Unione europea, Nizza 2000).

COSA SONO I DATI PERSONALI?

Con questo termine si intende qualsiasi informazione attraverso cui una persona fisica che può essere identificata o identificabile direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

SECONDO QUALI PRINCIPI DEVONO ESSERE TRATTATI I DATI PERSONALI?

La direttiva 95/46/CE impone il rispetto di principi sia di legittimità, sia di merito.

Principi di legittimità - Il trattamento di dati personali può essere effettuato soltanto quando la persona interessata ha manifestato il proprio consenso in maniera inequivocabile oppure qualora il trattamento sia necessario per:

- eseguire un contratto concluso con la persona interessata;
- adempiere un obbligo legale da parte del titolare del trattamento;
- tutelare l'interesse vitale della persona interessata;
- eseguire una funzione di pubblico interesse ;
- perseguire l'interesse legittimo del titolare del trattamento.

Principi di merito - I dati devono essere trattati lealmente e lecitamente, per finalità determinate, esplicite e legittime. I dati devono essere esatti, aggiornati, adeguati, pertinenti e non eccedenti (nel contenuto e nei tempi) rispetto alle finalità previste.

COSA SONO I DATI PERSONALI SENSIBILI?

Si tratta di informazioni che riguardano la sfera più privata di una persona. In questa definizione rientra qualsiasi informazione che possa rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati relativi alla salute e alla vita sessuale di una persona.

E' POSSIBILE TRATTARE DATI PERSONALI SENSIBILI?

La direttiva vieta il trattamento di dati personali sensibili. (Art.8 par.1)

Tuttavia, con opportune garanzie a livello nazionale, sono previste delle deroghe a questo divieto (art.8 par.2 e 3) nel caso in cui:

- la persona interessata abbia dato il proprio consenso esplicito;

- il trattamento sia necessario per consentire al titolare del trattamento di rispettare obblighi specifici in materia di diritto del lavoro;

- il trattamento sia necessario per salvaguardare un interesse vitale della persona interessata qualora la stessa non possa dare il proprio consenso per incapacità fisica o giuridica;

- il trattamento sia effettuato da un organismo no-profit con scopi politici, filosofici, religiosi o sindacali, nell'ambito della propria attività ed esclusivamente nei confronti dei propri membri;

- il trattamento riguardi dati resi manifestamente pubblici dalla persona interessata;

- il trattamento sia necessario alla prevenzione o alla diagnostica medica e venga effettuato da un professionista in campo sanitario soggetto al segreto professionale;

- il trattamento riguardi dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza: in tal caso il trattamento può essere effettuato solo sotto controllo dell'autorità pubblica sulla base del diritto nazionale (art. 8 par.5). Qualora il trattamento di dati riguardi sanzioni amministrative e/o procedimenti civili, gli Stati hanno la facoltà di prevedere che il trattamento venga effettuato sotto il controllo dell'autorità pubblica. Inoltre, gli Stati membri possono definire ulteriori deroghe per motivi di interesse pubblico rilevante. In questi casi, comunque, gli Stati membri hanno l'obbligo di notifica alla Commissione.

CHE POTERI ABBIAMO SUI NOSTRI DATI CHE VENGONO TRATTATI?

Gli artt. 10 e 11 della direttiva prevedono che il titolare del trattamento debba fornire alla persona interessata specifiche informazio-

ni, come ad es. l'identità del titolare del trattamento , le finalità del trattamento, i destinatari dei dati ecc.

Inoltre, l'art. 12 della direttiva prevede che l'interessato possa esercitare il diritto di accesso ai propri dati per:

- verificare l'esistenza o meno di trattamenti di dati che la riguardano, il tipo di dati trattati, le finalità e i destinatari del trattamento;

- chiedere la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non sia conforme alla direttiva.

Infine, l'art. 14 garantisce il diritto della persona interessata ad opporsi, per ragioni legittime, al trattamento di dati che la riguardano e di opporsi, su richiesta e gratuitamente, al trattamento di dati a fini di invio di materiale pubblicitario.

SONO PREVISTE DELLE DEROGHE AI PRINCIPI DELLA DIRETTIVA?

Oltre ai settori in cui la direttiva non si applica (rif. "Applicazione della direttiva"), la direttiva 95/46/EC all'art. 13 prevede che gli Stati membri possano adottare disposizioni legislative intese a limitare il diritto di accesso e di informazione degli interessati al trattamento, qualora tali restrizioni costituiscano una misura necessaria per:

- la sicurezza, la difesa, la pubblica sicurezza dello Stato;

- la prevenzione, la ricerca, l'accertamento e il perseguimento di infrazioni penali oltre che di violazioni della deontologia delle professioni regolamentate;

- la salvaguardia di un rilevante interesse economico o finanziario di uno Stato membro o dell'UE;

- la protezione della persona interessata o dei diritti e delle libertà altrui.

Nello specifico, la direttiva europea dispone che ciascuno Stato membro, esclusivamente nel caso in cui stia perseguendo uno de-

gli obiettivi sopraelencati, possa decidere di limitare i principi contenuti nei seguenti articoli:

- art. 6 par.1: derogando a questo articolo, lo Stato può evitare di rendere esplicite le finalità del trattamento dei dati, utilizzare i dati raccolti per scopi che eccedono le finalità per le quali sono stati raccolti originariamente, conservare i dati per un arco di tempo superiore a quello necessario al conseguimento delle finalità per le quali sono stati rilevati;

- art. 10 e art. 11 par.1: in questo caso lo Stato ha la possibilità di limitare il diritto della persona interessata a ricevere le informazioni riguardanti il trattamento dei propri dati;

- art. 12: la direttiva prevede anche la possibilità di negare alla persona interessata il diritto di accesso alle informazioni relative al trattamento dei propri dati;

- art. 21: in linea con le deroghe precedenti, vi è anche la possibilità di derogare all'obbligo di pubblicità dei trattamenti per gli Stati membri.

In sintesi, in materia di trattamento dei dati personali, gli Stati membri mantengono, a livello nazionale, un certo grado di autonomia nell'applicazione della direttiva in esame, sostanzialmente riconducibile a due ambiti, e cioè:

- le materie a cui le disposizioni della direttiva europea non sono applicabili (Rif. "Applicazione della direttiva");

- le deroghe ad alcuni articoli specifici della direttiva (di cui art. 13).

CHI SI OCCUPA DELLA SICUREZZA DEI DATI TRATTATI?

Il titolare del trattamento, o chiunque agisca sotto la sua autorità, può elaborare i dati personali ai quali ha accesso solo su istruzione del titolare stesso. Quest'ultimo ha il dovere di adottare misure appropriate per proteggere i dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla diffusio-

ne o dall'accesso non autorizzato.

Gli artt. 18, 19 e 20 della direttiva, inoltre, prevedono un obbligo di notificazione dei trattamenti all'autorità di controllo costituita nell'ambito di ciascun paese, prima di procedere alla realizzazione del trattamento stesso. La notificazione deve avere come oggetto: il nome e l'indirizzo del titolare del trattamento, le finalità del trattamento, una descrizione delle categorie di persone interessate e dei dati, i destinatari a cui possono essere comunicati i dati, i trasferimenti di dati previsti verso paesi terzi e una descrizione generale delle misure di sicurezza adottate. Una volta ricevuta la notificazione, l'autorità di controllo effettua esami preliminari volti ad accertare l'esistenza di rischi per i diritti e le libertà delle persone interessate. Sono esenti da questo obbligo solo i titolari che abbiano designato, conformemente alla legislazione nazionale applicabile, un responsabile del trattamento incaricato, appunto, di garantire che il trattamento non rechi pregiudizio ai diritti e alle libertà della persona interessata.

COSA SUCCEDE IN CASO DI VIOLAZIONE DELLE DISPOSIZIONI DELLA DIRETTIVA?

Fatta salva la possibilità di presentare ricorso amministrativo davanti all'autorità di controllo prima di adire l'autorità giudiziaria, la direttiva prevede che chiunque possa promuovere un ricorso giurisdizionale in caso di violazione dei diritti garantitigli dalle norme nazionali applicabili al trattamento in questione. Inoltre, chiunque subisca un danno cagionato da un trattamento illecito dei propri dati personali, o da qualsiasi altro atto incompatibile con la normativa nazionale di attuazione della direttiva, ha il diritto di ottenere il risarcimento del pregiudizio subito.

Infine, i singoli Stati stabiliscono le sanzioni da applicare in caso di violazione delle disposizioni di attuazione della presente direttiva.

In sintesi, la violazione della privacy è un reato: chi fa un cattivo uso dei nostri dati, può essere punito.

E' POSSIBILE TRASFERIRE I DATI PERSONALI FUORI DALL'UNIONE EUROPEA?

Sì, ma soltanto se il paese terzo in questione garantisce un livello di protezione adeguato. Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non sia affidabile (art. 25) e, qualora la Commissione verifichi che il paese terzo non garantisca un adeguato livello di protezione, gli Stati membri adottano tutte le misure necessarie al fine di impedire ogni trasferimento di dati.

Tuttavia, è possibile effettuare il trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata (art. 26) a condizione che:

- la persona interessata abbia manifestato il proprio consenso;

- il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il titolare del trattamento;

- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto a favore della persona interessata;

- il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante oppure per costatare, esercitare o difendere un diritto per via giudiziaria;

- il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata;

- il trasferimento avvenga a partire da un registro pubblico.

COME FUNZIONA L'AUTORITA' DI CONTROLLO?

L'art. 28 della direttiva dispone che ciascuno Stato membro debba istituire una o più autorità pubbliche e completamente indipendenti, incaricate di sorvegliare, all'interno del proprio territorio, l'applicazione delle disposizioni di attuazione della presente direttiva. I rappresentanti di queste autorità di controllo nazionali, insieme ai rappresentanti delle autorità di controllo create per le istituzioni e gli organismi comunitari e ad un rappresentante della Commissione,

compongono il "gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" (artt. 29 e 30). Quest'ultimo ha il compito di:

- esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della direttiva;

- formulare un parere sul livello di tutela nella Comunità e nei paesi terzi;

- consigliare la Commissione in merito a ogni progetto di modifica della direttiva stessa;

- formulare un parere sui codici di condotta elaborati a livello comunitario.

2. EVOLUZIONE DELLA DIRETTIVA UE SULLA PROTEZIONE DEI DATI

Il 15 maggio 2003 la Commissione ha trasmesso al Parlamento **la prima relazione sull'applicazione della direttiva 95/46/EC (COM(2003) 265), a cui è seguita una risoluzione del Parlamento europeo (COM(2003) 265 – 2003/2153(INI)).**

Con questa relazione la Commissione ha fatto un primo bilancio della protezione della privacy nella UE. Inoltre, ha analizzato il problema dell'attuazione delle direttive, il problema del trasferimento dei dati personali a Stati terzi e le minacce poste dalle ingerenze dello Stato e da terzi alla protezione della privacy.

CONSIDERAZIONI

Nonostante i ritardi e le lacune costatate nella sua applicazione, tanto che l'11/1/2000 la Commissione ha avviato delle procedure d'infrazione nei confronti di Francia, Paesi Bassi, Germania e Irlanda, la direttiva ha raggiunto entrambi gli obiettivi principali che si era posta:

- eliminare gli ostacoli alla libera circolazione dei dati personali tra gli Stati membri,

- garantire un alto livello di protezione all'interno dell'Unione Europea.

Tuttavia, da questi documenti è emerso che le istituzioni sono concordi nell'affermare che l'obiettivo di livellare ed uniformare le diverse legislazioni in materia di tutela dei dati fra gli Stati membri non sia stato raggiunto. Queste disparità impediscono alle organizzazioni multinazionali di definire politiche paneuropee in materia di tutela dei dati.

CRITICITA'

Le principali difficoltà emerse rispetto all'applicazione della direttiva europea sulla protezione dei dati sono tre:

1. l'insufficienza di risorse destinate all'applicazione,

2. un rispetto della norma da parte dei titolari del trattamento disomogeneo;

3. la scarsa conoscenza dei propri diritti che sembrano avere le persone interessate, che può essere all'origine del fenomeno precedente.

In questi documenti le istituzioni europee mettono in luce anche la necessità di estendere l'applicazione della direttiva ai settori relativi a sicurezza, difesa e cooperazione giudiziaria, ancora regolati in modo parziale e frammentario da specifiche disposizioni nazionali.

Questa considerazione deriva dagli attacchi terroristici di matrice islamica che hanno colpito il mondo occidentale all'inizio degli anni 2000, che hanno spinto la Commissione a riconoscere la necessità di armonizzare la legislazione esistente all'interno di un quadro comune, conciliando l'esigenza della riservatezza individuale con l'interesse superiore della sicurezza interna degli stati membri.

Per questi motivi, il Parlamento europeo nella sua risoluzione esorta la Commissione a proporre "uno strumento giuridico" vincolante sulla protezione della vita privata nell'ambito della cooperazione di polizia e giudiziaria in materia penale, in particolare con riferimento a Europol e Eurojust (quello che una volta era definito il "terzo pilastro"), per arrivare alla definzione, nel minore tempo possibile, di un effettivo spazio europeo di libertà, sicurezza e giustizia caratterizzato dalla collaborazione contro la criminalità a livello sovranazionale.

Con la Relazione del 2003 la Commissione, inoltre, aveva presentato un programma di lavoro per migliorare l'applicazione della direttiva all'interno degli Stati membri prevedendo di svolgere le seguenti attività:

1. dialogo strutturato con gli Stati membri e le autorità incaricate della protezione dei dati sul recepimento a livello nazionale della direttiva;

2. collaborazione con le autorità dei paesi candidati per il recepi-

mento della direttiva nella legislazione nazionale per limitare al massimo future procedure formali d'infrazione,

3. miglioramento della notifica degli atti giuridici che recepiscono la direttiva,

4. esecuzione, notificazione e pubblicizzazione delle operazioni di trattamento, al fine di facilitare scambi di buone pratiche e offrire orientamenti;

5. disposizioni più armonizzate in materia di informazione;

6. semplificazione dei requisiti per i trasferimenti internazionali dei dati,

7. promozione delle tecnologie per aumentare la tutela della vita privata,

8. promozione dell'autoregolamentazione e dei codici di condotta europei: la Commissione è riuscita a fare approvare il codice di condotta europeo della Federazione del marketing diretto europeo (FEDMA);

9. sensibilizzazione dei cittadini europei sulla privacy (un'indagine Eurobarometro aveva messo in evidenza che i cittadini , pur interessati, non erano sufficientemente al corrente delle norme e dei meccanismi esistenti per tutelare i loro diritti).

Il lavoro svolto nell'ambito del programma di cui sopra viene dettagliatamente riferito dalla Commissione al Parlamento europeo e al Consiglio con la **Comunicazione del 27 marzo 2007 intitolata "Seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati"** (COM(2007)87 def.).

Dalla relazione emerge che la Commissione, rilevando un miglioramento nell'attuazione della direttiva, non ritiene necessario intervenire con degli emendamenti, tanto più che le imprese, adeguando la propria attività ai nuovi precetti, hanno già sostenuto dei costi.

La direttiva è considerata una base giuridica generale che soddisfa

gli obiettivi originari, dal momento che costituisce una garanzia sufficiente per il funzionamento del mercato interno pur assicurando un livello elevato di protezione. Essa rappresenta un punto di riferimento in numerosi settori d'azione, è neutra nei confronti della tecnologia e continua a fornire risposte solide ed adeguate ai problemi di questo tipo.

Due sono gli aspetti della norma che, secondo la Commissione, richiedono una certa attenzione:

- l'indipendenza e l'autonomia delle autorità nazionali di controllo, responsabili dell'applicazione della direttiva;

- il margine di autonomia che alcuni disposizioni della direttiva, formulate in maniera vaga, lasciano, esplicitamente o implicitamente, agli Stati membri nell'adozione delle legislazione nazionale e che potrebbero causare divergenze nell'applicazione della norma comunitaria.

Infine, la Commissione richiama l'attenzione sulla necessità di prevedere, nel percorso di miglioramento della legislazione sulla protezione dei dati a livello europeo, procedure più efficaci nel settore della libertà, sicurezza e giustizia, in conformità a quanto previsto nei trattati attuali

In questo senso il primo strumento normativo adottato dalle istituzioni europee è la decisione quadro del Consiglio dell'Unione Europea sulla protezione dei dati personali nella cooperazione giudiziaria e di polizia in materia penale del 2008, di cui si dirà al Cap. 4.

3. LE COMUNICAZIONI ELETTRONICHE E LA TUTELA DELLA VITA PRIVATA

Lo sviluppo della società dell'informazione ha avuto, tra le sue conseguenze, l'introduzione di nuovi servizi di comunicazione elettronica. L'accesso alle reti digitali mobili è ormai a disposizione e alla portata di un vasto pubblico e questo significa che, se da un lato la diffusione delle nuove tecnologie e di internet ha consentito agli utenti di usufruire di nuove possibilità, dall'altro ha messo in luce ulteriori esigenze di tutela dei dati personali e della vita privata degli utenti.

In quest'ottica il Parlamento europeo e il Consiglio dell'Unione europea hanno provveduto ad adottare la ***direttiva 2002/58/CE del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche,*** successivamente modificata dalla **Direttiva 2009/136/CE del 25 novembre 2009.**

LA DIRETTIVA UE

La direttiva 2002/58/CE, che integra la direttiva 95/46/CE, nel perseguire l'obiettivo di tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche nel settore delle reti pubbliche di comunicazione, tende all'armonizzazione delle disposizioni legislative e regolamentari degli Stati membri affinché non vi siano ostacoli alla promozione e allo sviluppo di nuovi servizi e reti di comunicazione elettronica all'interno dell'Unione europea.

Analogamente alla direttiva 95/46/CE, questa direttiva non altera l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di adottare i provvedimenti necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato e l'applicazione della legge penale. Gli stati membri, quindi, hanno la facoltà di effettuare intercettazioni legali di comunicazioni elettroniche, o di prendere altre misure per perseguire tali scopi, sempre e comunque nel rispetto della Convenzione europea di salvaguardia dei diritti dell'uomo e delle liberà fondamentali.

APPLICAZIONE DELLA DIRETTIVA

La direttiva 2002/58/CE si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità (art. 3).

PRINCIPALI PUNTI CHIAVE SULLA SICUREZZA DEI DATI

Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve adottare misure tecniche e organizzative appropriate per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete (art. 4).

Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico (art. 5).

I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione.

Il fornitore dei servizi deve informare l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del trattamento (art. 6).

4. LA PROTEZIONE DEI DATI PERSONALI NELL'AMBITO DELLA COOPERAZIONE GIUDIZIARIA E DI POLIZIA IN MATERIA PENALE

Nel novembre 2008 il Consiglio dell'Unione europea ha adottato una Decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (Decisione quadro 2008/977/GAI del 27 novembre 2008).

Si tratta del primo strumento europeo adottato per la protezione dei dati in questo settore.

Questa decisione quadro intende proteggere i diritti e le libertà fondamentali delle persone fisiche quando i loro dati personali sono trattati ai fini della prevenzione, dell'indagine, dell'accertamento o del perseguimento dei reati o dell'esecuzione delle sanzioni penali. Essa si applica al trattamento di dati personali, interamente o parzialmente automatizzato, nonché al trattamento non automatizzato di dati personali figuranti negli archivi.

È opportuno sottolineare che, comunque, la decisione quadro in questione non pregiudica in alcun modo gli interessi fondamentali della sicurezza nazionale e specifiche attività di informazione nel settore della sicurezza nazionale. (art.1)

IN CHE MODO VENGONO TUTELATI I NOSTRI DATI IN QUESTO SETTORE?

I dati personali possono essere raccolti dalle autorità competenti degli Stati membri soltanto per finalità specifiche, esplicite e legittime, e possono essere trattati solo per la finalità per la quale sono stati raccolti. (art.3)

Tuttavia, la decisione quadro 2008/977/GAI prevede la possibilità di un trattamento dei dati per un'altra finalità rispetto a quella per cui i dati sono stati raccolti solo a condizione che:

- l'ulteriore trattamento non sia incompatibile con le finalità per le quali i dati sono stati raccolti;

- le autorità competenti siano autorizzate a tale trattamento;

- il trattamento sia necessario e proporzionato alla nuova finalità.

I dati personali sono rettificati se inesatti e, laddove possibile e necessario, sono completati o aggiornati. I dati personali sono cancellati, resi anonimi o, in alcuni casi, bloccati, se non sono più necessari per le finalità per le quali sono stati raccolti. Sono previsti adeguati termini per la cancellazione dei dati personali o per il controllo periodico necessario alla memorizzazione dei dati.

Le autorità competenti degli Stati membri devono verificare che i dati personali da trasmettere o resi disponibili siano esatti, aggiornati e completi. Ai fini della verifica della legalità del trattamento dei dati e per garantire l'integrità e la sicurezza dei dati, tutte le trasmissioni di dati personali devono essere registrate o documentate. (da art.4 a art.10).

POSSONO ESSERE TRATTATI I DATI SENSIBILI?

In linea di principio, il trattamento di dati personali sensibili, cioè quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati relativi alla salute e alla vita sessuale, non è ammesso. Il loro trattamento è ammesso solo se strettamente necessario e se la legislazione nazionale prevede adeguate garanzie. (art.6).

TRASMISSIONE DEI DATI (da art. 11 a art. 14)

I dati personali ricevuti da un altro Stato membro devono essere trattati solo per le finalità per le quali sono stati trasmessi.

Tuttavia, in alcuni casi, possono essere trattati per finalità diverse, ad esempio per la prevenzione, l'indagine, l'accertamento o il perseguimento di altri reati, l'esecuzione di altre sanzioni penali o la prevenzione di gravi minacce alla sicurezza pubblica. Lo Stato membro ricevente deve rispettare le eventuali restrizioni allo scambio di dati, previste dalla legge dello Stato membro che trasmette i dati.

In taluni casi lo Stato membro ricevente può trasferire i dati personali a paesi terzi o a organismi internazionali. A tal fine, lo Stato membro che per primo ha reso disponibili i dati deve acconsentire al trasferimento. Il trasferimento dei dati senza il consenso preliminare è ammesso solo in casi urgenti. I dati personali possono anche essere trasmessi a privati negli Stati membri per finalità esclusive, a condizione che l'autorità competente dello Stato membro presso cui i dati sono stati ottenuti abbia dato il consenso.

QUALI SONO I NOSTRI DIRITTI? (da art. 15 a art. 21)

La persona interessata deve essere informata della raccolta o del trattamento di dati personali che la riguardano. Tuttavia, qualora siano stati trasmessi dati personali tra Stati membri, ciascuno Stato membro può chiedere che l'altro Stato membro non informi la persona interessata.

Ogni persona interessata ha il diritto di richiedere una conferma del fatto che dati che la riguardano siano stati trasmessi, nonché informazioni sui destinatari e sui dati che sono oggetto di trattamento, e una conferma che sono state effettuate tutte le verifiche necessarie dei dati. In alcuni casi gli Stati membri possono limitare l'accesso alle informazioni da parte della persona interessata. Qualsiasi decisione di restrizione dell'accesso deve essere comunicata per iscritto alla persona interessata, insieme ai motivi di fatto o di diritto sui quali la decisione si basa. La persona interessata deve anche essere informata del diritto a presentare ricorso contro tale decisione.

La persona interessata può richiedere che i dati personali che la riguardano siano rettificati, cancellati o bloccati. Qualsiasi rifiuto di dar seguito a tali azioni deve essere comunicato per iscritto alla persona interessata, che deve essere informata della opportunità di presentare un reclamo o un ricorso.

Chiunque subisca un danno cagionato da un trattamento illegale dei dati personali o da qualsiasi altro atto incompatibile con la presente decisione quadro, ha il diritto di ottenere il risarcimento. In caso di violazione dei suoi diritti, la persona interessata ha il diritto di ricorrere in via giurisdizionale.

CHI SI OCCUPA DELLA SICUREZZA DEI NOSTRI DATI? (artt. 22-23).

Le autorità competenti devono adottare le misure di sicurezza necessarie per proteggere i dati personali da qualsiasi forma illegittima di trattamento, nonché dalla perdita accidentale, alterazione, divulgazione o accesso non autorizzati. In particolare, devono essere adottate misure specifiche per il trattamento automatizzato dei dati.

Le autorità nazionali di controllo all'interno degli Stati membri sorvegliano e forniscono consulenza sull'applicazione della presente decisione quadro. A tale scopo, ogni autorità di controllo dispone di poteri investigativi, di poteri effettivi d'intervento, nonché del potere di promuovere azioni giudiziarie. In caso di violazione delle disposizioni della presente decisione quadro, gli Stati membri devono stabilire sanzioni efficaci, proporzionate e dissuasive.

Come previsto dalla direttiva 95/46/EC, di cui al precedente Cap. 2, anche in questo caso sono gli Stati membri a stabilire sanzioni efficaci, proporzionate e dissuasive in caso di violazione delle disposizioni adottate. (art. 24).

Infine, l'articolo 27 della decisione quadro 2008/977/GAI dispone che entro il 27 novembre 2013, gli Stati membri comunichino alla Commissione le rispettive disposizioni nazionali adottate per conformarsi pienamente alla normativa europea. A distanza di un anno, la Commissione riferirà al Parlamento europeo e al Consiglio in merito ai risultati della valutazione prevista. (art. 27).

5. GLI ULTIMI SVILUPPI

Il 25 gennaio 2012 la Commissione europea ha presentato la proposta del nuovo Regolamento europeo che andrà a sostituire la direttiva 95/46/EC che rafforzerà i diritti della provacy on-line e darà una spinta all'economia digitale dell'Europa. Il progresso tecnologico e la globalizzazione, infatti, hanno cambiato profondamente il modo in cui vengono raccolti e trattati i dati. Inoltre, all'interno degli Stati membri vi sono disparità nell'applicazione pratica della direttiva 95/46/EC.

La riforma nasce dalla necessità di definire un quadro unico di riferimento per tutte le autorità nazionali incaricate della protezione dei dati in modo che la materia sia trattata ovunque in maniera uniforme, coerente e armonica.

L'obiettivo è quello di formulare una legge unica in grado di far fronte all'attuale frammentazione e di ridurre i grandi oneri economici e amministrativi, in modo da riuscire a risparmiare circa 2.3 miliardi di euro all'anno. L'iniziativa aiuterà anche a rafforzare la fiducia dei consumatori nei servizi on line, dando quindi una spinta propulsiva a questo settore.

COSA PROPONE LA RIFORMA?

La Commissione intende semplificare e ottimizzare le regole sulla protezione dei dati in Europa, rafforzando l'armonizzazione tra le normative in essere. La direttiva 95/46/EC, pur essendo stata adottata e implementata in modo pressoché uniforme in tutti gli Stati dell'Unione europea, ha dato vita ad un sistema normativo che presenta ancora degli squilibri e le imprese possono trovarsi nella condizione di rispettare le diverse legislazioni per la protezione dei dati personali! Ne deriva una cornice legale frammentata, incerta e diseguale. Il sistema com'è oggi comporta dei costi superflui e un peso amministrativo rilevante per chiunque voglia intraprendere delle attività economiche. Questa situazione complessa disincentiva il business – soprattutto quello delle piccole e medie imprese (SMEs) – e rappresenta un ostacolo per la crescita economica.

Con il nuovo Regolamento che sarà direttamente e immediatamente esecutivo e non necessiterà del recepimento da parte degli Stati membri si potrà avere una singola legge applicabile in tutta l'Unione europea e si raggiungerà un'armonizzazione sostanziale di protezione dei dati. I risparmi stimati che ne deriveranno ammonteranno a circa 2.3 miliardi di euro all'anno.

La Commissione stabilirà un sistema in cui le imprese avranno a che fare con una singola autorità per la protezione dei dati, e cioè, l'autorità del paese in cui l'impresa ha la propria sede principale.

Le autorità nazionali per la protezione dei dati coopereranno sulle singole questioni adottando una visione europea più ampia, garantendo la protezione del diritto alla privacy di tutti gli europei, in qualsiasi paese membro essi risiedano.

In questo modo, le attività delle singole imprese economiche faciliteranno lo sviluppo del mercato unico digitale, favorendo la crescita economica, l'innovazione e la creazione di posti di lavoro. I soggetti economici che avranno maggiori benefici da questa riforma saranno le piccole-medie imprese. Inoltre il nuovo regime porterà dei vantaggi alle imprese europee anche all'interno della competizione globale, poiché saranno in grado di offrire ai propri clienti delle garanzie basate su una legislazione forte e completa.

Un unico sistema di regole a livello europeo avrà infatti un impatto significativo sul business e rafforzerà la visione di un'Europa in cui conviene investire e fare affari.

.

Aspetti sostanziali della riforma

Con il nuovo Regolamento gli interessati avranno nuove tutele e nuovi diritti, che si traduranno in nuovi obblighi a carico di Titolari e Responsabili del trattamento di dati personali.

Le principali novità del regolamento saranno:

il diritto all'oblio (vicino al principio di common-law "the right to be let alone): l'interessato avrà il diritto di ottenere dal Titolare del trattamento la cancellazione totale dei dati personali che lo riguardano e la rinuncia a una loro ulteriore diffusione;

il diritto alla portabilità dei dati personali: l'interessato potrà sia trasferire i propri dati da un sistema elettronico ad un altro, sia ottenere gli stessi in un formato elettronico che consenta di farne un ulteriore uso;

i diritti dei minori: data la diffusione delle tecnologie anche tra i più giovani, la proposta di regolamento pone un'attenzione particolare ai mezzi attraverso cui ottenere il consenso per il trattamento dei dati personali appartenenti a minorenni;

i confini di applicabilità della normativa: la normativa si applicherà anche ai trattamenti svolti al di fuori della UE se relativi all'offerta di beni o sevizi a cittadini UE, indipendentemente quindi dalla sede del Titolare del trattamento. Tale modifica è notevole, in quanto innalzerà il livello di tutela per i cittadini europei all'interno dello spazio digitale, poiché, soprattutto nell'era del "cloud computing", avrà grandi ricadute su quelle imprese che offrono servizi via internet, ma non hanno sede in Europa;

gli obblighi del titolare del trattamento: il titolare avrà l'obbligo di e conservare opportune documentazioni in quanto dovrà essere in grado di dimostrare che i trattamenti effettuati sono conformi alla normativa. In caso di trattamenti rischiosi avrà l'obbligo di prevedere valutazioni e verifiche preventive da parte dell'Autorità al fine di limitare i rischi. Per contro non avrà più l'obbligo di notificare i trattamenti all'autorità, con evidente semplificazione amministrati-

va e risparmio economico per le imprese;

l'obbligo di notifica di violazioni: in caso di violazione di sicurezza che provoca, anche accidentalmente, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso a dati personali, il Titolare avrà l'obbligo provvedere alla relativa notifica alle autorità e, in alcuni casi, ai diretti interessati;

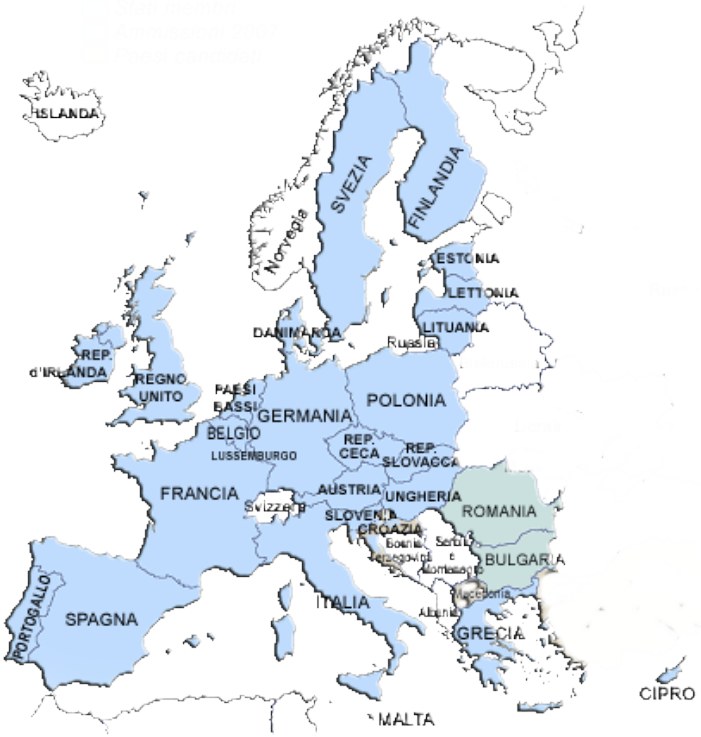
il sistema delle sanzioni: in caso di violazioni, le multe potranno essere pari anche al 2% del volume d'affari annuo dell'impresa;

il Data protection officer (o Privacy officer): la proposta di regolamento prevede che le aziende con più di 250 dipendenti e tutti i soggetti pubblici dovranno istituire tale figura professionale. Il Data protection officer (Responsabile della protezione dei dati) dovrà sorvegliare l'attuazione e l'applicazione del regolamento, con particolare riguardo ai requisiti concernenti la protezione e la sicurezza dei dati fin dalla progettazione del processo aziendale e degli applicativi informatici di supporto. Inoltre dovrà curare l'informazione agli interessati e le richieste di questi ultimi di esercitare i propri diritti. Potrà essere una figura interna o esterna all'azienda, indipendente, con un'ampia conoscenza della normativa, funzionalmente dipendente dai vertici aziendali.

N.B. Il Data Protection Officer è una figura professionale già riconosciuta in alcuni Paesi europei, ma non prevista, al momento, dalla normativa italiana. L'ex Presidente dell'Autorità Garante per la Privacy, Francesco Pizzetti, intervenne a favore della sua istituzione già nel 2006, in occasione dell'European Privacy Officers Forum – Epof, Associazione che riunisce, appunto, i Privacy Officers operanti all'interno di circa 35 società multinazionali con sede in Europa.

SECONDA PARTE

LE SCHEDE DEI PAESI DELL'UNIONE EUROPEA



AUSTRIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita con il Data Protection Act, Gazzetta Federale parte I No. 165/1999 e successive modifiche/integrazioni.
DEFINIZIONE DI DATI PERSONALI	Qualunque informazione relativa ad un soggetto identificato o identificabile.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Austrian Data Protection Commission Datenschutzkommision
	Salvo eccezioni, i trattamenti su dati personali con sistemi automatizzati devono essere notificati dai titolari del trattamento all'Autorità nazionale per la protezione dei dati che li conserva in un registro accessibile al pubblico. Le eccezioni sono definite per decreto dal Federal Chancellor. La notificazione deve includere le seguenti informazioni standard: - titolo e finalità della richiesta di dati; - contatto del titolare del trattamento e/o dell'eventuale rappresentante; - categorie dei dati personali trattati;

	- se sono stati trattati dati sensibili; - i destinatari dei dati trattati; - chi può effettuare il trattamento; - una descrizione delle misure di sicurezza; - il riferimento all'eventuale autorizzazione al trasferimento di dati all'estero concessa dall'Autorità per la protezione dei dati.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Le organizzazioni non hanno l'obbligo legale di nominare al loro interno un DPO.
RACCOLTA E TRATTAMENTO DEI DATI	Il titolare può raccogliere e trattare i dati solo se legalmente autorizzato e nei seguenti casi: - ha il consenso dell'interessato (che può essere revocato in qualsiasi momento); - il trattamento è necessario per consentire al titolare di adempiere ai propri diritti/doveri; - il trattamento è necessario per proteggere gli interessi vitali del soggetto interessato; - il trattamento è necessario affinché il Titolare del trattamento, o terzi, possa proteggere

	un interesse legittimo (salvo il caso in cui sia prioritario proteggere un diritto soggettivo dell'interessato). In caso di trattamento di dati sensibili, esiste una lista di specifiche condizioni da rispettare. In ogni caso non si viola il diritto alla riservatezza quando: 1) i dati sono resi chiaramente pubblici dal'interessato; 2) i dati sono usati solo in forma personale indiretta; 3) l'uso dei dati è autorizzato o richiesto per legge e per l'interesse pubblico; 4) i dati sono usati dalle autorità statali per un'assistenza tra le autorità; 5) i dati si riferiscono esclusivamente all'esercizio di una funzione pubblica dell'interessato; in questo caso la revoca è possibile in qualsiasi momento; 6) l'interessato ha dato il consenso esplicito; 7) il trattamento dei dati è necessario per salvaguardare gli interessi vitali dell'interessato dei dati e il consenso non può essere ottenuto in tempo;

	8) l'uso dei dati è necessario per salvaguardare gli interessi vitali di una parte terza; 9) l'uso dei dati è necessario per tutelare e difendere il titolare del trattamento di fronte all'autorità, sempre che tali dati siano stati raccolti a norma di legge; 10) l'uso dei dati è solo per scopi privati, statistici o di ricerca; 11) l'uso dei dati è necessario in conformità alla legge sul lavoro; 12) l'uso dei dati è richiesto in ambito sanitario e i dati sono usati solo dallo staff medico o da altre persone che sono tenute al dovere di riservatezza; 13) i dati riguardanti opinioni politiche e ideologiche sono usati da organizzazioni no-profit con obiettivi politici, filosofici, religiosi o relativi a sindacati e tali dati si riferiscono a membri o sostenitori.
TRASFERIMENTO DEI DATI	E' legale solo se: - i dati hanno origine da un trattamento legale; - i destinatari sono legittimati a ricevere tali dati; - sono tutelati gli interessi dei soggetti dei dati.

	Il trasferimento a destinatari fuori dall'UE può avvenire previa autorizzazione da parte dell'Autorità nazionale per la protezione dei dati, salvi i casi in cui: - il destinatario risieda in un paese che, secondo quando stabilito per decreto dal Federal Chancellor, offre un livello di "protezione adeguata"; - l'interessato acconsente al trasferimento; - sia necessario per l'esecuzione di un contratto a favore dell'interessato; - i dati sono stati legalmente pubblicati in Austria; - i dati trasferiti sono solo indirettamente personali; - il trasferimento transnazionale è autorizzato da regolamenti austriaci aventi il valore di legge e sono immediatamente applicabili; - i dati sono per scopi privati; - i dati sono stati raccolti legalmente ed il trasferimento è necessario per affrontare un contenzioso di fronte ad una autorità straniera; - il trasferimento è espressamente nominato in un trattamento

	standard; - il trasferimento origina da un trattamento per cui non è necessaria la notificazione.
SICUREZZA	Sulla base della tecnologia disponibile e dei costi, i titolari e i responsabili del trattamento devono implementare misure tecniche e organizzative appropriate per proteggere i dati personali contro la distruzione o la perdita intenzionale o accidentale, contro l'accesso o la comunicazione non autorizzati e contro ogni forma di trattamento illegale.
NOTIFICA DI VIOLAZIONE	Dall'inizio del 2010, il Data Protection Act prevede che il titolare del trattamento notifichi al soggetto interessato trattamenti illegali o sistematici dei propri dati, a meno che il danno potenziale all'interessato sia irrilevante o la notifica richieda una spesa irragionevole.
APPLICAZIONE	Chiunque può presentare un reclamo all'autorità nazionale per la protezione dei dati. L'autorità nazionale ha il potere di chiedere dei chiarimenti al titolare del trattamento, di ispezionare la documentazione e, qualora abbia ragionevoli sospetti di illiceità, è autorizzata

	ad indagare sui trattamenti. Qualsiasi violazione del diritto alla segretezza, alla rettifica o alla cancellazione deve essere portata davanti alla corte civile di competenza. L'inosservanza del Data Protection Act può essere sanzionata dall'autorità amministrativa competente con multe fino a 25.000 €.

BELGIO

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita con il Data Protection Act 08/12/1992. La sua applicazione spetta all'Autorità per la protezione dei dati.
DEFINIZIONE DI DATI PERSONALI	Qualunque informazione relativa a una persona fisica identificata o identificabile, direttamente o indirettamente, in particolare con riferimento a un numero di identificazione o a uno o più fattori specifici relativi alla sua identità fisica, psicologica, mentale, economica, culturale o sociale.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Il Data Protection Act del Belgio individua tre categorie di dati personali sensibili, a cui sono applicate regole diverse: 1) dati personali che rivelano l'origine etnica o razziale, le opinioni politiche, il credo religioso o filosofico, la vita sessuale o l'appartenenza a un sindacato di una persona; 2) i dati personali relativi alla salute; 3) i dati personali relativi a controversie davanti a corti, tribunali, anche amministrativi, in materia penale, di sanzioni amministrative o di sicurezza.

AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	*Commission for the Protection of Privacy*
NOTIFICAZIONE DEL TRATTAMENTO	Salvo eccezioni, i trattamenti effettuati su dati personali con sistemi automatizzati devono essere notificati dai titolari all'Autorità nazionale per la protezione dei dati affinché siano registrati e resi pubblici. La notifica deve includere le seguenti informazioni standard: - le finalità del trattamento; - i contatti del titolare del trattamento e/o dell'eventuale rappresentante; - se il trattamento include alcune categorie di dati personali sensibili e, in tal caso, quali; - le categorie di destinatari dei dati e le garanzie che devono essere applicate alla comunicazione a terzi; - il modo in cui i soggetti interessati saranno informati sul trattamento e l'ufficio a cui possono rivolgersi per esercitare il loro diritto d'accesso; - i termini di conservazione dei dati; - una descrizione generale delle misure di sicurezza;

	- in caso di trasferimento fuori dall'UE, le categorie di dati trasferiti e, per ogni categoria, il paese di destinazione.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Le organizzazioni non hanno l'obbligo di nominare al proprio interno il DPO, ma è comunque raccomandato. Il titolare del trattamento e gli incaricati devono comunque adottare tutte le misure tecniche e organizzative necessarie. L'Autorità nazionale ha emesso delle Linee guida per la sicurezza dei trattamenti dei dati che non hanno valore legislativo, ma solo morale. Nelle linee guida si raccomanda la nomina di un Responsabile per la sicurezza per l'implementazione della politica di sicurezza dei dati personali.
RACCOLTA E TRATTAMENTO DEI DATI	Il titolare può raccogliere e trattare i dati qualora: - l'interessato dia il suo consenso; - il trattamento dei dati sia necessario per rispettare un contratto in cui è parte l'interessato; - il trattamento sia necessario per permettere al titolare di rispettare un obbligo legale;

	il trattamento sia necessario per proteggere gli interessi vitali dell'interessato; - il trattamento sia necessario per assolvere un dovere nell'interesse pubblico; - il trattamento sia necessario per esercitare l'autorità pubblica; - il trattamento sia necessario per permettere al titolare del trattamento o a terzi a cui i dati sono stati divulgati, di proteggere un interesse legittimo, eccetto il caso in cui questo interesse non sia di rango inferiore rispetto quello del soggetto interessato. In caso di trattamento di dati personali sensibili, i principi da rispettare sono differenti. Il titolare del trattamento deve comunicare al soggetto interessato il tipo di trattamento realizzato, i motivi e i destinatari dei dati personali, la possibilità di esercitare il diritto d'accesso e di rettifica dei dati, oltre a quello di opporsi nel caso in cui i dati siano trattati per motivi di marketing.

TRASFERIMENTO DEI DATI	Il trasferimento di dati personali a paesi non UE è consentito solo se il paese è in gradi di offrire una "protezione adeguata". Per il trasferimento di dati agli USA, le compagnie che aderiscono ai principi del US/ EU Safe Harbor sono considerate come compagnie che garantiscono una protezione adeguata. I titolari possono trasferire dati personali fuori dall'UE a paesi che non offrono protezione adeguata nel caso in cui: - l'interessato abbia dato il proprio consenso; - il trasferimento sia necessario per l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; - il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto con una parte terza nell'interesse dell'interessato; - il trasferimento sia necessario per proteggere gli interessi vitali dell'interessato; - il trasferimento sia necessario in sede legale;

	- il trasferimento sia necessario o legalmente richiesto per proteggere un importante interesse pubblico; - un ente di diritto richieda dati contenuti in un registro pubblico. Se le condizioni sopra elencate non sono soddisfatte, l'Autorità nazionale per la protezione dei dati può autorizzare ugualmente il trasferimento solo se il titolare del trattamento presenta ulteriori tutele per la protezione dei diritti dell'interessato.
SICUREZZA	I titolari e i responsabili del trattamento devono implementare misure tecniche e organizzative appropriate per proteggere i dati personali contro la distruzione, la perdita, l'alterazione, l'accesso di tipo non autorizzato e accidentali.
NOTIFICA DI VIOLAZIONE	La legge non prevede un dovere di notifica in caso di violazione della sicurezza dei dati.
APPLICAZIONE	In caso di ricorsi, l'autorità nazionale per la protezione dei dati è autorizzata ad investigare e ad agire come mediatore. L'Autorità può anche nominare degli esperti. In caso di azioni criminose l'Autorità deve notificare l'autorità

	pubblica, le sanzioni possono essere sia detentive, che pecuniarie fino a 550.000 €.

BULGARIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita con il Data Protection Act, Gazzetta Statale N. 1 del 4 gennaio 2002. Ultima modifica: Gazzetta statale, N. 81 del 18 ottobre 2011.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione relativa ad un individuo identificato o identificabile direttamente o indirettamente attraverso un documento di identità o uno o più segni specifici.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Sono dati che rivelano: a) l'origine etnica o razziale; b) il credo politico, religioso, filosofico, la partecipazione politica ad organizzazioni e associazioni religiose, filosofiche, politiche o sindacali; c) lo stato di salute, la vita sessuale o il genoma umano.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Commissione per la protezione dei dati personali. Комисия за защита на личните данни
NOTIFICAZIONE DEL TRATTAMENTO	L'Autorità nazionale per la protezione dei dati supporta i seguenti registri pubblici: - registro dei titolari;

	- registro dei titolari esenti da notificazione del trattamento; - registro dei titolari a cui è stata rifiutata la notificazione del trattamento. La notifica preventiva deve specificare le seguenti informazioni standard: - dati di identificazione del titolare; - la sede del titolare; - se il titolare tratta i dati con scopi di difesa, sicurezza nazionale, ordine pubblico o procedimenti criminali; - la principale attività del titolare del trattamento; - se i dati sono trattati dal titolare del trattamento o da incaricati; - il numero di registri di dati. Nel modulo per la notifica occorre indicare: - il nome e l'indirizzo del registro; - il motivo del trattamento; - la base legale per il trattamento dei dati; - se vi è o meno un'elaborazione automatica dei dati;

	- le categorie dei soggetti dei dati; - le categorie dei dati personali trattati, inclusi i dati sensibili; - i destinatari o le categorie di destinatari; - un'eventuale richiesta di trasferimento a paesi stranieri ed eventualmente quali paesi; - le fonti per la raccolta dei dati; - se vi è un consenso esplicito da parte dei soggetti; - le descrizioni delle misure tecniche e organizzative per la protezione dei dati in accordo con la regolazione prevista dal DPA. Sono previste delle eccezioni nei seguenti casi: - i titolari del trattamento operano in un registro pubblico sulla base di legge che è pubblicamente accessibile o accessibile a coloro che hanno un interesse legale; - organizzazioni no-profit che svolgono trattamenti a scopi di censimento; - i titolari del trattamento sono esplicitamente esentati dalla notificazione del trattamento all'autorità nazionale qualora il

	trattamento non danneggia i diritti e gli interessi legali dei titolari dei dati. Le regole e le condizioni di questa specifica eccezione sono specificate in un regolamento speciale dell'autorità nazionale. I titolari del trattamento devono, in questi casi, rivolgersi alla autorità nazionale per ottenere da quest'ultima la decisione che li solleva dall'obbligo di notifica. L'autorità nazionale può in ogni caso svolgere il controllo previsto dalla legge.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Ad oggi non vi è l'obbligo di nominare all'interno delle organizzazioni il DPO, anche se è raccomandato dall'Autorità nazionale.
RACCOLTA E TRATTAMENTO DEI DATI	Qualsiasi dato personale deve essere trattato in modo in accordo ai seguenti principi: - il trattamento deve essere corretto e legale; - il trattamento deve essere basato solo su motivi specifici e legali e deve essere fatto solo per i motivi dichiarati al momento della raccolta dei dati stessi; - sia adeguato, rilevante e non ecceda i motivi dichiarati; - sia accurato, completo e aggiornato laddove necessario;

	- non sia più lungo del necessario; - rispetti i diritti dell'interessato previsti dalla legge; - sia conservato con sicurezza; - non sia trasferito a paesi che non hanno adeguate leggi di protezione dei dati a meno che non ci sia una protezione specifica adeguata. Oltre ai principi generali sopra elencati, nel trattare i dati personali i titolari del trattamento devono rispettare almeno anche una delle seguenti condizioni: - il trattamento venga svolto nel rispetto degli obblighi di legge a carico del titolare; - l'interessato abbia fornito il proprio consenso esplicito; - il trattamento sia necessario per il rispetto di un contratto di cui l'interessato è parte; - il trattamento sia necessario affinché il titolare del trattamento porti avanti i propri doveri secondo legge o con lo scopo di interesse pubblico; - il trattamento sia necessario per la tutela di interessi legittimi perseguiti dal titolare del trat-

	tamento o dai destinatari, posto che siano protetti i diritti dell'interessato. In caso di dati "sensibili", vi sono condizioni specifiche per il trattamento. Se almeno una delle condizioni sopra elencate è rispettata, il titolare del trattamento deve innanzitutto fornire le seguenti informazioni all'interessato: - l'identificazione del titolare del trattamento e del suo rappresentante; - gli scopi per cui i dati verranno trattati; - i destinatari o le categorie di destinatari alle quali i dati potranno essere comunicati; - se i dati sono comunicati per adempiere ad un obbligo o volontario; - le categorie di dati personali; - informazioni riguardo al diritto di accesso e di rettifica dei dati raccolti. L'obbligo di notifica preventiva non è applicabile qualora i responsabili di trattamento non raccolgano dati direttamente dagli interessati e sia rispettata

	una delle seguenti condizioni: - il trattamento è fatto a fini statistici o per scopi di ricerca storica o scientifica e la comunicazione dei dati è impossibile o richiederebbe uno sforzo sproporzionato; - la registrazione e la divulgazione dei dati sono esplicitamente previste dalla legge; - il soggetto a cui tali dati si riferiscono ha già le informazioni richieste.
TRASFERIMENTO DEI DATI	-Il trasferimento di dati personali all'interno dell'UE è libero, nel rispetto della legge nazionale di protezione dei dati . Il trasferimento dei dati personali al di fuori dello spazio UE-EEA è permesso solo a condizione che lo stato ricevente possa assicurare un adeguato livello di protezione dei dati. Questa verifica è fatta dall'autorità nazionale, salvo i casi in cui la Commissione Europea con propria decisione ha già stabilito l'adeguato livello di protezione di un paese.
SICUREZZA	titolari del trattamento devono implementare le adeguate misure tecniche e organizzative per proteggere i dati personali contro la perdita o la distruzio-

	ne accidentale o intenzionale dei dati, contro l'apertura o l'accesso non autorizzati, contro la distribuzione o la modifica dei dati. I titolari del trattamento devono implementare misure speciali di protezione nei casi di trasferimento elettronico dei dati. Il livello minimo di queste misure è specificato dall'Autorità nazionale.
NOTIFICA DI VIOLAZIONE	La legge non dispone alcun obbligo di notifica per la violazione della sicurezza dei dati.
APPLICAZIONE	L'Autorità nazionale per la protezione dei dati è responsabile dell'applicazione della legge e può, su richiesta dell'interessato o d'ufficio, avviare un'indagine; fornire istruzioni o ordini; prevedere un termine obbligatorio per la rettifica della violazione; proibire temporaneamente qualsiasi trattamento illegale dei dati dopo una notifica preliminare; imporre sanzioni amministrative. Le sanzioni pecuniarie possono andare approssimativamente dai 5.000 ai 50.000€. I titolari del trattamento sono responsabili di qualsiasi danno causato al soggetto per trattamento illegale.

	Contro le decisioni dell'autorità nazionale si può ricorrere di fronte alla Corte amministrativa suprema bulgara entro 14 giorni dalla comunicazione, l'interessato può inoltre ricorrere contro il titolare del trattamento in caso di violazione dei suoi diritti di fronte alla Corte amministrativa suprema. Il trasferimento o la distribuzione di password di sistema per la diffusione di dati costituiscono un crimine secondo il Codice Penale bulgaro e la pena per questi crimini può comportare la reclusione fino a 3 anni.

CIPRO

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita nel novembre 2001 con la Legge sul trattamento dei dati personali n. 37(I)/2003 e successive modifiche.
DEFINIZIONE DI DATI PERSONALI	Qualunque informazione relativa ad un soggetto vivente; i dati consolidati di natura statistica, dai quali non si può identificare un soggetto, non sono dati personali.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati concernenti origine razziale o etnica, convinzioni politiche, credo religioso o filosofico, partecipazione ad un ente, associazione o sindacato, salute, vita sessuale, orientamento sessuale, dati giudiziari.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Office of the Commissioner for Personal Data Protection ("Commissioner")
NOTIFICAZIONE DEL TRATTAMENTO	I titolare o i responsabili del trattamento devono notificare all'Autorità nazionale l'operazione di trattamento dei dati. L'informazione fornita sarà poi inserita nell'apposito Registro. La notifica deve includere le seguenti informazioni: - nome completo e indirizzo del titolare del trattamento dei dati;

	- indirizzo dove il sistema di archiviazione è stabilito; - una descrizione dello scopo del trattamento dei dati; - le categorie dei soggetti dei dati; - le categorie di dati che si vogliono trattare; - il periodo di tempo durante il quale i dati verranno trattati o archiviati; - i destinatari a cui verranno comunicati i dati: - le trasmissioni di dati a paesi terzi e il relativo scopo; - le caratteristiche base del sistema e le misure per la sicurezza del sistema di archiviazione o del trattamento.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	La legge obbliga le organizzazioni che trattano dati personali a designare, comunicandolo all'Autorità, il DPO che è, in ultima istanza, il responsabile del trattamento dei dati.
RACCOLTA E TRATTAMENTO DEI DATI	I titolari del trattamento possono trattare dati personali qualora sia rispettata una delle seguenti condizioni: - vi sia il consenso dell' interessato;

	- il titolare del trattamento abbia bisogno di trattare i dati per sottoscrivere o adempiere ad un contratto di cui l'interessato è parte; - il trattamento sia necessario affinché il titolare rispetti le normative previste; - il trattamento protegga gli interessi vitali del titolare; - il trattamento sia necessario per un interesse pubblico o nell'esercizio di un'autorità pubblica; - il trattamento sia necessario per la salvaguardia di interessi legittimi da parte del titolare del trattamento, o di terzi a cui sono comunicati i dati personali, a condizione che tali interessi siano di rango superiore rispetto ai diritti, agli interessi e alle libertà fondamentali dell'interessato.
TRASFERIMENTO DEI DATI	I titolari dei trattamenti possono trasferire dati personali fuori dall'Unione Europea solo dopo avere ottenuto dall'Autorità un'autorizzazione specifica che viene rilasciata solo se il paese destinatario assicura un adeguato livello di protezione.

	La trasmissione di dati personali ad un paese che non assicura un adeguato livello di protezione è autorizzata in via eccezionale nel rispetto di almeno una delle seguenti condizioni: - l'interessato dà il suo consenso ; - la trasmissione è necessaria per proteggere gli interessi vitali dell'interessato; - la trasmissione è necessaria per la conclusione e l'esecuzione di un contratto in cui l'interessato è parte; - la trasmissione è necessaria per l'esecuzione di misure precontrattuali adottate in seguito a una richiesta dell'interessato; - la trasmissione è necessaria per la salvaguardia di un interesse pubblico superiore; - la trasmissione è necessaria per la definizione, l'esercizio o la difesa di controversie legali di fronte ad una corte; - la trasmissione è fatta partendo da un registro pubblico che, in base alle disposizioni legislative, fornisce informazioni pubbliche o a qualsiasi persona che possa dimostrare un interesse legittimo.

SICUREZZA	Il trattamento dei dati è confidenziale e deve essere eseguito esclusivamente da incaricati che agiscono sotto l'autorità del titolare o del responsabile del trattamento. I titolari del trattamento devono adottare misure tecniche e organizzative appropriate per la sicurezza dei dati, la loro protezione contro la distruzione accidentale o illegale, la perdita accidentale, l'alterazione, la disseminazione o l'accesso non autorizzati e qualsiasi altra forma di trattamento illegale. Queste misure devono assicurare un livello di sicurezza appropriato al livello di rischio del trattamento stesso. L'autorità dà delle direttive rispetto al livello di sicurezza dei dati e alle misure di protezione che devono essere adottate per qualsiasi categoria di dati, in relazione anche allo sviluppo tecnologico. Se il trattamento è fatto da un elaboratore automatico di dati, l'attribuzione del trattamento deve essere fatta per iscritto. L'attribuzione deve garantire che l'elaboratore tratti i dati solo seguendo le istruzioni date dal titolare del trattamento.

NOTIFICA DI VIOLAZIONE	Non vi è l'obbligo di notificare eventuali violazioni.
APPLICAZIONE	L'applicazione della legge dipende dall'Autorità nazionale che può imporre le seguenti sanzioni amministrative al titolare o al responsabile del trattamento o ai loro rispettivi rappresentanti: - una multa fino a 8543€; - una revoca temporanea della licenza; - una revoca permanente della licenza; - un avviso con un limite temporale specifico per porre fine alla contravvenzione; - la distruzione del sistema di archiviazione o la cessazione del trattamento dei dati e la loro distruzione. La sezione 26(1) della legge prevede un elenco di violazioni per cui sono previste le seguenti pene: - reclusione per un tempo non superiore ai 3 anni o una multa di circa 5130 €, oppure reclusione per un tempo non superiore ai 5 anni o una multa di circa 8453 €, in base ai seguenti fattori:

	- il reato è stato causato per negligenza, oppure - la persona che ha commesso il reato intendeva ottenere un beneficio finanziario illegale per se stesso o per qualcun altro o causare un danno a una parte terza, oppure - il reato commesso ha messo in pericolo il Governo della Repubblica o la sicurezza nazionale. I reati commessi contravvenendo alle disposizioni della sezione 26(1), per i quali non sono espressamente previste pene, sono punibili con la reclusione per un periodo non superiore a 1 anno e/o con una multa non superiore ai 3417,20 €.

REPUBBLICA CECA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita con Atto n. 101/2000 Coll.
DEFINIZIONE DI DATI PERSONALI	Qualunque informazione relativa a un soggetto identificato o identificabile, attraverso un numero, un codice o uno o più fattori relativi alla sua identità fisica, psicologica, fisiologica, psichica, economica, culturale o sociale.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati che rivelano la nazionalità, l'origine etnica o razziale, le attitudini politiche, l'appartenenza a un sindacato, il credo religioso o filosofico, lo stato di salute, la vita sessuale, dati biometrici o genetici dell'interessato.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	The Office for Personal Data Protection ("Office")
NOTIFICAZIONE DEL TRATTAMENTO	Chiunque in qualità di responsabile del trattamento intenda trattare dati personali, o modificare un trattamento già esistente, è obbligato a notificarlo per iscritto all'Autorità nazionale prima di cominciare il trattamento dei dati. La notifica deve includere almeno le seguenti informazioni:

	- dettagli per l'identificazione del titolare del trattamento dei dati; - scopo del trattamento; - categorie dei soggetti e dei dati personali; - fonti dei dati; - descrizione del modo in cui verranno trattati i dati; - luogo del trattamento dei dati; - destinatario o categoria di destinatari dei dati; - intenzione di trasferire i dati ad altri paesi; - descrizione delle misure adottate per assicurare la protezione dei dati personali.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Non vi è l'obbligo di nominare all'interno delle organizzazioni il DPO.
RACCOLTA E TRATTAMENTO DEI DATI	Il consenso inequivocabile (e revocabile) dell'interessato è richiesto per il trattamento dei dati. Il consenso scritto non è richiesto; anche se è meglio ottenerlo, poiché il titolare del trattamento deve essere in grado di dimostrare tale consenso durante tutto il trattamento dei dati.

	L'interessato deve essere informato in modo chiaro su tutti gli aspetti del trattamento. I dati personali possono essere trattati solo se in misura adeguata e non eccessiva rispetto agli scopi specifici per i quali i dati sono stati raccolti. I dati personali devono essere mantenuti in modo accurato. Il titolare del trattamento non può fornire i dati personali a parti terze senza il consenso dell'interessato, eccetto laddove previsto dalla legge. I dati personali possono essere cancellati una volta cessato il motivo per cui sono stati raccolti. Comunque, ci possono essere delle eccezioni previste dalla legge (es. Legge di archiviazione). I dati personali devono essere archiviati in un formato che permetta al soggetto di esercitare il proprio diritto di accedere, rettificare, cancellare e opporsi. Sono previste delle regole di protezione speciali in caso di trattamento di dati sensibili. Inoltre, dall'1 gennaio 2006 sono state introdotte particolari regole per il trattamento delle nascite: un numero di 10 ci-

	fre contiene informazioni riguardo la data di nascita e il sesso dei cittadini cechi.
TRASFERIMENTO DEI DATI	E' prevista per legge la libera circolazione dei dati personali tra stati membri della UE. Verso gli altri paesi, la legge distingue diversi gruppi. 1. Primo gruppo: La libera circolazione dei dati personali è ammessa, a meno che non vi siano limiti posti da un trattato internazionale firmato dai paesi coinvolti e ratificato dal Parlamento Ceco. 2. Secondo gruppo: il trasferimento dei dati personali è possibile sulla base di una decisione di un'istituzione dell'UE. Ci sono anche decisioni europee che prevedono che i dati personali possono essere trasferiti senza un'approvazione ufficiale a patto che il contratto includa determinate clausole contrattuali standard individuate dalla decisione stessa. Nessuno dei metodi di trasferimento sopra elencati è soggetto ad un'approvazione ufficiale. In tutti gli altri casi, i titolari del trattamento devono ottenere un permesso preventivo da parte dell'Autorità nazionale.

	A questo scopo il titolare deve provare che: - il trasferimento dei dati è portato avanti con il consenso dell'interessato; - in un paese terzo, dove sono trattati i dati, ci sono delle garanzie specifiche sufficienti; - i dati personali riguardano una parte di dati accessibili al pubblico sulla base di una legge che preveda la possibilità di accesso ai dati se si ha un interesse legale specifico: - il trasferimento è necessario per negoziare la conclusione o la modifica di un contratto portato avanti dal soggetto dei dati; - il trasferimento è necessario per adempiere ad un contratto tra il titolare del trattamento e una parte terza, concluso nell'interesse dell'interessato o per esercitare altri reclami legali; - il trasferimento è necessario per la protezione dei diritti o di importanti interessi vitali dell'interessato (in particolare per salvare vite o fornire aiuto medico).

SICUREZZA	I responsabili e gli incaricati del trattamento sono obbligati ad adottare le misure necessarie per prevenire l'accesso accidentale o non autorizzato ai dati, la loro alterazione, distruzione o perdita o la trasmissione non autorizzata. Sono anche obbligati a sviluppare e documentare le misure tecnico-organizzative adottate e implementate al fine di assicurare la protezione dei dati personali come previsto dalla legge.
NOTIFICA DI VIOLAZIONE	Non vi sono obblighi legislativi che prevedono la notifica all'Ufficio o all'interessato in caso di violazioni o perdite di dati.
APPLICAZIONE	Il titolare e il responsabile del trattamento sono i soggetti perseguibili in caso di violazione della legge. L'Autorità nazionale può imporre misure restrittive o sanzioni pecuniarie fino a 175000 €. In alcuni casi, ad esempio se sono violate le regole per il trattamento dei dati sensibili, le multe possono arrivare fino a 350000 €.

CROAZIA

LEGGE	La protezione dei dati personali è un diritto riconosciuto dalla Costituzione della Repubblica Croata (art. 37). La Legge per la Protezione dei dati personali è la n. 103/03 e successive modifiche, armonizzata rispetto alla direttiva UE 95/46/EC.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione relativa a una persona identificata o identificabile. Un soggetto identificabile è colui che può essere identificato direttamente o indirettamente attraverso un numero di identificazione personale o attraverso uno o più dati fisici, fisiologici, mentali, economici, culturali o sociali.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	La legge 103/03 non dà un definizione diretta di dati personali sensibili, ma al Titolo III – art. 8 parla di categorie speciali dati personali, includendo tra questi: l'origine etnica o razziale, opinioni politiche, convinzioni religiose o di altro tipo, appartenenza ad associazioni sindacali, lo stato di salute, la vita sessuale, i procedimenti penali.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Agencija za zaštitu osobnih podataka - Croatian Personal Data Protection Agency (istituita con la legge 103/03)

NOTIFICAZIONE DEL TRATTAMENTO	Prima di iniziare qualsiasi trattamento, i titolari devono provvedere ad inviare all'Agenzia di Protezione dei dati personali la notificazione (ad eccezione di quelli previsti dalla legge) per il suo inserimento nel Registro Centrale. Il Registro è conservato presso l'Agenzia, è pubblico e contiene informazioni sui trattamenti in corso.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO- Data Protection Officer)	Tra le figure che si occupano di protezione dei dati, la normativa croata prevede anche quella del DPO.
RACCOLTA E TRATTAMENTO DEI DATI	I dati personali possono essere raccolti ed elaborati esclusivamente; – con il consenso dell'interessato e solo per lo scopo per il quale l'interessato ha dato il suo consenso, oppure – nei casi stabiliti dalla legge, oppure – al fine di adempiere gli obblighi derivanti dalla legge da parte del responsabile della raccolta dei dati personali, oppure – al fine di stipulare e attuare contratti nei quali l'interessato è una delle parti, oppure – al fine di tutelare la vita o l'integrità corporea dell'interessato

	o di un'altra persona nel caso in cui l'interessato sia fisicamente o giuridicamente impossibilitato a dare il suo consenso, oppure – quando il trattamento dei dati è indispensabile per adempiere i compiti che sono realizzati per il pubblico interesse o nell'attuazione dei poteri pubblici che ha il responsabile della raccolta dei dati personali o di una terza parte alla quale i dati sono presentati, oppure – quando il trattamento dei dati è indispensabile al fine di adempiere gli interessi legittimi del responsabile dei dati personali o di una terza parte alla quale sono comunicati i dati, tranne quando prevalgano gli interessi per la tutela dei diritti e delle libertà fondamentali degli interessati, oppure – qualora lo stesso interessato abbia pubblicato questi dati. L'interessato ha il diritto di rinunciare in qualsiasi momento al consenso dato e richiedere la cessazione del trattamento dei suoi dati, ad eccezione dei casi in cui si tratta di elaborazioni di dati a scopo statistico a seguito delle quali i dati personali non permettono più di identificare la persona alla quale si riferiscono.

	I dati personali che riguardano i minori possono essere raccolti ed elaborati in conformità alla Legge e osservando misure di tutela più stringenti, prescritte da leggi particolari. Per quanto riguarda i dati sensibili la legge prescrive che è vietato raccogliere e trattare ulteriormente i dati personali che riguardano la provenienza razziale o etnica, la posizione politica, la convinzione religiosa o altra convinzione, l'appartenenza a sindacati, la salute o la vita sessuale e i dati personali sul procedimento penale e relativo alle infrazioni. In via eccezionale, tali dati possono venir raccolti e trattati nei seguenti casi: – con il consenso dell'interessato, oppure – quando il trattamento dei dati è necessario al fine di adempiere i diritti e gli obblighi del responsabile della raccolta dei dati personali in conformità a normative speciali, oppure – quando il trattamento è indispensabile al fine di tutelare la vita o l'integrità fisica dell'interessato o di un'altra persona nel caso in cui l'interessato sia fisicamente o giuridicamente impossibilitato a dare il suo consenso, oppure

	– nel caso in cui il trattamento si svolge nell'ambito dell'attività dell'istituzione, dell'associazione o di qualsiasi altro organo no profit con fine politico, filosofico, religioso, sindacale o altro e a condizione che il trattamento riguardi esclusivamente i loro membri e che i dati non siano svelati a una terza parte senza il consenso dell'interessato, oppure – quando il trattamento dei dati è necessario al fine di stabilire, realizzare o tutelare le pendenze prescritte dalla legge, oppure – qualora lo stesso interessato abbia pubblicato questi dati, oppure – quando il trattamento dei dati è necessario ai fini della medicina preventiva, della diagnosi, dell'assistenza sanitaria o della gestione dei servizi sanitari, a condizione che i dati siano elaborati da un operatore sanitario in base alle regole e ai regola golamenti emessi dalle autorità competenti. In questi casi il trattamento dei dati deve essere particolarmente tutelato e anche le forme di conservazione e protezione tecnica saranno disciplinate da norme speciali che regolano il settore della sicurezza informativa.

	Per quanto riguarda i dati personali relativi reati e precedenti penali, questi devono essere trattati esclusivamente sotto il controllo delle autorità competenti.
TRASFERIMENTO DEI DATI	Il trasferimento dei dati per ulteriori trattamenti è previsto solo verso quei paesi o organizzazioni che garantiscono un adeguato livello di protezione. Tra i vari compiti che la normativa assegna all'Agenzia per la protezione dei dati personali, vi è anche quello di compilare un elenco di stati e organizzazioni internazionali che garantiscono tale adeguatezza.
SICUREZZA	I dati personali sono conservati all'interno di database e devono essere adeguatamente protetti per evitare accessi non consentiti, distruzione, perdita, alterazione, anche accidentale. I titolari del trattamento e gli incaricati devono adottare le misure tecniche e organizzative più idonee a proteggere i dati per evitare perdita e/o distruzione, anche accidentale, accessi, alterazioni o disseminazioni non autorizzate e tutte le altre forme di abuso. Sono inoltre tenuti a rispettare l'obbligo della riservatezza.

	Per quanto riguarda il trattamento di dati sensibili, il Governo ha emesso un regolamento (n. 139/04 "Regolamento sulle procedure per la conservazione e le misure speciali per la protezione delle categorie speciali di dati") che specifica come tali dati devono essere conservati e con quali misure di protezione.I database devono essere consegnati all'Agenzia per la protezione dei dati personali per il loro inserimento nel Registro Centrale. I dati che vengono trattati da autorità statali autorizzate per fini legati alla sicurezza, difesa e prevenzione del crimine non devono essere inseriti nel Registro.
NOTIFICA DI VIOLAZIONE	L'interessato ha il diritto di: - presentare un reclamo presso l'Agenzia per la protezione dei dati personali qualora i propri dati siano stati trattati in modo improprio; - presentare una richiesta di indennizzo qualora ritenga che i propri diritti siano stati violati. Nel caso in cui l'Agenzia accerti tale violazione, che può consistere nell'uso non autorizzato dei dati o nella loro divulgazione a terzi, è il titolare del trattamento che è ritenuto responsabile e deve provvedere al risarcimento danni di fronte al Tribunale.

APPLICAZIONE	L'Autorità nazionale per la protezione dei dati personali è indipendente e responsabile di fronte al Parlamento. Ha numerose funzioni, tra cui: - controlla che i trattamenti siano effettuati nel rispetto della legge; - indica le violazioni accertate durante la raccolta dei dati personali; - compila la lista dei paesi e organizzazioni internazionali che garantiscono una adeguata protezione dei dati; - esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati; - conserva il Registro centrale. Se l'Agenzia accerta l'esistenza di una violazione nell'applicazione della legge, notifica al titolare del trattamento le irregolarità riscontrate ed emette una decisione con la quale può disporre: - l'eliminazione di tali irregolarità entro una certa data; - la sospensione della raccolta, del trattamento e dell'uso dei dati personali oggetto della violazione; - la cancellazione dei dati; - il divieto del trasferimento dei dati all'estero. Contro tale decisione non può essere presentato appello, tuttavia si può avviare un contenzioso amministrativo. L'Agenzia può inoltre decidere di adire le vie giudiziarie.

DANIMARCA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita nel giugno 2000.
DEFINIZIONE DI DATI PERSONALI	Qualunque informazione relativa a una persona identificata o identificabile.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Sono dati relativi all'origine etnica o razziale, opinioni politiche, credo religioso o filosofico, appartenenza sindacale, salute, vita sessuale.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Datatilsynet
NOTIFICAZIONE DEL TRATTAMENTO	A differenza della maggior parte dei paesi UE, in Danimarca non è prevista la notificazione relativa ai trattamenti dei dati, ai titolari o ai database contenenti dati personali. Tuttavia, i responsabili che svolgono trattamenti con sistemi elettronici devono inviare notifica all'Autorità prima dell'inizio dell'attività stessa. Inoltre, qualora il trattamento includa dati sensibili, il titolare ha l'obbligo di notificare l'Autorità inviando le seguenti informazioni: - nome e indirizzo del titolare del trattamento ed eventualmente del suo rappresentante e addetto;

	- la categoria del trattamento e il suo scopo; - una descrizione generale del trattamento; - una descrizione delle categorie dei soggetti dei dati e delle rispettive categorie di dati; - i destinatari o le categorie di destinatari dei dati: - l'intenzione di trasferire i dati a paesi terzi; - una descrizione generale delle misure prese per garantire la sicurezza del trattamento; - la data di inizio del trattamento; - la data di cancellazione dei dati.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Le organizzazioni non hanno l'obbligo di nominare il DPO.
RACCOLTA E TRATTAMENTO DEI DATI	Il trattamento è possibile quando: - l'interessato ha fornito consenso esplicito; - è necessario all'esecuzione di un contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta dell'interessato;

	- è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento; - è necessario per proteggere gli interessi vitali della persona interessata; - è necessario per l'esecuzione di un compito di interesse pubblico; - è necessario per l'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o una terza parte a cui vengono comunicati i dati; - è necessario per il perseguimento dell'interesse legittimo del titolare del trattamento, o dei terzi a cui vengono comunicati i dati, a condizione che tale interesse non prevalga su quelli della persona interessata. Per quanto riguarda l'uso dei dati personali a fini commerciali, una ditta può trattare dati relativi ai propri clienti per attività di marketing solo nel caso in cui tale trattamento venga effettuato per perseguire gli interessi legittimi della ditta e questi interessi siano di rango inferiore rispetto agli interessi del consumatori. In tutti gli altri casi, per

	il trattamento dei dati personali a fini commerciali occorre il consenso. I dati personali sensibili possono essere trattati solo se: - il soggetto dei dati ha dato consenso esplicito al trattamento di tali dati; - il trattamento è necessario per proteggere gli interessi vitali dell'interessato dei dati o di un'altra persona se quest'ultima è fisicamente o legalmente incapace di fornire il proprio consenso; - il trattamento si riferisce a dati che sono stati resi pubblici dal soggetto; - il trattamento è necessario per costatare, esercitare, difendere un diritto per via giudiziaria. I dati personali riguardanti affari puramente privati, inclusi quelli relativi ai reati penali e a gravi problemi sociali, possono essere trattati solo se: - il soggetto dei dati ha dato consenso esplicito; - la comunicazione dei dati è necessaria per perseguire interessi pubblici o privati di rango chia-

	ramente superiore rispetto agli interessi della segretezza; - la comunicazione è necessaria per l'esercizio dell'attività di un'autorità o per la formulazione di una decisione da parte dell'autorità stessa; - la comunicazione è necessaria per l'assoluzione di un obbligo da parte una personal o una ditta nei confronti dell'autorità pubblica. Inoltre, il titolare del trattamento dei dati deve fornire all'interessato le informazioni necessarie, tra cui l'identità del titolare, gli scopi del trattamento e qualsiasi altra informazione necessaria riguardante le circostanze specifiche in cui sono stati raccolti i dati.
TRASFERIMENTO DEI DATI	Il trasferimento dei dati personali fuori dall'unione europea è possibile se: - l'interessato ha dato il proprio consenso esplicito; - è necessario per l'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento o per l'esecuzione di misure pre-contrattuali adottate su richiesta dell'interessato; - è necessario per la conclusione

	o l'esecuzione di un contratto concluso nell'interesse del soggetto tra il titolare del trattamento e una parte terza; - è necessario o prescritto dalla legge per la salvaguardia di interesse pubblico rilevante o per costatare, esercitare o difendere un diritto per via giudiziaria; - è necessario per proteggere gli interessi vitali del soggetto interessato; - è fatto partendo da un registro pubblico; - è necessario per la prevenzione, investigazione e persecuzione di reati penali e l'esecuzione di sentenze o la protezione di persone coinvolte in procedimenti penali; - è necessario per la salvaguardia della pubblica sicurezza o della sicurezza nazionale. Per quanto riguarda gli Stati Uniti, è stato istituito un programma speciale - il Safe Harbor Programme – e le compagnie che vi aderiscono sono considerate ditte con sede in paesi terzi che garantiscono un adeguato livello di protezione. Inoltre, l'Autorità nazionale per la protezione dei dati può auto-

	rizzare un trasferimento di dati personali a un altro paese terzo qualora il titolare del trattamento ritenga sia garantito un adeguato livello di protezione.
SICUREZZA	I titolari del trattamento devono implementare misure tecniche e organizzative appropriate per proteggere i dati contro la distruzione, la perdita o l'alterazione accidentale o illegale e contro la visione non autorizzata, l'abuso o altre violazioni.
NOTIFICA DI VIOLAZIONE	Non è previsto l'obbligo di notifica in caso di violazione, anche se è ritenuta una buona pratica.
APPLICAZIONE	L'Autorità nazionale per la protezione dei dati, composta da un Consiglio e da una Segreteria, è responsabile della supervisione delle operazioni di trattamento previste dalla legge e i suoi pareri hanno valore legale. Inoltre, l'Autorità può imporre sanzioni pecuniarie o detentive fino a 4 mesi a chi non rispetta la legge.

ESTONIA

LEGGE	Il Parlamento estone (Riigikogu), ha approvato nel giugno del 1996 il Decreto sulla Protezione dei Dati Personali (Personal Data Protection Act o PDPA), che è stato modificato il 12 febbraio 2003 per recepire la direttiva UE 95/46/EC ed è entrato in vigore il 1 ottobre 2003. Il 14 aprile 2004 è stato ulteriormente modificato e la vigente normativa è entrata in vigore il 1 maggio 2004.
DEFINIZIONE DI DATI PERSONALI	Qualunque informazione relativa a una persona identificata o identificabile in base alle sue caratteristiche fisiche, mentali, psicologiche, economiche, culturali o sociali.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati che rivelano le opinioni politiche o le convinzioni religiose o filosofiche, l'origine etnica o razziale, lo stato di salute, le informazioni genetiche, la vita sessuale, l'appartenenza sindacale, i procedimenti penali.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	*Estonian Data Protection Inspectorate*
NOTIFICAZIONE DEL TRATTAMENTO	Non è previsto un obbligo di notificazione del trattamento per dati trattati conformemente alla legge. I titolari del tratta-

	mento devono invece notificare il trattamento dei dati sensibili presso l'autorità nazionale.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Non vi è l'obbligo di nominare all'interno delle organizzazioni il DPO
RACCOLTA E TRATTAMENTO DEI DATI	Il trattamento dei dati personali può avvenire solo con il permesso della persona interessata oppure se: - è necessario per portare a termine un contratto di cui l'interessato è parte, - è necessario per proteggere la vita, la salute o la libertà del soggetto o di un'altra persona, - è necessario per portare a termine un obbligo prescritto dalla legge. Ci sono requisiti separati per il trattamento dei dati personali sensibili e del numero di identità.
TRASFERIMENTO DEI DATI	Il trasferimento al di fuori dell'Unione è possibile se: - l'interessato ha dato il proprio consenso esplicito; - è necessario per la conclusione di un contratto di cui il soggetto è parte; -è necessario per l'esecuzione di un accordo tra il titolare del

	trattamento e una parte terza nell'interesse del soggetto a cui i dati si riferiscono; - è necessario per proteggere gli interessi vitali del soggetto interessato; - è necessario o previsto dalla legge per proteggere un importante interesse pubblico; - è fatto partendo da una banca dati che può essere consultata liberamente o per motivi specifici come previsto dalla legge; - il titolare del trattamento dà adeguate garanzie di protezione sulla privacy e i diritti degli individui; - è fatto sulla base di clausole contrattuali standard adottate dalla Commissione Europea. Il trasferimento dei dati a paesi non UE/EEA è permesso se i paesi garantiscono un adeguato livello di protezione dei dati, così come previsto dalla Commissione Europea, o se il livello di protezione dei dati è sufficientemente garantito dal titolare del trattamento dei dati.

SICUREZZA	In base a quanto offerto dalla tecnologia, I titolari e i responsabili del trattamento devono implementare le tecniche e le misure appropriate, per proteggere i dati personali contro la distruzione o la perdita, sia intenzionale che accidentale, e contro l'apertura e l'accesso non autorizzati.
NOTIFICA DI VIOLAZIONE	L'atto non prevede un obbligo di notifica in caso di violazione della sicurezza dei dati.
APPLICAZIONE	Spetta all'Autorità nazionale che può agire di propria iniziativa o sulla base di un ricorso. Per le persone giuridiche sono previste multe fino a 3200 € oltre la reclusione.

FINLANDIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita nel giugno 1999 con l'Atto per i Dati Personali n. 523/1999.
DEFINIZIONE DI DATI PERSONALI	Qualunque informazione relativa ad un individuo, comprese le informazione sulle sue caratteristiche personali o le circostanze personali da cui è possibile risalire alla sua identità.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati personali relativi a origini etniche o razziali, affiliazione sociale, politica o religiosa o appartenenza a un sindacato; atti criminali e sanzioni penali; stato di salute, malattia o handicap di una persona o il trattamento medico di una persona; preferenze e vita sessuali; necessità di assistenza sociale di una persona.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	The Data Protection Ombudsman
NOTIFICAZIONE DEL TRATTAMENTO	La legge non prevede l'obbligo di notifica del trattamento, tranne che in alcuni casi particolari, ad esempio quando il trattamento dei dati è fatto in automatico o è appaltato a terzi oppure quando i dati personali sono trasferiti fuori da UE e EEA.

	In ogni caso, i titolari del trattamento devono redigere una descrizione dell'archivio dati fornendo le seguenti informazioni: (a) nome e indirizzo del titolare del trattamento e, dove necessario, del suo rappresentante; (b) scopo del trattamento dei dati; (c) descrizione del gruppo o dei gruppi dei soggetti dei dati; (d) destinatari regolari; (e) descrizione dei principi con cui viene garantita la sicurezza dei dati.
RESPONSABILE DELLA PROTEZIONE DEI DATI DPO (Data Protection Officer)	La legge non prevede l'obbligo del DPO. Comunque all'interno dei luoghi in cui si trattano dati, deve esservi una persona di riferimento da inserire nella descrizione degli archivi di cui al punto precedente.
RACCOLTA E TRATTAMENTO DEI DATI	I titolari del trattamento possono raccogliere e trattare dati se: - l'interessato fornisce consenso esplicito; - l'interessato ha dato il suo consenso per concludere un contratto in cui egli stesso è parte o possano essere eseguite misure precontrattuali da lui richieste; - il trattamento è necessario per proteggere gli interessi vitali dell'interessato;

	- il trattamento è previsto da norme legislative o è necessario per adempiere un obbligo legale a cui è tenuto il titolare; - c'è una relazione rilevante tra l'interessato e le operazioni del titolare del trattamento, ad es. l'interessato è cliente, o membro, o lavora presso il titolare del trattamento; - i dati si riferiscono a clienti o impiegati di un gruppo di compagnie o altri gruppi economici equiparabili e i dati sono trattati all'interno di questo gruppo; - il trattamento riguarda dati disponibili sullo status, i doveri e le performance di un singolo all'interno di un ente pubblico o privato ed si rende necessario per la salvaguardia dei diritti e degli interessi del titolare del trattamento o di una parte terza che riceve i dati; - il Data Protection Board ha garantito il permesso per il trattamento dei dati in accordo con la legge. Per il trattamento dei dati personali sensibili e del numero di identità ci sono altri requisiti. Inoltre, ci sono specifici scopi (storici, scientifici o statistici) per

	cui i dati personali possono essere trattati. Gli scopi per il trattamento dei dati personali devono essere definiti in anticipo e i dati non devono essere trattati per scopi incompatibili con quelli definiti. Quando vengono raccolti i dati, il titolare del trattamento deve fornire all'interessato le informazioni relative ai dati del titolare del trattamento, gli scopi del trattamento, i destinatari dei dati e le modalità per fare rispettare i propri diritti.
TRASFERIMENTO DEI DATI	Il trasferimento dei dati fuori dall'UE e dall'EEA è possibile solo se: - il soggetto interessato ha manifestato il proprio consenso in maniera inequivocabile; - è necessario all'esecuzione di un contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona; - è necessario per eseguire o concludere un accordo tra il titolare del trattamento e una parte terza nell'interesse del soggetto interessato; -il trasferimento è necessario per proteggere gli interessi

	vitali del soggetto; - il trasferimento è necessario o richiesto per legge per proteggere un importante interesse pubblico; - il trasferimento è fatto da un archivio i cui dati possono essere comunicati sia per motivi generici sia per motivi specifici come previsto dalla legge; - il titolare del trattamento dà adeguate garanzie di protezione della privacy e dei diritti degli individui e la Commissione Europea, in base agli artt. 3 e 26(3) della Direttiva sulla protezione dei dati, ritiene che tali garanzie siano adeguate; - il trasferimento è fatto sulla base di clausole contrattuali standard adottate dalla Commissione Europea, sulla base dell'art. 26(4) della Direttiva sulla protezione dei dati. Il trasferimento dei dati a paesi non UE/EEA è permesso se i paesi di destinazione o il titolare del trattamento garantiscono un adeguato livello di protezione dei dati come prescritto dalla Commissione Europea. Per trasferimenti verso gli USA, si fa riferimento ai principi del programma US/EU Safe Harbor.

SICUREZZA	Il titolare del trattamento deve prendere tutte le misure tecniche e organizzative necessarie per assicurare i dati personali contro l'accesso non autorizzato, la distruzione accidentale o illegale, la manipolazione, la visione e il trasferimento non autorizzati.
NOTIFICA DI VIOLAZIONE	In caso di violazione o perdita di dati, la legge non prevede alcun obbligo di notifica né all'interessato né all'autorità nazionale. Tuttavia l'autorità nazionale ha la facoltà di prevedere a carico del titolare determinate azioni, tra cui anche quella di informare l'interessato di eventuali violazioni.
APPLICAZIONE	Il Data Protection Ombudsman e il Data Protection Board sono responsabili dall'applicazione della legge. In particolare: - il Data Protection Ombudsman emette direttive e linee guida per il trattamento dei dati personali, verifica la conformità del trattamento alla legge e pubblica istruzioni e regole per prevenire condotte illegali. - Il Data Protection Board può, su richiesta del Data Protection Ombudsman, (a) proibire il trattamento dei dati se contrario alla legge; (b) obbligare a rime-

	diare a una condotta illegale; (c) ordinare lo stop alle operazioni di trattamento se compromettono seriamente la protezione della privacy dell'interessato e i suoi interessi; (d) revocare un permesso di trattamento se ritiene che non vengano rispettate certe condizioni. Il mancato rispetto della legge può richiedere l'applicazione del codice penale finlandese (38/1889) e può essere punito con pene pecuniarie o la reclusione fino a 1 anno.

FRANCIA

LEGGE	La legge principale che regola la protezione dei dati in Francia è la n. 78-17 del 6 gennaio 1978 su "Computer e Libertà". La direttiva Europea sulla protezione dei dati 95/46/EC è stata recepita con la legge numero 2004-8021 del 6 agosto 2004, apportando cosi modifiche alla legge precedente. L'applicazione della legge spetta alla "Commissione Nazionale Informatica e Libertà" (CNIL).
DEFINIZIONE DI DATI PERSONALI	Qualunque informazione relativa a una persona fisica che può essere identificata, direttamente o indirettamente, riferendosi a un numero di identificazione o a uno o più fattori specifici.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati che rivelano direttamente o indirettamente le origini etniche o razziali, le opinioni politiche, filosofiche e religiose, l'affiliazione a un sindacato, la vita sessuale e la salute.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Commission Nationale de l'Informatique et des Libertés (CNIL)
NOTIFICAZIONE DEL TRATTAMENTO	Normalmente, il trattamento dei dati richiede una dichiarazione preventiva al CNIL, salvo eccezioni. La dichiarazione preventiva deve specificare:

	- gli scopi del trattamento dei dati; - l'identità e l'indirizzo del titolare del trattamento dei dati; - le possibili interconnessioni tra i diversi database; - i dati personali trattati e le categorie di persone coinvolte; - il periodo di tempo per cui verranno tenuti i dati; - il dipartimento o le persone incaricate ad implementare il trattamento dei dati; - i destinatari o le categorie di destinatari dei dati personali; - le misure prese per garantire la sicurezza del trattamento. Per alcuni trattamenti è prevista una notificazione preventiva semplificata. Il CNIL inoltre può decidere che per alcuni trattamenti non sia necessario inviare la notificazione, sulla base ad esempio dello scopo, della natura dei dati trattati o del tempo di conservazione, ecc.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	La legge non prevede l'obbligatorietà per le organizzazioni di nominare al proprio interno un DPO. Tuttavia, se un'organizzazione nomina il DPO può esse-

	re esentata dalla dichiarazione preventiva al CNIL. Il DPO deve verificare il rispetto della legge e comunicare, a chiunque lo richieda, informazioni sul trattamento dei dati (scopi, interconnessioni, tipi di dati e categorie di persone coinvolte, durata della conservazione dei dati).
RACCOLTA E TRATTAMENTO DEI DATI	Qualsiasi dato personale deve essere trattato seguendo i seguenti principi generali: - tutti i dati personali sono trattati in modo onesto e legale; - tutti i dati personali sono raccolti e trattati per scopi specifici, espliciti e legittimi; - tutti i dati personali sono corretti, completi e, se necessario, aggiornati. Il trattamento dei dati personali è possibile se: - l'interessato ha manifestato il proprio consenso; - è richiesto dalla legge; - il suo scopo è quello di salvare la vita del soggetto interessato o fornire un servizio pubblico; - è collegato alla esecuzione di un contratto di cui l'interessato è parte;

	- è necessario per il perseguimento dell'interesse legittimo del titolare, sempre che non crei pregiudizio sull'interesse, i diritti e le libertà fondamentali del soggetto interessato. Quando i dati personali sensibili sono trattati, vi è una specifica lista di condizioni da rispettare. In questo caso occorre che il soggetto interessato sia informato su: - identità del titolare del trattamento; - scopi del trattamento; - destinatari o le categorie di destinatari dei dati; - diritto ad opporsi, per uno scopo legittimo, alla raccolta di tali dati; diritto d'accesso; diritto alla rettifica dei dati; - eventuale trasferimento dei dati fuori dallo spazio UE, luogo e motivo del trasferimento.
TRASFERIMENTO DEI DATI	Il trasferimento dei dati a paesi non UE/EEA è permesso se il paese di destinazione fornisce un livello di protezione adeguato in termini di vita privata, diritti e libertà fondamentali dell'individuo. Per il trasferimento dei dati ver-

	so gli USA, le compagnie che aderiscono ai principi del Programma US/EU Safe Harbor sono considerate come aventi un "livello di protezione adeguato". Il trasferimento fuori dell'EEA può essere effettuato se necessario per: - salvaguardare la vita individuale; - salvaguardare l'interesse pubblico; - adempiere un obbligo legale; - la consultazione di un registro pubblico volto all'informazione pubblica; - l'esecuzione di un contratto concluso tra il titolare del trattamento e l'interessato o l'esecuzione di misure precontrattuali prese su richiesta del soggetto interessato; - la conclusione o l'esecuzione di un contratto tra il titolare del trattamento e una parte terza nell'interesse del soggetto. Qualora non siano rispettate le condizioni sopraelencate, il CNIL può acconsentire al trasferimento se il livello adeguato di protezione è garantito attraver-

	so clausole contrattuali, es. le clausole standard approvate dalla Commissione europea (Model Clauses) che si applicano a chi esporta e importa dati.
SICUREZZA	Chi esegue il trattamento deve adottare tutte le misure necessarie riguardo alla natura dei dati e al rischio collegato al trattamento, per preservare la sicurezza dei dati e prevenire che parti terze accedano ai dati senza autorizzazione. Il responsabile del trattamento può trattare i dati solo in base alle istruzioni del titolare del trattamento. Il responsabile deve avere garanzie sufficienti in termini di sicurezza e riservatezza. E' comunque il titolare che deve garantire la conformità del trattamento agli obblighi di legge.
NOTIFICA DI VIOLAZIONE	La legge non prevede alcun obbligo di notifica al CNIL o all'interessato in caso di violazione della sicurezza.
APPLICAZIONE	Il CNIL ha il potere di verificare ogni trattamento dei dati e può richiedere una copia di ogni documento che considera utile a tale scopo. Il CNIL ha anche il potere imporre sanzioni che possono variare in base alla gravità della violazione

APPLICAZIONE	commessa: - avvisi e notifiche in caso di inosservanza della legge; - sanzione pecuniaria fino a 150.000 € in mancanza di notificazione. Se nei successivi 5 anni la violazione si ripete, la multa può aumentare fino a 300.000 € o essere pari al 5% del giro d'affari della compagnia (ma comunque fino a un massimo di 300.000€), oltre all'immediata cessazione del trattamento dei dati. In accordo con gli articoli 226-16 a 226-24 del codice penale francese, varie violazioni possono costituire reato penale. Per esempio, la violazione, anche per negligenza, della dichiarazione preventiva (vedi "Notificazione del trattamento") è punibile fino a 5 anni di prigione e/o con multe fino a 300.000 € per le persone fisiche e fino a 1.500.000€ per le persone giuridiche.

GERMANIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita con la principale fonte legale per la protezione dei dati in Germania è il Federal Data Protection Act (BDSG). Inoltre, ogni stato tedesco ha una propria legge sulla protezione dei dati. In principio, le leggi per la protezione dei dati dai singoli stati intendono proteggere i dati dal trattamento e dall'utilizzo da parte delle pubbliche autorità degli stati, mentre il BDSG intende proteggere i dati personali dal trattamento e dall'uso da parte delle autorità pubbliche federali e da enti privati. L'applicazione compete all'autorità dei singoli stati. La competenza di ciascuna autorità statale dipende dal luogo di lavoro del titolare del trattamento dei dati.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione concernente circostanze personali o materiali di una persona identificata o identificabile.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Qualsiasi informazione sull'origine etnica o razziale, le opinioni politiche, il credo religioso o filosofico, l'appartenenza a un sindacato, la vita sessuale e lo stato di salute.

AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Ogni Stato tedesco ha una propria Autorità per la protezione dei dati che è responsabile dell'applicazione della legge e competente sui titolari dei trattamenti.
NOTIFICAZIONE DEL TRATTAMENTO	A differenza della maggior parte degli stati europei, la legge tedesca non prevede la notifica del trattamento dei dati, che è prevista solo in casi eccezionali. L'obbligo della notifica viene meno qualora il titolare del trattamento dei dati nomini il responsabile della protezione dei dati (DPO), obbligatorio all'interno delle compagnie di una certa dimensione. Le operazioni automatiche di trattamento dei dati sensibili sono soggette a un controllo preventivo da parte del rispettivo DPO.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	I Titolari del trattamento che impiegano più di 9 persone nel trattamento automatico di dati personali sono obbligati a nominare il DPO, che può essere uno degli impiegati o un consulente esterno con un grado di conoscenza sufficiente nel settore del trattamento dei dati. Il DPO deve in particolare monitorare l'uso appropriato dei programmi di trattamento dati e prendere i provvedimen-

	ti necessari affinché le persone coinvolte acquisiscano dimestichezza con le disposizioni sulla protezione dei dati. Per quanto riguarda i dati personali sensibili, questi sono soggetti a un esame preventivo all'inizio del trattamento da parte del DPO, salvo il caso in cui l'interessato abbia dato il proprio consenso. In caso di dubbio, il DPO si coordina con le autorità competenti.
RACCOLTA E TRATTAMENTO DEI DATI	La raccolta, il trattamento e l'uso dei dati personali sono ammessi se esplicitamente previsti dalla Legge per la protezione dei dati (BDSG) o da qualsiasi altra disposizione legislativa o se l'interessato ha dato il proprio consenso preventivamente. In pratica si applica la Sezione 28 del BDSG che dispone che la raccolta, il trattamento e l'uso dei dati personali sono ammissibili se: - necessari per perseguire o adempiere un obbligo legale rispetto al soggetto interessato; - necessari alla salvaguardia di un interesse legittimo del titolare, qualora il soggetto interessato non abbia un interesse legittimo superiore che impedi-

	sca al titolare di svolgere il trattamento, ecc. - i dati personali sono accessibili o il titolare è autorizzato alla loro pubblicazione. Il trattamento dei dati personali sensibili può essere effettuato se: - è necessario per proteggere gli interessi vitali dell'interessato qualora sia fisicamente o legalmente incapace di dare il proprio consenso; - i dati sono stati resi pubblici in modo manifesto dal soggetto dei dati; - è necessario per costatare, esercitare o difendere un diritto in sede legale qualora l'interessato non abbia un interesse legittimo superiore che impedisca al titolare di raccogliere, trattare o usare i dati; - è necessario per gli scopi scientifici di ricerca per i quali l'interesse scientifico supera in modo significativo quello del soggetto interessato. Il trattamento dei dati di dipendenti per scopi legati ad obblighi lavorativi è permesso solo per l'avvio, l'esecuzione e la

	chiusura del contratto di lavoro ed è soggetto a una disposizione separata (sec.32 BDSG). In ogni caso, il titolare deve garantire che il trattamento è corretto, leale ed eseguito secondo la legge, per questo deve sempre fornire all'interessato informazioni sull'identità del titolare del trattamento, gli scopi del trattamento e ogni altra informazione ritenuta utile.
TRASFERIMENTO DEI DATI	Il trasferimento dei dati verso i paesi EEA può avvenire tranquillamente grazie all'armonizzazione delle leggi tra paesi europei. Il trasferimento verso paesi non EEA può avvenire solo se: - c'è il consenso dell'interessato; - è esplicitamente permesso dal BDSG o da qualsiasi altra disposizione legale; - il destinatario dei dati garantisce un adeguato livello di protezione dei dati. La Commissione Europea ha stilato un elenco di paesi considerati adeguati con riferimento al livello di protezione dei dati: Andorra, Svizzera, Canada, Argentina, Guernsey, Isle of Man, isole Faeroe e Israele. In caso di trasferimento

	verso gli USA, si fa riferimento ai principi del Programma Safe Harbour.
SICUREZZA	I titolari del trattamento devono adottare misure tecniche e organizzative che assicurano un livello di sicurezza adeguato contro il trattamento non autorizzato o illegale e contro la perdita accidentale o la distruzione o il danneggiamento dei dati personali.
NOTIFICA DI VIOLAZIONE	L'obbligo di notifica in caso di violazione è stato recentemente implementato dal BDSG con la Sez. 42 in cui è previsto l'obbligo di notifica se: - si verifica abuso, perdita o acquisizione non autorizzata di dati personali sensibili, dati personali soggetti a segretezza professionale, dati personali relativi a reati criminali e/o amministrativi, dati personali concernenti conti bancari o carte di credito, dati online; - attraverso il trattamento di dati online vi è un serio rischio di interferire con gli interessi degli individui coinvolti.
APPLICAZIONE	Possono essere inflitte sanzioni pecuniarie fino a 300.000 € e anche sanzioni detentive fino a un massimo di 2 anni.

GRECIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita nell'ottobre 1997 con la legge 2472/1997 sulla protezione degli individui riguardo al trattamento dei dati personali. L'esecuzione dipende dal Data Protection Authority. (DPA).
DEFINIZIONE DI DATI PERSONALI	Tutte quelle informazioni riguardanti l'interessato.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati riguardanti l'origine etnica o razziale, le opinioni politiche, il credo religioso o filosofico, l'appartenenza a un sindacato, la salute, l'assistenza sociale, la vita sessuale, i carichi penali pendenti e le convinzioni personali.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Autorità per la protezione dei dati
NOTIFICAZIONE DEL TRATTAMENTO	Il titolare del trattamento deve notificare per iscritto all'Autorità l'avvio del trattamento dei dati. La notifica deve includere: - il nome, l'impiego e l'indirizzo del titolare del trattamento; - l'indirizzo in cui il sistema di trattamento dei dati è situato; -la descrizione degli scopi del trattamento;

	- la categoria dei dati personali; - il periodo di tempo nel quale verranno analizzati e mantenuti i dati; - i destinatari o le categorie di destinatari dei dati; - qualsiasi trasferimento e lo scopo di questo trasferimento a paesi terzi; - le caratteristiche del sistema e le misure di sicurezza prese per la protezione del file e del trattamento dei dati. Questi dati saranno poi registrati nell'archivio del DPA.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Non vi è l'obbligo di nominare all'interno delle organizzazioni il DPO.
RACCOLTA E TRATTAMENTO DEI DATI	La raccolta e il trattamento dei dati personali sono consentiti solo se l'interessato manifesta il proprio consenso preventivo. Eccezionalmente, il trattamento può avvenire senza consenso se: - è necessario per l'esecuzione di un contratto di cui l'interessato è parte; - necessario affinché il titolare del trattamento adempia ad obblighi legali; - è necessario per proteggere gli interessi vitali dell'interessato

	qualora quest'ultimo sia fisicamente o legalmente incapace di fornire il proprio consenso; - è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare o una terza parte a cui vengono comunicati i dati; - il trattamento è assolutamente necessario per il perseguimento di un interesse legittimo da parte del titolare del trattamento o di terzi a cui i dati sono comunicati, a condizione che siano pregiudicati gli interessi, i diritti e le libertà fondamentali del soggetto interessato. Il trattamento dei dati personali sensibili è in via generale proibito. La raccolta e il trattamento di questi dati sono permessi dall'Autorità nazionale quando una o più delle seguenti condizioni è rispettata: - l'interessato ha dato il proprio consenso per iscritto; - il trattamento è necessario per proteggere gli interessi vitali dell'interessato dei dati; -il trattamento si riferisce a dati resi pubblici dall'interessato

	o è necessario per costituire, esercitare, difendere un diritto per via giudiziaria; - il trattamento è necessario per scopi di medicina preventiva, diagnosi medica o servizi sanitari ed è tutelato da un professionista in campo sanitario, soggetto al segreto professionale o al rispetto di codici deontologici; - il trattamento è effettuato da un'Autorità Pubblica ed è necessario per scopi di sicurezza nazionale e politiche di sicurezza; per la protezione della salute pubblica o per il controllo pubblico sul fisco e i servizi sociali; - il trattamento è necessario per scopi scientifici e di ricerca; - il trattamento riguarda dati pubblici, relativo all'esercizio di uffici di pubblica utilità e siano trattati per scopi puramente giornalistici. L'Autorità nazionale per la protezione dei dati può permettere questo trattamento solo se è assolutamente necessario per assicurare il diritto di informazione su questioni di pubblico interesse. L'Autorità nazionale per la protezione dei dati può permettere la raccolta e il trattamento dei dati sensibili su richiesta del

	titolare del trattamento. Il permesso è concesso per un periodo di tempo specifico, a secondo dello scopo del trattamento. Può essere rinnovato tramite una nuova richiesta da parte del titolare del trattamento. Il permesso deve necessariamente contenere le seguenti informazioni: - il nome completo o il nome dell'ente, l'indirizzo del titolare del trattamento e di un suo eventuale rappresentante; - l'indirizzo del luogo in cui risiede il file; - le categorie dei dati personali inclusi nel file; - il periodo di tempo del permesso; - eventuali termini e condizioni imposte dal DPA; - l'identità dei destinatari. I permessi vengono registrati in un apposito registro tenuto dall'Autorità nazionale. Qualsiasi modifica diversa dall'indirizzo del titolare del trattamento, comporta l'emissione di un nuovo permesso, sempre che i termini e le condizioni previsti dalla legge siano rispettati.

TRASFERIMENTO DEI DATI	Il trasferimento è concesso senza problemi all'interno degli stati membri UE. Verso gli altri paesi, il trasferimento deve essere autorizzato dall'Autorità nazionale che concede l'autorizzazione sulla base dell'adeguatezza del livello di protezione del paese a cui i dati vengono trasferiti. Tale autorizzazione non è prevista qualora i paesi di destinazione siano quelli identificati dalla Commissione Europea. Il trasferimento dei dati a un paese non UE che non assicura un adeguato livello di protezione può essere effettuato con un'autorizzazione dell'Autorità se: - il soggetto dei dati ha manifestato il proprio consenso; - è necessario per proteggere gli interessi vitali dell'interessato, se questo è fisicamente o legalmente incapace di dare il proprio consenso; - è necessario per la conclusione e l'esecuzione di un contratto tra l'interessato e il titolare del trattamento o tra il titolare del trattamento e una parte terza nell'interesse del soggetto dei dati;

	- è necessario per l'implementazione di misure precontrattuali prese in risposta alla richiesta dell'interessato; - è necessario per salvaguardare un interesse pubblico superiore, specialmente per l'esecuzione di un accordo di cooperazione con le autorità pubbliche di un altro paese, premesso che il titolare del trattamento fornisca tutele adeguate in rispetto alla protezione della privacy e alle libertà fondamentali; - è necessario per l'esercizio o la difesa di un diritto davanti a un tribunale; - è fatto da un registro pubblico che per legge fornisce informazioni pubbliche ed è quindi accessibile a chiunque dimostri un interesse legittimo; - il titolare del trattamento deve fornire tutele adeguate per quanto riguarda la protezione dei dati e l'esercizio dei loro diritti. Nel caso in cui vengano utilizzate clausole contrattuali approvate dalla Commissione Europea, o, se il destinatario dei dati risiede negli USA e ha aderito al Programma Safe Harbor,

	non è richiesta alcuna autorizzazione preventiva.
SICUREZZA	Il trattamento dei dati deve essere confidenziale. Deve essere portato avanti solo ed esclusivamente da addetti che agiscono sotto l'autorità del titolare del trattamento. Il titolare del trattamento deve scegliere persone che abbiano qualifiche professionali tali da garantire il rispetto della riservatezza. Il titolare del trattamento deve implementare le misure tecniche e organizzative idonee ad assicurare i dati e proteggerli contro la distruzione accidentale o illegale, la perdita accidentale, l'alterazione, la visione non autorizzata.
NOTIFICA DI VIOLAZIONE	Non è previsto un obbligo di notifica in caso di violazione.
APPLICAZIONE	L'Autorità nazionale per la protezione dei dati può infliggere ai titolari o loro eventuali rappresentanti, le seguenti sanzioni amministrative: - un avviso con un ordine di cessazione del trattamento entro uno specifico limite temporale; - una multa tra gli 880 € e i 147000 €; - una revoca temporanea del

	permesso; - una revoca definitiva del permesso; - la distruzione del file o un divieto di trattamento e la distruzione o la restituzione dei dati. Inoltre, possono anche essere inflitte le seguenti sanzioni penali: - chiunque sbagli a notificare all'Autorità le operazioni di trattamento verrà punito con la reclusione fino a un massimo di 3 anni e una multa tra i 2940 € e i 14705 €. - chiunque possieda un file senza permesso, può essere punito con la reclusione di almeno 1 anno e una multa tra i 2940 € e i 14705 €. - chiunque proceda all'interconnessione di file senza notificarlo al DPA verrà punito con la reclusione fino a massimo 3 anni e una multa tra i 2940 € e i 14705 €. - chiunque interferisca in modo illegale durante il trattamento sarà punito con la reclusione di almeno un anno e con una multa tra i 2940 € e i 29411 €.

	- qualunque titolare del trattamento che non rispetti le decisioni dell'Autorità può essere punito con la reclusione per almeno 2 anni e una multa tra i 2940 € e i 14705 €. Se il titolare del trattamento non è una persona fisica, allora ci si rivolgerà ai rappresentanti della persona giuridica. Qualsiasi persona fisica o giuridica che violi la legge sarà considerata pienamente responsabile. Se non c'è un danno materiale, verrà richiesto un risarcimento di almeno 5 882€ come previsto dall'articolo 932 del codice civile.

IRLANDA

LEGGE	Il nucleo della legge irlandese sulla privacy è il Data Protection Act (DPA) del 1988 emendato nel 2003 con l'implementazione della Direttiva UE 95/46/EC.
DEFINIZIONE DI DATI PERSONALI	Dati relativi a un individui che può essere identificato da questi dati.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Sono dati relativi a: a) origine etnica o razziale, opinioni politiche, credo religioso o filosofico; b) l'appartenenza a un sindacato; c) la condizione fisica, la salute mentale o la vita sessuale; d) la commissione di atti illegale da parte dell'interessato; e) qualsiasi procedimento per offesa o la sentenza di una corte riguardo questa offesa.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Office of the Data Protection Commissioner (DPC).
NOTIFICAZIONE DEL TRATTAMENTO	I titolari e i responsabili del trattamento devono registrarsi presso l'Autorità nazionale. Per quanto riguarda la notificazione, alcune categorie di titolari del trattamento sono soggette ad un obbligo assoluto di

	di notifica. Sono invece previste ampie eccezioni per certe categorie di trattamento, per le quali non esiste l'obbligo di notifica. La legge del 2003 prevede eccezioni per: - organizzazioni no-profit, premesso che il trattamento dei dati si riferisce solo alle loro attività; - titolari e responsabili del trattamento che trattano dati conservati in registri pubblici o che effettuano trattamenti manuali. Il Data Protection Act del 1988 esonera le seguenti categorie dall'obbligo della notifica del trattamento: - titolari del trattamento che trattano dati dei dipendenti durante il normale corso del rapporto di lavoro; - candidati per uffici politici e rappresentanti eletti; - scuole, collegi, università e simili istituzioni educative; - notai e avvocati; - responsabili che trattano dati di azionisti, direttori o altri funzionari passati e presenti, in

	adempienza alle Irish Companies Acts; - titolari del trattamento che trattano dati a fini giornalistici, letterari o artistici; - titolari o responsabili che operano in base ad un codice statutario di protezione dei dati (tuttavia, al momento non esistono codici di questo tipo). Hanno invece un obbligo assoluto di notifica del trattamento banche, compagnie di assicurazione, società commerciali, agenzie di credito, compagnie di telecomunicazione, medici e chiunque tratti dati genetici. I titolari o gli addetti al trattamento dati sono obbligati a rinnovare la notifica di trattamento ogni anno. Il DPC può, in determinati casi, rifiutare la richiesta di notifica del trattamento. In questo caso, si può esercitare il diritto di appello davanti alla Corte d'Appello circoscrizionale.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Le organizzazioni non hanno l'obbligo di nominare il DPO, anche se sarebbe auspicabile che lo facessero e, qualora all'interno di un'organizzazione sia presente tale figura, il soggetto interessato ne deve esse-

	re informato. L'autorità nazionale inoltre raccomanda che i titolari del trattamento nominino un coordinatore per la gestione delle richieste di accesso.
RACCOLTA E TRATTAMENTO DEI DATI	La normativa nazionale ha accolto i principi contenuti della Direttiva UE 95/46/EC per quanto riguarda la raccolta e il trattamento dei dati. Inoltre, nel trattare i dati personali occorre rispettare almeno una delle seguenti condizioni definite con il Data Protection Act: - il soggetto dei dati ha dato il consenso al trattamento; - il trattamento è richiesto per l'esecuzione di un contratto di cui l'interessato è parte; - il trattamento è necessario per evitare lesioni o danni personali alla salute dell'interessato; - il trattamento serve a proteggere gli interessi vitali di un essere umano; - il trattamento è necessario per amministrare la giustizia; - il trattamento rientra nell'ambito degli interessi legittimi perseguiti dal titolare del trattamento.

	Per quanto riguarda i dati sensibili, ci sono ulteriori condizioni da soddisfare. Ad esempio, il consenso "esplicito" dell'interessato dei dati. Le basi per il trattamento dei dati sensibili sono piuttosto restrittive e a volte può essere difficile ottenere l'autorizzazione al loro trattamento.
TRASFERIMENTO DEI DATI	L'Autorità nazionale per la protezione dei dati prevede un certo numero di restrizioni sul trasferimento di dati personali fuori dall'EEA. Il trasferimento può avere luogo se il paese destinatario offre un adeguato livello di protezione sulla privacy e in questo senso la Commissione ha identificato un numero limitato di paesi considerati idonei. In base a quanto stabilito dall'Autorità, il trasferimento dei dati in paesi non EEA è possibile solo se: - l'interessato ha dato consenso al trasferimento; - è necessario per l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; - è necessario per ragioni di pubblico interesse;

	- è necessario sulla base di obblighi internazionali dello stato; - è richiesto o autorizzato per legge; - è necessario per ottenere un parere legale; - è necessario per prevenire lesioni o danni personali alla salute dell'interessato; - è fatto in base ad uno degli accordi UE ("Approved Model Data Transfer Agreements"). Visti i diversi standard di protezione dei dati in USA, il trasferimento verso gli Stati Uniti può avere luogo se la compagnia americana ha aderito al programma Safe Harbour.
SICUREZZA	I titolari e i responsabili al trattamento dati devono adottare adeguate misure di sicurezza per impedire l'accesso, l'alterazione o la distruzione dei dati non autorizzati. Essi devono prendere appropriati provvedimenti per la sicurezza, tenendo presente: - lo stato attuale della tecnologia a disposizione; - il costo di implementazione delle misure di sicurezza; - la natura dei dati personali;

	- il danno che può risultare da un trattamento non autorizzato o dalla perdita dei dati. I titolari e i responsabili sono anche obbligati ad assicurare che tutti coloro che all'interno dell'organizzazione si occupano di trattamento dati conoscano e applichino le misure di sicurezza previste.
NOTIFICA DI VIOLAZIONE	Con la legge è stato pubblicato il Personal Data Security Breach Code nel quale è previsto che qualsiasi comunicazione di dati non autorizzata deve essere notificata all'Autorità, salvo i casi in cui la divulgazione di tali dati si riferisca a meno di 100 persone, non riguardi dati sensibili o finanziari e sia stata comunicata agli interessati. Inoltre, qualsiasi violazione nell'ambito dell'uso della rete o dei servizi elettronici deve essere notificata al Commissario per la Protezione dei Dati e, laddove tale violazione violi i dati personali o la privacy degli abbonati, vi è l'obbligo di informare anche questi ultimi. In circostanze molto limitate, i titolari del trattamento possono non notificare la violazione nel caso in cui abbiano reso inac

	cessibili i dati ad utenti non autorizzati (ad es. criptaggio).
APPLICAZIONE	L'Autorità nazionale è responsabile dell'applicazione del DPA e della successiva legislazione europea in materia. Le violazioni di specifiche disposizioni possono essere oggetto di sanzioni penale. Tra queste: - la mancata notifica del trattamento da parte del titolare o dell'addetto al trattamento dati; - la comunicazione di dati personali senza autorizzazione; - la non applicazione di una notifica esecutiva Le sanzioni inflitte sono: - multa di massimo 3000€; - messa in stato d'accusa e multa fino a massimo 100 000€. La violazione di altre disposizioni di legge non comporta di per sé una responsabilità penale, ma l'Autorità può investigare sull'incidente ed emettere delle notifiche esecutive a carico del titolare del trattamento. Inoltre, violare le norme danneggia l'immagine e la reputa-

	zione di compagnie e istituzioni, in quanto le violazioni sono rese pubbliche attraverso il Report Annuale dell'Autorità nazionale.

ITALIA

LEGGE	Con il Decreto Legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali" è stata recepita la direttiva UE 46/1995/EC e la direttiva 58/202/EC.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione, anche indiretta, che permette di risalire all'identità di una persona (*), ivi compreso un numero di identificazione personale. * Fino al dicembre 2011 la legge italiana considerava come "persona interessata" del trattamento dei dati non solo le persone fisiche ma anche quelle giuridiche. L'art. 40, comma 2, lett. a) e b), del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214 ha invece disposto l'allineamento della definizione nazionale di "persona interessata" con quella prevista dalla direttiva europea, e quindi si intendono solo le persone fisiche, non più anche quelle giuridiche. La prima conseguenza è che i dati che si riferiscono ad Aziende, Pubbliche Amministrazioni, fondazioni, associazioni ecc. potranno essere liberamente trattati senza informativa e senza le tutele previste dal Codice per la protezione dei dati personali. Inoltre, le persone

	giuridiche non potranno più presentare istanza di accesso ai dati personali che li riguardano.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Qualsiasi dato che svela origine etnica o razziale, credo religioso, filosofico o di altro tipo, opinioni politiche, appartenenza ai partiti, sindacati, associazioni, organizzazioni a carattere religioso, filosofico, politico o sindacale, vita sessuale o salute.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Garante per la protezione dei dati personali.
NOTIFICAZIONE DEL TRATTAMENTO	In base all'art. 37 del codice, il titolare deve notificare il trattamento dei dati esclusivamente se tale trattamento concerne: - dati genetici, dati biometrici o altri dati che svelino la posizione geografica degli individui attraverso rete di comunicazione elettronica; - dati idonei a rivelare lo stato di salute e la vita sessuale, trattati per gli scopi di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi o tessuti, spese di monitoraggio della spesa sanitaria;

	- dati idonei a rivelare la vita sessuale e la sfera psichica trattati da associazioni, enti od organismi no-profit anche non riconosciuti a carattere politico, filosofico, religioso o sindacale; - dati trattati con l'aiuto di mezzi elettronici per delineare il profilo della persona interessata e/o la sua personalità, analizzando abitudini e scelte di consumo, monitorando l'uso di servizi elettronici di comunicazione eccetto per quelle operazioni tecnicamente indispensabili per fornire tali servizi agli utenti; - dati sensibili registrati in banche dati per scopi di selezione del personale per conto di terzi, nonchè dati sensibili usati per sondaggi di opinione, ricerche di mercato o di altro tipo; - dati conservati in banche dati ad hoc gestite con mezzi elettronici relativi alla solvibilità economica, attività e passività, obbligazioni, condotte illegali e/o fraudolente.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Non vi è l'obbligo di nominare all'interno delle organizzazioni il DPO.
RACCOLTA E TRATTAMENTO DEI DATI	Enti privati o pubblici economici hanno il permesso di raccogliere e trattare i dati qualora l'in-

	teressato abbia dato il proprio consenso che deve essere reso liberamente, per iscritto e su specifici trattamenti chiaramente indicati. All'interessato deve inoltre essere consegnata l'informativa prevista all'art. 13 del Codice. Tuttavia, il consenso non è richiesto se il trattamento dei dati personali: - è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; - è necessario per eseguire obblighi derivanti da un contratto di cui è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato; - concerne i dati presi da registri pubblici, elenchi, atti o documenti pubblici, fermo restando limiti e modalità stabiliti da leggi, regolamenti o normativa comunitaria riguardo la loro visione e pubblicazione; - concerne dati relativi a attività economiche che sono trattati nel rispetto della legislazione in materia di segreto industriale e aziendale;

	- è necessario per salvaguardare la vita o l'integrità fisica di una parte terza. Se questo scopo concerne la persona interessata e quest'ultima non può dare il proprio consenso perché fisicamente o legalmente incapace, il consenso sarà dato da chi esercita legalmente la potestà; - è necessario ai fini dello svolgimento delle investigazioni difensive o per difendere un diritto in sede giudiziaria; - è necessario per perseguire un interesse legittimo del titolare del trattamento o di una parte terza destinataria dei dati, qualora non prevalgano diritti e libertà fondamentali, la dignità o un legittimo interesse dell'interessato; - è effettuato da associazioni, enti, organismi no profit, anche non riconosciuti, per il perseguimento di scopi determinati individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo con riferimento agli iscritti o a soggetti che hanno con tali organismi contratti regolari; - è necessario esclusivamente per scopi scientifici e statistici in conformità a codici deontologici definiti;

	- riguarda dati contenuti nei curricula; - concerne comunicazioni di dati tra società, enti o associazioni per scopi amministrativi e contabili, purché tali finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa. I dati sensibili possono essere trattati previo consenso scritto dell'interessato e previa autorizzazione del Garante, tranne che nei seguenti casi: - dati che riguardano membri di enti religiosi o soggetti che hanno rapporti regolari con questi enti per scopi puramente religiosi, a condizione che tali dati vengano trattati o dagli enti stessi o da enti civilmente riconosciuti e non vengano comunicati o diffusi fuori da questi enti; - dati relativi all'adesione a associazioni sindacali o di categoria; - i dati contenuti nei Curricula. I dati sensibili possono anche essere trattati senza consenso, previa autorizzazione del Garante quando:

	- il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati negli atti costitutivi e statutari e in relazione ai dati degli aderenti o dei soggetti che hanno contatti regolari con tali associazioni, sempre che i dati non vengano comunicati o diffusi all'esterno; - il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se tale finalità riguarda l'interessato e quest'ultimo non può dare il proprio consenso per impossibilità fisica o per incapacità di intendere o di volere, il consenso deve essere dato da chi esercita legalmente la potestà; - il trattamento è necessario per lo svolgimento delle investigazioni difensive o per fare valere in sede giudiziaria un diritto. Se i dati possono rivelare lo stato di salute e la vita sessuale, il diritto deve essere di pari rango rispetto a quello dell'interessato, o essere un diritto della per-

	sonalità o altro diritto o libertà fondamentale e inviolabile; - il trattamento è necessario per adempiere a specifici obblighi o compiti previsti dalla legge per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza. Il Garante ha emesso autorizzazioni generali per il trattamento dei dati sensibili.
TRASFERIMENTO DEI DATI	Il titolare del trattamento può liberamente trasferire dati personali all'interno degli stati membri dell'Unione europea. I dati personali possono essere trasferiti fuori dal territorio UE se: - l'interessato dei dati ha fornito il proprio consenso esplicito o in forma scritta se si tratta di dati sensibili; - Il trasferimento è necessario per l'esecuzione di obblighi derivanti da un contratto di cui la persona interessata è parte o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o l'esecuzione di un contratto stipulato nel suo interesse;

	- il trasferimento è necessario per salvaguardare un interesse pubblico rilevante individuato con legge o regolamento o, se riguarda dati sensibili o giudiziari, specificato o individuato con riferimento agli artt. 20 e 21 del codice sulla privacy; - il trasferimento è necessario per salvaguardare la vita o l'integrità fisica di una parte terza. Se tale finalità concerne l'interessato e quest'ultimo non può dare il proprio consenso per incapacità fisica o legale, il consenso verrà dato da chi esercita legalmente la potestà; - il trasferimento è necessario per lo svolgimento delle investigazioni difensive o in generale per far valere o difendere un diritto in sede giudiziaria; - il trasferimento è effettuato in seguito ad una richiesta di accesso ai documenti amministrativi, o ad una richiesta di informazioni da un pubblico registro; - il trasferimento è necessario esclusivamente per scopi scientifici, statistici o storici in conformità ai rispettivi codici deontologici. Il trasferimento di dati personali a paesi non appartenenti all'U-

	nione Europea può essere permesso se autorizzato dal Garante in base ad adeguate garanzie dei diritti della persona interessata. Il trasferimento è vietato quando i paesi di destinazione o di transito dei dati non assicurano un livello di tutela adeguato. Inoltre bisogna tenere in considerazione i metodi usati per il trasferimento e le operazioni di trattamento dei dati, gli scopi rilevanti, la natura dei dati e le misure di sicurezza.
SICUREZZA	I dati personali trattati devono essere conservati e controllati, anche in base al progresso tecnologico, in modo tale da minimizzare il rischio di distruzione o perdita, anche accidentale, dei dati, o di accesso non autorizzato. Il trattamento di dati personali attraverso mezzi elettronici deve essere permesso solo se le misure minime di sicurezza sono adottate secondo specifiche tecniche di cui all'allegato B del codice sulla privacy: - autenticazione informatica; - assegnazione delle credenziali di autenticazione;

	- implementazione di una procedura di autorizzazione; - aggiornamenti regolari di specifiche concernenti lo scopo del trattamento; - utilizzazione di idonei strumenti elettronici per la protezione di dati sensibili e giudiziari per evitare operazioni illegali e accessi non autorizzati; - implementazione di idonee procedure per il salvataggio di copie backup; - implementazione di tecniche di criptaggio o codici di identificazione per specifiche operazioni di trattamento dati portate avanti da organismi sanitari in relazione a dati sulla salute e sulla vita sessuale. Il trattamento di dati personali senza mezzi elettronici dovrebbe essere permesso solo se sono adottate le seguenti misure minime di sicurezza: - aggiornamento regolare di specifiche concernenti lo scopo delle operazioni di trattamento dati; - implementazione di procedure per salvaguardare le registrazioni e i documenti;

	- implementazione di procedure per mantenere certe registrazioni in sistemi ad accesso ristretto e regolazione dei meccanismi di accesso in modo da essere in grado di identificare le entità che vi accedono. Certi responsabili sono autorizzati ad implementare misure di sicurezza semplificate.
NOTIFICA DI VIOLAZIONE	In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza alcun ritardo detta violazione al Garante dimostrando, se possibile, di avere utilizzato misure tecnologiche di protezione che rendono i dati oggetto della violazione inintelligibili a chiunque non sia autorizzato ad accedervi. Qualora ciò non sia possibile, il fornitore ha l'obbligo di comunicare, senza ulteriori ritardi, tale violazione all'abbonato e/o altre persone qualora la violazione possa arrecare pregiudizio ai loro dati personali o alla loro riservatezza. Queste informazioni devono anche essere fornite al Garante e all'Autorità per la Salvaguardia delle Comunicazioni (AGCOM).

APPLICAZIONE	L'Autorità nazionale per la protezione dei dati personali opera in completa autonomia e indipendenza di giudizio e valutazione. Ha numerose funzioni, tra cui: - controllare che i trattamenti siano effettuati nel rispetto della legge e in conformità alla notificazione; - esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano; - obbligare i titolari a rendere conforme alla legge il trattamento; - vietare tutto o in parte il trattamento illecito o non corretto o disporne il blocco. Inoltre può nominare esperti, procedere con ispezioni, richiedere al titolare o al responsabile del trattamento informazioni o documenti. In caso di illeciti penali, l'Autorità nazionale per la protezione dei dati deve darne comunicazione all'autorità giudiziaria. Il codice sulla privacy prevede sanzioni amministrative di tipo

	pecuniario, la cui entità può variare a seconda della natura della violazione da € 6.000 a € 300.000. Il Decreto individua i casi in cui le sanzioni vengono applicate in misura ridotta, così come i casi in cui le stesse possono essere quadruplicate. Infine, il Codice sulla privacy prevede anche sanzioni penali con pene di tipo detentivo che possono andare da tre mesi a due anni.

LETTONIA

LEGGE	La Costituzione della Lettonia, adottata il 14 febbraio 1922, stabilisce che la privacy è un diritto fondamentale della persona e per questo tutte le leggi che proteggono la privacy si applicano indifferentemente ai cittadini lettoni e agli stranieri. La Legge sulla Protezione dei Dati personali è stata approvata dal Parlamento il 23 marzo 2000 ed è entrata in vigore il primo gennaio 2001. Essa è stata modificata il 24 ottobre del 2002, il 19 dicembre 2006, il primo marzo del 2007 ed il 21 febbraio del 2008, per incorporare le varie direttive in materia dell'Unione Europea. La vigente versione è entrata in vigore il 6 marzo del 2008.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione relativa a una persona identificata o identificabile.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati personali che rivelano la razza, l'origine etnica, le convinzioni religiosi, filosofiche o politiche, l'appartenenza sindacale, la salute o la vita sessuale.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	*Data State Inspectorate*

NOTIFICAZIONE DEL TRATTAMENTO	I titolari del trattamento devono inviare notifica al Data State Inspectorate, a meno che non siano previste specifiche eccezioni. Qualsiasi variazione o modifica dei dati richiede una variazione della notificazione del trattamento. Esiste un modulo ufficiale che deve essere compilato con le seguenti informazioni: a. identità del titolare del trattamento e del suo rappresentante; b. principali caratteristiche del software; c. scopi del trattamento; d. eventuali enti terzi responsabili del trattamento; e. qualsiasi dato personale che sarà raccolto in ciascun registro (specificare se si tratta di dati sensibili); f. basi legali per la raccolta dati e una breve descrizione dei metodi usati; g. mezzi e metodi disponibili per l'aggiornamento dei dati; h. mezzi di comunicazione a altri enti; i. trasferimento di dati a pa-

	esi terzi, i motivi, le basi e le misure adottate in ciascun trasferimento.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Non vi è l'obbligo di nominare all'interno delle organizzazioni il DPO.
RACCOLTA E TRATTAMENTO DEI DATI	Il trattamento dei dati può essere effettuato se: - c'è il consenso dell'interessato, - è necessario all'esecuzione di un contratto concluso con la persona interessata; - è necessario affinché il titolare del trattamento adempia ai propri obblighi e doveri, - è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; - è necessario per rispettare diritti umani e libertà fondamentali dell'interessato.
TRASFERIMENTO DEI DATI	Il trasferimento dei dati a paesi non UE/EEA è permesso se il paese fornisce un livello di protezione sufficiente in termini di vita privata o diritti e libertà fondamentali dell'individuo. Per il trasferimento dei dati agli USA, si fa riferimento ai principi di cui al programma Safe Harbor.

	I titolari del trattamento possono trasferire i dati personali fuori dell'EEA se il trasferimento : - è necessario per salvaguardare la vita individuale; - è necessario per salvaguardare l'interesse pubblico; - è necessario affinché vengano rispettati obblighi legali a cui è tenuto il responsabile del trattamento; - avviene partendo da un registro pubblico predisposto per l'informazione o la consultazione pubblica; - è necessario all'esecuzione di un contratto tra il titolare del trattamento e l'interessato; - è necessario alla conclusione o all'esecuzione di un contratto tra il titolare del trattamento e una parte terza, nell'interesse del soggetto dei dati.
SICUREZZA	I titolari del trattamento devono implementare le misure tecniche e organizzative appropriate per proteggere i dati personali contro perdita o distruzione accidentale o intenzionale, contro l'apertura o l'accesso non autorizzati, contro la distribuzione o la modifica dei

	dati. I titolari devono inoltre implementare misure speciali di protezione nei casi di trasferimento elettronico dei dati. Il livello minimo di queste misure è specificato dalla DPA.
NOTIFICA DI VIOLAZIONE	Non prevista dalla legge.
APPLICAZIONE	Spetta al Data State Inspectorate.

LITUANIA

LEGGE	La Lituania ha recepito la direttiva UE 95/46/EC attraverso diverse leggi nazionali, l'ultima delle quali è entrata in vigore l'1/09/2011. Inoltre, la Lituania ha pienamente recepito la direttiva 2006/24/EC attraverso la legge nazionale sulle Comunicazioni Elettroniche del 15 aprile 2004.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione relativa a una persona fisica identificata o identificabile direttamente o indirettamente in riferimento a dati come numero di identificazione personale o uno o più fattori specifici riguardo alla sua identità fisica, fisiologica, mentale, economica, culturale o sociale.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati relativi all'origine razziale o etnica di una persona fisica, le sue opinioni politiche, i credo religiosi o filosofici, l'appartenenza a un sindacato, la sua saluta, vita sessuale o condanne criminali.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	The State Data Protection Inspectorate
NOTIFICAZIONE DEL TRATTAMENTO	La notificazione del trattamento è obbligatoria solo per quei titolari che trattano dati attraverso mezzi automatici, tranne

	i casi in cui il trattamento sia effettuato: - per scopi di amministrazione interna; - per scopi politici, filosofici, religiosi o sindacali da parte di una fondazione, associazione o qualsiasi altra organizzazione no profit a condizione che i dati trattati si riferiscono solo ai membri di tale organizzazione o ad altre persone che partecipano regolarmente alle sue attività, in connessione con gli scopi di tali organizzazioni; - dai media per dare informazioni di tipo artistico e letterario al pubblico; - in base al regolamento sul segreto di stato e segreto ufficiale. I titolari che vogliono inviare una notifica all'ispettorato sul trattamento dei dati devono compilare un modulo standard di notifica, che includa informazioni riguardo: - lo scopo del trattamento; - i gruppi dei soggetti; - le fonti dei dati; - i gruppi di destinatari dei dati;

	- la lista di categorie di dati personali che vengono trattati; - i trasferimenti di dati a paesi stranieri; - il periodo di conservazione dei dati; - il processore dei dati; - la lista delle misure di sicurezza. Dopo la notifica, i titolari del trattamento sono registrati nell'apposito Registro tenuto presso l'Autorità nazionale. La notifica e la registrazione sono gratuite. Se i dati non sono trattati da mezzi automatici, non c'è l'obbligo di notifica. Tuttavia, certi trattamenti possono essere effettuati solo dopo che l'Autorità nazionale ha effettuato un controllo preventivo e ha concesso apposita autorizzazione. Il controllo preventivo avviene nei casi seguenti: - quando il titolare del trattamento intende trattare dati personali sensibili attraversi mezzi automatici, eccetto quando il trattamento è fatto per gli scopi di amministrazione interna o nei casi di prevenzione e investigazione su attività illegali, co-

	così come per udienze giudiziarie; - quando il titolare del trattamento intende trattare dati pubblici attraverso mezzi automatici, a meno che non siano previste leggi per casi eccezionali; - quando i titolari del trattamento di istituzioni pubbliche intendono autorizzare i responsabili a trattare dati personali, eccetto i casi in cui disposizioni legislative stabiliscano il diritto del titolare del trattamento ad autorizzare un particolare responsabile del trattamento o qualora l'addetto individuato dal titolare sia una persona giuridica; - quando i dati sulla salute sono trattati da mezzi automatici o per scopi di ricerca medico-scientifica; - quando i dati sono trattati per valutare la solvibilità di una persona e gestire il suo debito; - quando i dati sono trattati per scopi statistici, storici o scientifici.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Le organizzazioni titolari del trattamento hanno il diritto, ma non l'obbligo, di designare un DPO. Il titolare del trattamento deve inviare una notifica all'Ispettorato entro 30 giorni.

	Il responsabile della protezione dei dati deve: - rendere pubbliche le azioni per il trattamento dei dati effettuate dal titolare secondo la procedura stabilita dal governo; - supervisionare se i dati personali sono trattati rispettando le disposizioni di legge; - iniziare la procedura delle notifiche all'Ispettorato in caso di controllo preventivo; - monitorare il trattamento dei dati effettuato dagli addetti del titolare del trattamento; - presentare proposte e risultati al titolare del trattamento riguardo la definizione di misure per la protezione e il trattamento dei dati e verificare l'implementazione e l'utilizzo di tali misure; - adottare misure per eliminare qualsiasi violazione nel trattamento dei dati senza ritardi; - istruire gli impiegati autorizzati a trattare i dati sulle disposizioni di legge; - istruire le richieste all'Ispettorato circa il trattamento e la protezione di dati personali;

	- assistere gli interessati per l'esercizio dei propri diritti; - inviare notifica scritta all'Ispettorato qualora il titolare del trattamento tratti dati personali in violazione delle leggi rifiutandosi di rettificare tali violazioni. Nel caso in cui non venga nominato il DPO, sarà l'amministratore delegato del titolare del trattamento il responsabile ex officio della protezione dei dati e di qualsiasi violazione.
RACCOLTA E TRATTAMENTO DEI DATI	I dati personali possono essere trattati se: - la persona interessata ha dato il proprio consenso; - deve essere concluso o firmato un contratto di cui l'interessato è parte; -c'è un obbligo legale per il titolare del trattamento di trattare i dati personali; - il trattamento è necessario per proteggere gli interessi vitali dell'interessato; - il trattamento è necessario per l'esercizio di una potestà legislativa; - il trattamento è necessario per perseguire un interesse legitti-

	mo del titolare del trattamento o di una parte terza a cui i dati sono comunicati, a condizione che non prevalgano gli interessi della persona interessata. I dati personali sensibili possono essere trattati solo nei casi seguenti: - la persona interessata ha dato il proprio esplicito consenso per iscritto - il trattamento è necessario per scopi connessi con l'ambiente di lavoro; - è necessario per proteggere gli interessi vitali dell'interessato o di qualsiasi altra persona, qualora sia attestata l'incapacità fisica o giuridica di dare il proprio consenso; - il trattamento dei dati è effettuato per scopi politici, filosofici, religiosi, sindacali da una fondazione, associazione o qualsiasi altra organizzazione no profit, come parte delle sue attività, a condizione che i dati personali trattati riguardino solamente i membri di tale organizzazione o altre persone che partecipano regolarmente a tale organizzazione in connessione con i suoi scopi;

	- i dati sono resi pubblici dall'interessato; - i dati sono necessari, nei casi previsti dalla legge, per scopi investigativi e di prevenzione delle attività criminali; - i dati sono necessari la difesa di un diritto in via giudiziaria; - la legge autorizza il trattamento ditali dati. Inoltre, il titolare del trattamento deve informare gli interessati se i dati personali sono raccolti direttamente o da terzi, e se tali dati sono comunicati a terzi. Tale informazione deve contenere: - l'identità e il luogo di residenza del titolare del trattamento e del suo eventuale rappresentante; - gli scopi del trattamento dei dati; - altre informazioni addizionali se necessarie per assicurare un trattamento onesto dei dati, senza infrangere i diritti dell'interessato.
TRASFERIMENTO DEI DATI	I dati possono essere trasferiti all'interno della zona EEA. I trasferimento fuori dall'EEA devono essere oggetto di un'autorizzazione speciale da parte dell'Autorità nazionale a meno

	che non siano soddisfatte condizioni eccezionali al trasferimento, e cioè: - la persona interessata ha dato il proprio consenso al trasferimento; - il trasferimento di dati è necessario per la conclusione o l'esecuzione di un contratto tra il titolare del trattamento e una parte terza nell'interesse dell'interessato; - il trasferimento è necessario per l'esecuzione di un contratto tra il titolare del trattamento e l'interessato o per l'esecuzione di misure precontrattuali prese su richiesta dell'interessato; - il trasferimento di dati personali è necessario (o richiesto dalla legge) per l'esecuzione di un compito di interesse pubblico o per scopi connessi a procedimenti per via giudiziaria; - il trasferimento è necessario per la protezione di interessi vitali della persona interessata; - il trasferimento è necessario per scopi investigativi e preventivi dell'attività criminale; -i dati personali sono trasferiti a

	partire da un registro pubblico che in base alla legge è aperto alla consultazione pubblica. L'Ispettorato concederà l'autorizzazione posto che il paese destinatario sia tra quelli inclusi nella lista dei paesi affidabili stilata dalla Commissione europea, o comunque garantisca un adeguato livello di protezione legale dei dati attraverso: - clausole contrattuali approvato dalla Commissione Europea; - regole societarie vincolanti; - nel caso di trasferimento dati verso gli Stati Uniti, sottoscrizione dei principi del programma Safe Harbour.
SICUREZZA	I titolari e gli addetti ai trattamenti sono obbligati ad implementare misure tecniche e organizzative appropriate per la protezione dei dati contro distruzione, alterazione, comunicazione accidentale o non autorizzate, così come contro qualsiasi altro trattamento illegale. Queste misure devono assicurare un livello di sicurezza appropriato alla natura dei dati personali. Inoltre, devono essere definite in un documento scritto, in accordo con i requisiti generali previsti dall'Ispettorato.

NOTIFICA DI VIOLAZIONE	I provider di servizi di comunicazione elettronica aperti al pubblico hanno l'obbligo di notificare la violazione dei dati all'Ispettorato senza ritardi ingiustificati. Quando la violazione viola la privacy dell'interessato, il provider deve inviare la notifica di violazione anche all'interessato stesso, eccetto nel caso in cui il provider abbia dimostrato in modo soddisfacente all'Ispettorato di avere applicato misure tecnologiche di protezione appropriate. Altri titolari del trattamento non hanno l'obbligo generale di notificare violazioni della sicurezza dei dati agli interessati o all'Ispettorato. E' consigliabile inviarla come "bona fide" per ridurre la responsabilità civile.
APPLICAZIONE	L'applicazione della legge viene fatta dall'Autorità nazionale che deve supervisionare le attività dei titolari del trattamento al fine di evitare violazioni nel trattamento e garantire la protezione dei diritti dell'interessato. Qualsiasi violazione dei dati comporta una responsabilità amministrativa. Non è prevista alcuna responsabilità penale per la violazione della protezione dei dati.

	L'Ispettorato non ha il potere di imporre pene per la violazione, anche se può evidenziare l'illecito amministrativo, in base al quale le corti nazionali poi possono imporre multe che vanno dai 140 € ai 570 € circa. Queste sanzioni amministrative possono essere applicate solo alle persone fisiche. Se una persona giuridica commette una violazione, i responsabili dell'illecito amministrativo sono o il responsabile del trattamento o l'amministratore delegato. Inoltre, colui che ha subito l'illecito può anche richiedere un risarcimento danni oltre ai danni morali.

LUSSEMBURGO

LEGGE	*La legge per la protezione degli individui relativamente al Trattamento dei Dati Personali è del 02/08/2002. A questa ha fatto seguito la legge del 30/05/2005 che prevede specifiche disposizioni relativamente al trattamento dei dati personali nel settore delle comunicazioni elettroniche.*
DEFINIZIONE DI DATI PERSONALI	*Qualsiasi informazione in qualsiasi formato concernente una persona fisica identificata o identificabile. Una persona fisica può essere identificata direttamente o indirettamente, in particolare con riferimento a un numero di identificazione o uno o più fattori specifici della sua identità fisica, fisiologica, genetica, mentale, culturale, sociale o economica.*
DEFINIZIONE DI DATI PERSONALI SENSIBILI	*Dati relativi all'origine etnica o razziale, opinioni politiche, credo religioso o filosofico, appartenenza sindacale, salute o vita sessuale, dati genetici.*
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Commission Nationale pour la Protection des Données ("CNPD")
NOTIFICAZIONE DEL TRATTAMENTO	**Notificazione preventiva al CNDP** *I trattamento dei dati deve es-*

	sere notificato al CNPD in anticipo. Le notifiche devono contenere le informazioni di cui all'art.13 della legge e sono effettive nel momento in cui sono completate e firmate. L'art. 13 della legge prevede 14 casi specifici eccezionali per i quali non sussiste l'obbligo di notifica che si aggiungono alle eccezioni generali di cui all'art. 12 par. 2. **Autorizzazione preventiva del CNDP** I trattamenti che presentano maggiori rischi per il rispetto dei diritti e delle libertà individuali devono essere preventivamente autorizzati dal CNPD. I trattamenti soggetti a tale obbligo sono elencati all'art. 14 della legge, tra questi, per esempio, i trattamenti dei dati biometrici. Genericamente, l'autorizzazione del CNDP è richiesta prima dell'utilizzo di mezzo tecnici per il controllo delle persone con registrazione dei dati, in particolare videocamere, tracciati elettronici, ecc. Qualora i dati raccolti non vengano registrati è sufficiente la notifica.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Il titolare del trattamento può nominare un DPO. Questa nomina solleva il titolare del tratta-

	mento dall'obbligo di notifica del trattamento, ma non dall'obbligo di richiedere l'autorizzazione preventiva dove prevista. Il DPO deve verificare che i trattamenti siano conformi alle disposizioni di legge e ha il diritto ad essere informato e ad informare il titolare del trattamento circa le formalità da svolgere in conformità alle disposizioni di legge e regolamentari.
RACCOLTA E TRATTAMENTO DEI DATI	Il titolare deve assicurare che i trattamenti si svolgano secondo i principi di legalità e trasparenza. Questo significa che: - i dati devono essere raccolti per scopi specifici, espliciti e legittimi e possono essere utilizzati unicamente per questi scopi; - la raccolta, la notificazione del trattamento e l'uso dei dati personali è strettamente limitata a ciò che è necessario per la realizzazione degli obiettivi specificamente dichiarati in anticipo da parte dell'autorità, l'agenzia, la compagnia, l'associazione, il professionista, ecc.; - il trattamento deve essere adeguato e non eccessivo in relazione agli scopi per cui i dati sono stati raccolti;

	- il trattamento dei dati personali è limitato ai casi in cui c'è una connessione diretta con lo scopo iniziale del trattamento e i dati che permetto l'identificazione dei soggetti sono conservati per un periodo limitato di tempo; - occorre aggiornare i dati raccolti affinché siano corretti, poiché un'informazione incompleta e non vera può danneggiare l'interessato. In caso contrario i dati devono essere rettificati o cancellati. La legge protegge anche i soggetti contro qualsiasi decisione negativa automaticamente presa da un computer senza che la persona interessata possa fornire la propria visione dei fatti; Il trattamento dei dati è permesso solo se c'è una ragione legittima che lo giustifichi. I dati possono essere trattati solo per: - adempiere un obbligo legale a cui è soggetto il titolare del trattamento; - l'esecuzione di un compito di interesse pubblico; - l'esecuzione di un contratto di cui la persona interessata è parte;

	- perseguire un interesse legittimo del titolare del trattamento o di terzi a cui i dati sono stati comunicati, a condizione che non prevalgano l'interesse, i diritti e le libertà fondamentali della persona interessata; - per proteggere gli interessi vitali dell'interessato. Il trattamento di dati sensibili è proibito e può essere permesso esclusivamente in circostanze particolarmente eccezionali. L'art. 10 elenca una serie di condizioni che regolano il trattamento dei dati a scopo di supervisione all'interno di luoghi accessibili o non accessibili al pubblico. Questo tipo di trattamento è legittimo per la prevenzione di incidenti, quando vi sia un rischio per la sicurezza degli utenti, ma anche quando c'è il rischio di vandalismo o furto. Il CNPD valuterà i criteri di necessità e proporzionalità caso per caso. Generalmente la legge permette il trattamento a scopi di supervisione: - se l'interessato ha fornito il proprio consenso; - in luoghi che non essendo di proprietà privata siano rischiosi

	per gli utenti a causa della propria natura, posizione, configurazione o frequentazione; - in luoghi privati quando la persona fisica o legale residente è il titolare del trattamento; - per permettere alle autorità legali competenti di registrare reato penale o intraprendere un'azione legale. La supervisione sul luogo di lavoro è possibile solo in certe circostanze: - per la sicurezza e la salute degli impiegati; - per proteggere la proprietà della compagnia; - per controllare il processo produttivo in relazione ai soli macchinari; - per controllare per periodi di tempo definiti la produzione o i l'attività dei lavoratori se si ritiene che tale misura sia l'unico modo per determinare i guadagni esatti; - in connessione con l'organizzazione del lavoro sotto uno schema di orari flessibili in accordo con la legge che tutela i lavoratori.

	Il soggetto interessato deve essere informato preventivamente dei trattamenti che lo riguardano. Il consenso dell'interessato al trattamento, non rende quest'ultimo legittimo.
TRASFERIMENTO DEI DATI	I dati possono essere trasferiti a un paese terzo se quest'ultimo assicura un adeguato livello di protezione e le disposizioni di legge sulla protezione dei dati sono rispettate. L'adeguatezza del livello di protezione deve essere stimata dal titolare del trattamento alla luce delle circostanze in cui vengono svolte le operazioni di trasferimento, in particolare, devono essere tenuti in considerazione la natura dei dati, lo scopo e la durata delle operazioni. In caso di dubbio il titolare del trattamento informerà immediatamente il CNPD il quale considererà se il livello di protezione nel paese terzo è adeguato. Il trasferimento di dati a paesi terzi che non offrono un adeguato livello di protezione può avere luogo se: - l'interessato ha dato il proprio consenso al trasferimento; - il trasferimento è necessario per l'esecuzione di un contrat-

	to concluso tra il titolare del trattamento e una parte terza nell'interesse dell'interessato; - il trasferimento è necessario o previsto dalla legge per l'esecuzione di compiti di interesse pubblico o per costatare, esercitare o difendere un diritto per via giudiziaria; - il trasferimento è necessario per un registro pubblico. Il CNDP può autorizzare un trasferimento di dati a paesi terzi che non offrano un adeguato livello di protezione se il titolare del trattamento offre sufficienti garanzie rispetto alla protezione della privacy, delle libertà e dei diritti fondamentali dell'interessato.
SICUREZZA	Il titolare del trattamento deve attuare tutte le misure tecniche e organizzative appropriate per assicurare la protezione dei dati trattati contro la distruzione accidentale o illegale, la perdita accidentale, la falsificazione, la diffusione non autorizzata, in particolare quando sono coinvolte le trasmissioni di dati attraverso una rete. Attualmente la legge prevede che qualora il CNPD lo richieda, deve essere fornita una descrizione di que-

	ste misure entro 15 giorni. Se il trattamento è gestito a nome del titolare del trattamento, quest'ultimo deve scegliere un addetto che fornisca garanzie sufficienti. Qualsiasi trattamento gestito a nome di qualcun altro deve essere amministrato da un contratto scritto che leghi l'addetto al titolare del trattamento.
NOTIFICA DI VIOLAZIONE	Chiunque effettui un trattamento in violazione di un'autorizzazione preventiva sarà ritenuto responsabile e condannato ad un periodo di reclusione che può andare dagli 8 giorni a 1 anno e ad una multa tra i 251 € e i 125 000 €.
APPLICAZIONE	Nel caso in cui un trattamento violi la legge, il CNDP, la procura o la parte lesa può richiedere la conclusione del trattamento stesso, punibile attraverso l'applicazione di sanzioni amministrative e/o penali.

MALTA

LEGGE	La legge di riferimento è il Data Protection Act (Capitolo 440 Laws of Malta) e i successivi regolamenti emessi.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Qualsiasi informazione relativa a una persona fisica identificata o identificabile direttamente o indirettamente, in particolare con riferimento ad un numero di identificazione o a uno o più fattori specifici della sua identità fisica, fisiologica, mentale, economica, culturale o sociale.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Office of the Data Protection Commissioner
NOTIFICAZIONE DEL TRATTAMENTO	Generalmente, i titolari del trattamento devono inviare una notifica al Commissario prima di avviare trattamenti totalmente o parzialmente automatizzati definendone gli scopi, salvo i casi eccezionali previsti dal Commissario nella legge e nei regolamenti. Il Commissario tiene un Registro di queste operazioni in cui sono contenute le seguenti informazioni: - nome e indirizzo del titolare del trattamento o di qualsiasi altra persona che agisca in suo nome; - scopo del trattamento;

	- descrizione della/e categoria/e dei soggetti dei dati e dei dati; - destinatari o categorie di destinatari dei dati; - proposte di trasferimento di dati a paesi terzi.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	La legge non prevede l'obbligo di nominare il DPO. Tuttavia, il titolare del trattamento notifica al Commissario la sua nomina o destituzione. Il DPO ha, tra le altre, la funzione di assicurare che il titolare del trattamento tratti i dati in modo corretto e legale.
RACCOLTA E TRATTAMENTO DEI DATI	I dati possono essere trattati solo se: - l'interessato ha fornito il proprio consenso esplicito; - il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte; - il trattamento è necessario per proteggere un interesse vitale dell'interessato; - il trattamento è necessario per lo svolgimento di un'attività di pubblico interesse; - il trattamento è necessario per tutelare un interesse legittimo del titolare del trattamento o di una parte terza a cui sono forniti i dati, a condizione che non

	prevalgano l'interesse, i diritti e le libertà fondamentali dell'interessato, con particolare riferimento al diritto alla privacy. Se l'interessato comunica al titolare del trattamento il proprio rifiuto, i dati personali non possono essere trattati a scopo di pubblicità diretta. Come regola generale, i dati personali sensibili non possono essere trattati, tranne i casi previsti dalla legge. L'interessato ha il diritto di ricevere, dal titolare del trattamento o da un suo rappresentante, le informazioni relative al titolare del trattamento (identità, residenza abituale o sede del luogo di lavoro); scopo del trattamento e qualsiasi informazione ulteriore come ad es. i destinatari dei dati; il diritto di accesso, di rettifica e di cancellazione dei dati. Il titolare del trattamento deve garantire che il trattamento avvenga correttamente nel rispetto dell'interessato.
TRASFERIMENTO DEI DATI	Il titolare del trattamento deve notificare all'Autorità nazionale qualsiasi proposta di trasferimento a paesi terzi, cioè che non sono parte della UE. Il trasferimento verso tali paesi può

	avvenire solo se l'Autorità nazionale ritiene che garantiscano un adeguato livello di protezione. Qualora il livello di protezione non venga ritenuto adeguato, il trasferimento di dati a un paese terzo può essere comunque effettuato, ma solo nel caso in cui l'interessato dia il proprio esplicito consenso oppure se il trasferimento: - è necessario per l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; - è necessario per l'esecuzione di un contratto concluso o da concludersi tra il titolare del trattamento e una terza parte a favore del soggetto interessato; - è necessario o previsto per legge per perseguire interessi pubblici o per costatare, esercitare o difendere un diritto per via giudiziaria; - è necessario per proteggere gli interessi vitali dell'interessato; - avviene a partire da un registro pubblico di informazioni che può essere consultato da chiunque possa dimostrare un interesse legittimo.

	In questi casi l'approvazione del Commissario non è richiesta ma il trasferimento deve essere comunque notificato. Verso i paesi terzi che non assicurano un adeguato livello di protezione, il Commissario può autorizzare il trasferimento di dati, a condizione che il titolare del trattamento garantisca adeguate misure di protezione della privacy e dei diritti umani fondamentali. Il Ministro per la libertà di informazione e la protezione dei dati può, al fine di dare attuazione a convenzioni internazionali, individuare, attraverso un suo atto, i paesi verso cui è possibile trasferire i dati per i quali non sono ammesse restrizioni. Oltre alla notificazione del Commissario, non sono previste ulteriori formalità in caso di trasferimento di dati personali verso: - stati membri UE/EEA - paesi terzi che la Commissione UE ritiene assicurino un adeguato livello di protezione; - organizzazioni che hanno aderito al Programma US Safe Harbor.

SICUREZZA	I titolari del trattamento devono adottare appropriate misure tecniche e organizzative per proteggere i dati personali trattati contro la distruzione o perdita accidentale o forme illegali di trattamento. Un adeguato livello di sicurezza deve tenere in considerazione: - le possibilità tecniche disponibili; - i costi di implementazione delle misure di sicurezza; - i rischi speciali che esistono nel trattamento dei dati personali; - la sensibilità dei dati trattati. Il titolare del trattamento deve assicurarsi che l'addetto al trattamento sia in grado di implementare le necessarie misure di sicurezza.
NOTIFICA DI VIOLAZIONE	In caso di violazione dei dati personali, il provider di servizi di comunicazione elettronica ha l'obbligo di notificare la violazione al Commissario senza alcun indugio. Se la violazione riguarda dati personali o la privacy delle persone, il provider ha l'obbligo di notificare immediatamente anche i soggetti coinvolti. La notifica deve includere almeno: la natura della

	violazione e i punti di contatto presso cui è possibile ottenere maggiori informazioni. I provider di servizi devono inoltre tenere un registro delle varie violazioni.
APPLICAZIONE	In base alla legge, chiunque si sottragga ad una inchiesta da parte del Commissario è considerato colpevole. Nel caso in cui il Commissario ritenga che un trattamento sia illegale, può ordinare al titolare del trattamento di rettificare o cancellare i dati; nel caso di reiterazione il Commissario può proibire il trattamento stesso. Il titolare del trattamento ha diritto di ricorrere in appello dinanzi alla Corte. In caso di omissione delle misure di sicurezza, il Commissario può imporre sanzioni pecuniarie. La parte lesa può avanzare una richiesta danni contro il titolare del trattamento. Inoltre, chiunque fornisca informazioni false agli interessati, o invii false notifiche al Commissarioo, in generale, violi le disposizioni di legge, è ritenuto responsabile del reato commesso per il quale è prevista o una multa non superiore ai 23.293,73 € o 6 mesi di carcerazione, o entrambe le pene.

PAESI BASSI

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita il 1 settembre 2001 con il Dutch Personal Data Protection Act (WBP). L'applicazione spetta al Dutch Data Protection Authority.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi dato relativo a una persona fisica identificata o identificabile.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati relativi alla vita religiosa o filosofica di una persona, razza, fede politica, salute e vita sessuale, appartenenza sindacale, fedina penale, condotta illegale.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	College Bescherming Persoonsgegevens (CBP)
NOTIFICAZIONE DEL TRATTAMENTO	Normalmente, i titolari che trattano dati attraverso mezzi automatici devono inviare una notifica al CBP in modo che il trattamento sia registrato e reso pubblico. Anche le successive modifiche devono essere notificate in modo da rettificare i dati personali. La notifica deve includere le seguenti informazioni: - nome e indirizzo del titolare del trattamento; - scopi del trattamento;

	- soggetti dei dati o categorie dei soggetti: - dati o categorie di dati; - destinatari o categorie di destinatari; - proposte di trasferimenti di dati personali ai paesi fuori dall'UE; - una descrizione generale delle misure di sicurezza che il titolare del trattamento ha intenzione di adottare. Nel caso in cui il titolare del trattamento modifichi in maniera sostanziale una delle seguenti informazioni: - lo scopo del trattamento; - le informazioni relative all'interessato o ai destinatari, o alle rispettive categorie; - le misure di sicurezza; - il paese a cui si intende inviare i dati, se non appartenente all'UE; -entro un anno dalla notifica precedente, deve notificare tali cambiamenti. Inoltre, qualsiasi modifica al nome o indirizzo del titolare del trattamento deve essere notificata alla Commissione entro

	una settimana.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Non vi è l'obbligo di nominare all'interno delle organizzazioni il DPO.
RACCOLTA E TRATTAMENTO DEI DATI	La raccolta dati deve essere effettuata per uno scopo specifico, esplicito, legittimo. Il trattamento può essere effettuato se: - l'interessato ha dato il proprio consenso preventivo ed esplicito; - il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte; - il trattamento è necessario affinché il titolare del trattamento rispetti un obbligo legale; - il trasferimento è necessario per proteggere gli interessi vitali dell'interessato; - il trasferimento è necessario o richiesto dalla legge per proteggere un importante interesse pubblico; - il trattamento è necessario per il perseguimento degli interessi legittimi del titolare del trattamento o di una parte terza a cui i dati sono comunicati, a condizione che non prevalgano l'interesse, i diritti e le libertà fon-

	damentali dell'interessato. Inoltre, i dati personali non possono essere ulteriormente trattati per scopi incompatibili rispetto a quelli per cui sono stati raccolti. L'incompatibilità va valutata sulla base delle seguenti circostanze: - la relazione tra lo scopo per il quale i dati sono stati raccolti e lo scopo dell'ulteriore trattamento; - la natura dei dati; - le conseguenze dell'ulteriore trattamento sull'interessato; - il modo in cui i dati sono stati ottenuti; - le garanzie date all'interessato. Infine il WBP pone delle regole particolarmente rigide per quanto riguarda i dati sensibili. La regola generale è che non è possibile trattare tali dati, a meno che l'interessato non abbia dato il proprio consenso esplicito.
TRASFERIMENTO DEI DATI	Il trasferimento di dati a paesi non UE/EEA è permesso qualora sia garantita una protezione adeguata. Per il trasferimento verso gli Stati Uniti, solo le compagnie che aderiscono al

	programma US/UE Safe Harbor sono considerate come destinatari che offrono protezione adeguata. I titolari del trattamento possono trasferire dati personali anche a paesi non EEA che non offrono una protezione adeguata, qualora venga rispettata una delle seguenti condizioni: - il soggetto dei dati ha dato il proprio consenso esplicito e univoco; - il trasferimento è necessario per l'esecuzione di un contratto tra il titolare del trattamento e l'interessato; - il trasferimento è necessario per l'esecuzione di un compito di interesse pubblico o per costatare, esercitare, difendere un diritto per via giudiziaria; - il trasferimento è basato su una delle Clausole Modello di cui all'art. 26(4) della direttiva 95/46/EC; - il Ministro di Giustizia emette specifico permesso, dopo consultazione con il CBP.
SICUREZZA	I titolari e gli addetti al trattamento devono adottare appropriate misure tecniche e or-

	ganizzative per proteggere i dati personali contro la distruzione accidentale o illegale o contro la perdita accidentale, l'alterazione o l'accesso non autorizzato.
NOTIFICA DI VIOLAZIONE	In caso di violazione, le legge non prevede un obbligo di notifica.
APPLICAZIONE	In caso di violazioni, il CBP può imporre sanzioni di tipo sia amministrativo, sia penale.

POLONIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita con il Personal Data Protection Act del 29 agosto 1997 e successive modifiche.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione relativa a una persona fisica identificata o identificabile direttamente o indirettamente, in particolare in riferimento a un numero di identificazione o a uno o più fattori specifici della sua identità fisica, fisiologica, mentale, economica, culturale o sociale.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati che rivelano l'origine razziale o etnica, le opinioni politiche, il credo religioso o filosofico, l'appartenenza sindacale, la salute, il codice genetico, le dipendenze, la vita sessuale, multe amministrative o procedimenti penali.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	General Inspector of Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych)
NOTIFICAZIONE DEL TRATTAMENTO	Generalmente, i titolari del trattamento devono comunicare all'autorità nazionale i sistemi di archiviazione dei dati trattati. Presso l'Autorità è conservato un registro dei titolari e dei

	sistemi di archiviazione accessibile al pubblico . Non c'è l'obbligo di registrare i sistemi di archiviazione qualora i titolari trattino dati che: - includono informazioni confidenziali; - sono stati raccolti come risultati di inchieste condotte da funzionari di enti autorizzati; - sono trattati da enti aventi competenze giurisdizionali sulla base delle disposizioni del Registro Penale Nazionale; - sono trattati dall'Ispettore Generale di Informazione Finanziaria; - sono trattati da enti aventi competenze sulla partecipazione della Polonia al Schengen Information System e al Visa Information System; - sono trattati da enti sulla base di leggi che regolano lo scambio di informazioni con organi esecutivi dei paesi UE; - si riferiscono a membri di chiese o altre associazioni religiose legalmente riconosciute e sono trattati per gli scopi riferibili alle loro attività di culto;

	- sono trattati per l'adempimento di obblighi lavorativi del titolare del trattamento; - si riferiscono a persone che usufruiscono di servizi sanitari, notarili, legali o di controllo, di consulenti fiscali e di brevetti; - sono creati sulla base di regole elettorali riguardanti la Camera Bassa del Parlamento Polacco, il Senato, il Parlamento Europeo, i consigli comunali, i consigli distrettuali e provinciali, il Presidente della Repubblica di Polonia, i sindaci, gli atti su referendum nazionali e municipali; - si riferiscono a persone private della libertà per motivi detentivi; - sono trattati per l'emissione di documenti contabili o per attività contabile; - sono disponibili al pubblico; - sono trattati nella preparazione di una tesi per conferire un diploma universitario; - sono trattati nell'attività quotidiana. Il titolare del trattamento può cominciare il trattamento dei dati dopo la notifica all'Autorità nazionale, a meno che il titolare

	del trattamento sia esentato da questo obbligo. La notifica deve includere, in particolare, le seguenti informazioni: - identità del titolare del trattamento e del processore di dati; - la base legale per il trattamento; - lo scopo del trattamento; - una descrizione delle categorie di soggetti; - i mezzi con cui vengono raccolti e comunicati i dati; - una descrizione delle misure tecniche e organizzative adottate; - possibile trasferimento a un paese terzo.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Il titolare del trattamento è obbligato a nominare un amministratore per la sicurezza delle informazioni che deve verificare la conformità delle misure di sicurezza applicate al fine di proteggere i dati personali da trattamenti o divulgazione non autorizzati, perdita, cambiamento, danno o distruzione.
RACCOLTA E TRATTAMENTO DEI DATI	Il trattamento è permesso solo se: - il soggetto dei dati ha dato il proprio consenso, a meno che

	il trattamento non consista nella cancellazione dei dati personali; - è necessario per adempiere un obbligo legale; - è necessario per l'esecuzione di un contratto di cui l'interessato è parte; - è necessario per l'esecuzione di un compito di interesse pubblico; - è necessario per il perseguimento dell'interesse legittimo del titolare del trattamento o dei terzi a cui i dati vengono comunicati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali dell'interessato. Quando sono trattati dati sensibili, deve essere soddisfatta almeno una delle seguenti condizioni: - il soggetto dei dati ha dato il proprio consenso, a meno che il trattamento consista nella cancellazione dei dati personali; - vi siano disposizioni specifiche di legge che permettono il trattamento di tali dati senza il consenso dell'interessato, a patto che vengano garantite prote-

	zioni adeguate; - il trattamento è necessario per proteggere gli interessi vitali dell'interessato, o di un'altra persona, qualora l'interessato sia fisicamente o legalmente incapace di dare il proprio consenso fino al momento in cui viene nominato un curatore; - il trattamento è necessario per realizzare gli obiettivi contenuti negli statuti di chiese e altre unioni religiose, associazioni, fondazioni e altre organizzazioni no profit o istituzioni con scopi politici, scientifici, religiosi, filosofici o sindacali, premesso che il trattamento riguardi solo i membri di tali organizzazione o persone che hanno un contatto regolare con loro, in connessione alla loro attività; - il trattamento è necessario per adire le vie legali; - il trattamento è necessario in quanto rientra tra gli obblighi del titolare e dei suoi impiegati nell'ambito del diritto del lavoro; - il trattamento è richiesto per gli scopi di medicina preventiva, cure e trattamenti, in cui i dati sono trattati da un profes-

	sionista del settore; - il trattamento riguarda dati che sono resi pubblici dall'interessato stesso; - è necessario per condurre ricerche scientifiche (anche tesi universitarie); - il trattamento è necessario in quanto derivante da provvedimenti giurisdizionali o amministrativi; Il titolare del trattamento è obbligato a fornire all'interessato le seguenti informazioni: identità del titolare del trattamento, scopo della raccolta dei dati, destinatari o categorie dei destinatari dei dati, l'esistenza del diritto di accesso ai dati e della loro rettifica da parte dell'interessato. Deve fornire ulteriori informazioni nel caso in cui i dati personali non sono stati ottenuti direttamente dal soggetto dei dati stessi.
TRASFERIMENTO DEI DATI	Il trasferimento dei dati a paesi terzi fuori dall'EEA può avere luogo solo se il paese di destinazione assicura un adeguato livello di protezione dei dati. Quest'ultimo è valutato tenendo conto di tutte le circostanze del caso, in particolare la natura dei dati, lo scopo e la durata

	delle operazioni di trattamento, il paese di origine e quello di destinazione finale, le leggi applicabili nel paese terzo, le misure di sicurezza e la condotta del business. Tuttavia, il titolare del trattamento dei dati può trasferire i dati personali a un paese terzo se: -l'interessato ha fornito il proprio consenso per iscritto; - il trasferimento è necessario per l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; - il trasferimento è necessario per l'esecuzione di un contratto concluso nell'interesse dell'interessato tra il titolare del trattamento e una parte terza; - il trasferimento è necessario o richiesto l'esecuzione di un compito di interesse pubblico o per costatare, esercitare o difendere un diritto per via giudiziaria; - il trasferimento è necessario per proteggere gli interessi vitali dell'interessato; - il trasferimento si riferisce a dati che sono disponibili al pubblico.

	In altri casi, il trasferimento a paesi terzi che non assicurino un adeguato livello di protezione può aver luogo solo previo consenso dell'Autorità nazionale, premesso che il titolare del trattamento assicuri il rispetto alla protezione della privacy, dei diritti e delle libertà dell'interessato. Per il trasferimento verso gli USA, il rispetto di quanto previsto nel US/UE Safe Harbor soddisfa i requisiti del PDPA e quindi non è richiesto il consenso dell'Autorità nazionale. Il trasferimento di dati personali è consentito anche quando è richiesto da disposizioni legali o da accordi internazionali ratificati che garantiscono un adeguato livello di protezione.
SICUREZZA	Il titolare del trattamento è obbligato ad adottare le misure tecniche e organizzative necessarie per proteggere i dati trattati, in relazione ai rischi e alla categoria dei dati protetti, e per proteggere i dati contro la divulgazione non autorizzata, la modifica, perdita, danneggiamento o distruzione dei dati. In particolare il titolare del trattamento deve:

	- tenere la documentazione che descrive il modo in cui i dati vengono trattati e le misure di sicurezza; - nominare un amministratore per la sicurezza delle informazioni, che supervisioni l'adempimento alle misure di sicurezza; - autorizzare gli incaricati al trattamento dei dati; - assicurare un controllo sul tipo di dati, sulla durata del trattamento, sull'identità degli addetti al trattamento e dei destinatari; - tenere un registro di persone autorizzate al trattamento dei dati. Il livello delle misure di sicurezza dipende dalla categoria dei dati: 1) livello base: non sono trattati dati sensibili e nessuno dei mezzi usati dal sistema è connesso con una rete pubblica (ad es. internet); 2) livello medio: sono trattati dati sensibili; 3) livello alto: quando almeno uno dei mezzi usati dal sistema è connesso con la rete pubblica.

NOTIFICA DI VIOLAZIONE	Il PDPA non prevede un obbligo di notifica. Tuttavia, in base al Codice di Procedura Penale Polacco, in caso di reato c'è il dovere civico di informare il Procuratore di Stato o la Polizia.
APPLICAZIONE	L'Autorità nazionale è responsabile dell'esecuzione del PDPA. In caso di violazione, l'Autorità (ex officio o sulla base di una mozione presentata) ordina di ristabilire il rispetto della legge. Il mancato adempimento alla decisione è soggetto a multe fino a circa 50.000 €. Inoltre, il non adempimento al PDPA può configurarsi come reato penale. Qualora il rappresentante legale del titolare del trattamento (ad es. un membro del consiglio d'amministrazione) venga ritenuto responsabile di un tale reato, può essere soggetto ad una multa (da circa 25€ a circa 270.000€), ad una restrizione parziale della libertà o alla reclusione fino a un massimo di 3 anni.

PORTOGALLO

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita con la legge sulla protezione dei dati n. 67/98 del 26 ottobre 1998.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione, in qualsiasi formato (anche sonoro e visivo) relativa a una persona fisica identificata o identificabile direttamente o indirettamente, in particolare con riferimento a uno specifico numero o a uno o più elementi riguardanti la sua identità fisica, fisiologica, mentale, economica, culturale o sociale.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Qualsiasi dato personale che riveli il credo filosofico o politico, appartenenza sindacale, religione, vita privata, origine etnica o razziale, salute, vita sessuale, dati genetici.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Comissão Nacional de Protecção de Dados (CNPD)
NOTIFICAZIONE DEL TRATTAMENTO	Il titolare del trattamento deve notificare al CNPD i trattamenti, salvo i casi in cui siano previste eccezioni. Qualsiasi variazione o modifica dei dati comporta un emendamento della notificazione. Il CNPD ha un formulario ufficiale che deve essere compilato in portoghese con le seguenti

	informazioni: - identità del titolare del trattamento e del suo rappresentante; - principali caratteristiche del software; - scopi del trattamento; - eventuali enti terzi responsabili del trattamento; - qualsiasi dato personale che sarà raccolto in ciascun registro (specificare se si tratta di dati sensibili); - presupposti legali per la raccolta dati e breve descrizione dei metodi usati; - mezzi e metodi disponibili per l'aggiornamento dei dati; - mezzi di comunicazione a altri enti; - eventuale trasferimento dei dati a paesi terzi, motivi, presupposti legali e misure di sicurezza adottate nel trasferimento.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Non vi è l'obbligo di nominare all'interno delle organizzazioni il DPO.
RACCOLTA E TRATTAMENTO DEI DATI	I dati personali possono essere trattati se l'interessato ha dato il proprio consenso esplicito o se il trattamento è ritenuto neces-

	sario per: - l'esecuzione di un accordo di cui l'interessato è parte; - per l'adempimento da parte del titolare di un obbligo legale; - proteggere gli interessi vitali dell'interessato qualora sia fisicamente o legalmente incapace di dare il proprio consenso; - l'esecuzione di un compito di interesse pubblico, o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati; - perseguire gli interessi legittimi del titolare del trattamento o di una parte terza a cui sono divulgati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata. Inoltre, il titolare del trattamento deve fornire all'interessato tutte le informazioni sulle operazioni di trattamento, incluse l'identità del titolare e gli scopi del trattamento, oltre ai diritti che può esercitare per accedere, emendare e cancellare i dati.

TRASFERIMENTO DEI DATI	Per i trasferimenti di dati all'interno dello spazio UE/EEA, è richiesta solo la notifica al CNPD. I trasferimenti a paesi non UE/EEA possono aver luogo se il paese destinatario assicura un adeguato livello di protezione. In qualsiasi caso è obbligatorio avviare una procedura di autorizzazione con il CNPD. Eccezionalmente, i trasferimenti possono essere attuati secondo lo standard delle Clausole Modello o, per gli Stati Uniti, secondo i principi del programma Safe Harbor.
SICUREZZA	Il titolare del trattamento deve adottare le misure tecniche e organizzative necessarie per proteggere i dati contro la distruzione o la perdita accidentale o illegale, l'alterazione o l'accesso non autorizzato, in particolare quando il trattamento è fatto con la trasmissione di dati in rete. L'adeguatezza di tali misure è valutata in relazione allo stato dell'arte, ai costi di implementazione, alla natura dei dati e agli scopi del trattamento.

NOTIFICA DI VIOLAZIONE	La legge non prevede un obbligo di notifica in caso di violazione.
APPLICAZIONE	In Portogallo, il CNPD è responsabile dell'applicazione della legge sulla protezione dei dati personali. In caso di violazione della legge vi possono essere sanzioni amministrative o penali. L'art. 43 della legge prevede pene di tipo pecuniario o la reclusione a carico di chi intenzionalmente: - non invia la notifica al CNPD o non richiede l'autorizzazione se prevista; - inserisce informazioni false nella notifica o nella richiesta di autorizzazione; - utilizza i dati personali in modo incompatibile con gli scopi per cui sono stati raccolti; - promuove una combinazione illegale di dati; - non adempie agli obblighi di legge; - continua a permettere l'accesso alle reti di trasmissione dei dati a titolari che non rispettano le disposizioni di legge. In caso di inadempimento, i trasgressori sono punibili con san-

	zioni pecuniarie di importo variabile rispetto alla loro natura legale: le persone fisiche possono essere punite con una multa tra 250 € e 2500 €; le persone giuridiche invece con una multa tra 1500 € e i 15000 €. Nei casi di non conformità relativi alle condizioni e alla sicurezza del trattamento dei dati e/o alle informazioni fornite all'interessato, sono previste multe tra i 500 e i 5000 €.

REGNO UNITO

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita nel marzo del 2000. L'applicazione spetta all'Ufficio del Commissario per l'Informazione (ICO).
DEFINIZIONE DI DATI PERSONALI	Dati relativi a individui che possono essere identificati grazie ai dati o altre informazioni che sono in possesso del titolare del trattamento.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Informazioni che rivelano l'origine etnica o razziale, le opinioni politiche, il credo religioso o simili, l'appartenenza sindacale, la salute fisica o mentale, la vita sessuale e condanne penali.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Information Commissioner's Office (ICO)
NOTIFICAZIONE DEL TRATTAMENTO	I titolari del trattamento devono notificare al Commissario i trattamenti in modo che possano essere registrati e resi pubblici. La notifica deve specificare la natura dei dati e il motivo per cui sono stati raccolti, le categorie degli interessati e se tali dati saranno trasferiti all'interno o all'esterno della EEA.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Le organizzazioni non hanno l'obbligo di nominare al loro interno il DPO.

RACCOLTA E TRATTAMENTO DEI DATI	I responsabili possono raccogliere e trattare i dati personali quando una delle seguenti condizioni è rispettata: - l'interessato dà il proprio consenso; - il titolare del trattamento ha bisogno di trattare i dati per portare a termine un contratto in cui l'interessato è parte; - il trattamento consente al titolare del trattamento di assolvere ai propri gli obblighi legali; - il trattamento protegge gli interessi vitali del titolare del trattamento; - il trattamento è richiesto per legge o dalla Corona o dal governo; -il trattamento è richiesto per motivi di pubblico interesse o per amministrare la giustizia; - il titolare del trattamento ha una ragione legittima per il trattamento, eccetto quando il trattamento danneggia i diritti dell'interessato, le libertà o gli interessi legittimi. In caso di trattamento di dati personali sensibili, oltre alle condizioni sopra elencate, deve

	essere rispettato un elenco di ulteriori condizioni più rigorose. In ogni caso il titolare del trattamento deve fornire all'interessato tutte le informazioni sul trattamento, incluse l'identità del titolare del trattamento, gli scopi del trattamento e le circostanze in cui vengono fatte le operazioni.
TRASFERIMENTO DEI DATI	I responsabili possono trasferire dati fuori dall'EEA se una delle seguenti condizioni è rispettata: - l'interessato dà il proprio consenso; - il trasferimento è essenziale per un contratto di cui l'interessato è parte; - il trasferimento è necessario per eseguire o concludere un contratto tra il titolare del trattamento e una parte terza nell'interesse del soggetto dei dati; - il trasferimento è legalmente richiesto o essenziale per un importante interesse pubblico; - il trasferimento protegge gli interessi vitali dell'interessato; - i dati sono pubblici. I trasferimenti di dati fuori dall'EEA sono consentiri qualora sia garantita una protezione

	adeguata per la sicurezza dei dati, o se il trasferimento è coperto da clausole contrattuali standard approvate dalla Commissione Europea, o soggetto alle Binding Corporate Rules di un'organizzazione. L'uso di clausole contrattuali standard non comporta obblighi di notifica a ICO. Per trasferimenti agli USA si fa riferimento allo US/UE Safe Harbor Principles.
SICUREZZA	I responsabili devono adottare misure tecniche e organizzative appropriate contro il trattamento non autorizzato o illegale e contro la perdita, la distruzione o il danneggiamento dei dati. La legge non specifica quali particolari misure di sicurezza bisogna adottare e implementare, tuttavia l'Information Commissioner's Office suggerisce che le organizzazioni adottino le migliori metodologie come, ad esempio, la norma ISO 27001.
NOTIFICA DI VIOLAZIONE	La legge non prescrive alcun obbligo di notifica all'Autorità nazionale e/o agli interessati in caso di violazione o perdita di dati personali. Tuttavia, qualora la violazione coinvolga molte persone o possa avere conseguenze molto gravi, l'Autorità

	nazionale dispone l'obbligo di notifica. Inoltre, sulla base dei Regolamenti del 2003 su "Privacy e Comunicazioni Elettroniche" (PEC Regulations), i fornitori di servizi di comunicazione elettronica pubblica hanno l'obbligo di notificare all'Autorità nazionale qualsiasi violazione dei dati personali. La mancata notifica può comportare una multa di circa 1000 sterline oltre a pubblicità negativa.
APPLICAZIONE	Responsabile dell'applicazione della legge è l'Autorità nazionale ICO che, dal 2010, può imporre multe fino a 500.000 sterline in caso di violazione dei principi legislativi che regolano la protezione dei dati. Inoltre in caso di violazione delle norme sul trattamento dei dati personali, il Commissario può, con atto esecutivo, imporre al titolare del trattamento la rettifica della propria posizione. Il mancato adempimento costituisce reato penale e può essere punito o dalla Magistrates' Court con multe fino a 5000 sterline, o dalla Crown Court con multe illimitate.

REPUBBLICA SLOVACCA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita nel settembre 2002, con la legge N. 428/2002 (Data Protection Act - DPA). L'applicazione è di competenza del Data Protection Office.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione relativa a una persona fisica identificata o identificabile, direttamente o indirettamente, in particolare in riferimento a uno o più fattori specifici della sua identità fisica, fisiologica, psichica, mentale, economica, culturale o sociale.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	L'Autorità nazionale per la protezione dei dati non dà una definizione. Tuttavia, in una delle disposizioni dell'Autorità nazionale si fa riferimento a "categorie speciali di dati" riferendosi ai dati relativi a razza, etnia, opinioni politiche, credo religioso, dati su reati civili e penali, dati biometrici e di salute mentale.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Data Protection Office of the Slovak Republic: Úrad na ochranu osobných údajov Slovenskej republiky
NOTIFICAZIONE DEL TRATTAMENTO	La legge prevede i casi in cui il titolare del trattamento ha l'obbligo di registrare i sistemi di informazione attraverso i quali

	tratta i dati personali in modo automatico. La registrazione va fatta presso l'Ufficio per la protezione dei dati che gestisce la notificazione del trattamento gratuitamente, assegna un numero a ciascun sistema ed emette un certificato di avvenuta registrazione. La legge individua inoltre i casi che necessitano di notificazioni particolari, tra questi, ad esempio, i trattamenti di "categorie speciali di dati" che devono essere trasferiti a paesi terzi che non garantiscono un adeguato livello di protezione. L'ufficio, in questi casi, valuta i dati e verifica se il loro trattamento viola i diritti e le libertà dell'interessato e decide, entro 60 giorni dal ricevimento della notifica, se concedere o meno il permesso al trattamento dei dati.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Il titolare del trattamento dei dati deve garantire che i trattamenti siano conformi alla legge. Per questo, nelle aziende che impiegano più di 5 persone, è obbligatorio nominare uno o più DPO con il compito di controllare che le disposizioni della legge vengano rispettate. Tale nomina va notificata all'autorità slovacca per la protezione dei dati entro 30 giorni.

RACCOLTA E TRATTAMENTO DEI DATI	Il titolare del trattamento che intende raccogliere dati personali deve: - determinare in modo univoco e specifico lo scopo del trattamento dei dati prima di iniziare il trattamento; - informare l'interessato circa il nome della compagnia, l'ufficio o la sede del titolare e del responsabile del trattamento e lo scopo del trattamento; - determinare i mezzi con cui verranno trattati e aggiornati i dati; - distruggere i dati personali per i quali il trattamento si è concluso; - trattare dati personali rispettando la morale pubblica e la legge. Generalmente, i dati personali possono essere trattati solo col consenso dell'interessato. Il trattamento di categorie speciali di dati è permesso solo con un consenso scritto da parte dell'interessato, rispettando specifiche condizioni poste dal DPA.
TRASFERIMENTO DEI DATI	**Trasferimento a parti terze all'interno del territorio slovacco**

	I dati personali possono essere trasferiti ad un'altra persona fisica o giuridica solo se l'interessato ha dato il proprio consenso **Trasferimento a paesi non UE che offrono un adeguato livello di protezione** I dati possono essere trasferiti a questi paesi se il titolare del trattamento ha informato l'interessato (ove previsto dalla legge). **Trasferimento a paesi non UE che non offrono un adeguato livello di protezione** Il trasferimento è possibile solo sulla base di una decisione della Commissione Europea o se una delle seguenti condizioni è rispettata: - l'interessato ha dato il proprio consenso scritto al trasferimento, sapendo che il paese di destinazione finale non assicura un adeguato livello di protezione; - il trasferimento è necessario per l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; - il trasferimento è necessario per la protezione degli interessi vitali dell'interessato dei dati;

	- il trasferimento riguarda dati personali contenuti in liste, registri o file che sono accessibili al pubblico sulla base di una legislazione speciale. Se il titolare del trattamento decide di trasferire dati personali a un paese terzo che non offre un adeguato livello di protezione, deve comunicarlo all'interessato per informarlo del suo diritto di rifiutare il consenso al trasferimento. Per il trasferimento verso agli USA si fa riferimento ai principi del programma US/EU Safe Harbor, fermo restando che è necessario presentare comunque una domanda di trasferimento presso l'Autorità nazionale.
SICUREZZA	Il titolare e il responsabile del trattamento devono garantire la sicurezza dei dati personali contro la distruzione o il deterioramento accidentale o illegale, la perdita, l'alterazione, l'accesso e l'uso non autorizzati. A tale scopo, il titolare del trattamento deve adottare misure tecniche e organizzative ragionevoli. Se il sistema informativo contiene speciali categorie di dati, il titolare del trattamento deve preparare un progetto di sicurezza e nominare per iscritto uno DPO (vedi sopra).

NOTIFICA DI VIOLAZIONE	Non c'è un obbligo legale di notifica in caso di violazione.
APPLICAZIONE	L'autorità nazionale è responsabile dell'applicazione della normativa. Su richiesta dell'interessato, o di un'altra persona coinvolta o di un'autorità pubblica, l'Ufficio può dar corso ad un procedimento amministrativo per accertare possibili violazioni del DPA ed eventualmente imporre multe comprese tra i 330 € e i 332.000 €.

ROMANIA

LEGGE	La Romania, nonostante sia membro dell'Unione Europea dal 1 gennaio 2007, ha recepito la direttiva UE 95/46/EC nel proprio ordinamento dal novembre del 2001 con la legge n. 677/2001.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione attraverso cui è possibile identificare in modo diretto o indiretto una persona fisica, in particolare attraverso un numero di identificazione personale o uno o più elementi distintivi della sua identità fisica, fisiologica, mentale, economica, culturale o sociale.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati sull'origine razziale o etnica, le convinzioni politiche, religiose, filosofiche o similari, l'affiliazione a certe associazioni, la salute, la vita sessuale.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	"Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal" o "ANSPDCP : l'Autorità Nazionale per la Sorveglianza del Trattamento dei Dati Personali (ANSPDCP) è stata fondata con la legge n. 102/2005 allo scopo di garantire la protezione dei diritti fondamentali e delle libertà individuali.

NOTIFICAZIONE DEL TRATTAMENTO	Il titolare deve notificare il trattamento all'Autorità nazionale comunicando informazioni quali: identificazione del titolare, ambito del trattamento, categorie dei dati trattati e metodi utilizzati per informare i soggetti interessati circa il trattamento. Per ogni notificazione l'Autorità nazionale raccoglie i dati in un registro pubblico e rilascia al titolare del trattamento un numero identificativo da indicare sui documenti.
RACCOLTA E TRATTAMENTO DEI DATI	Per la notifica il titolare del trattamento deve compilare una scheda disponibile sul sito dell'Autorità nazionale e caricare anche alcuni documenti richiesti. Successivamente la prima pagina della notifica va stampata, fatta firmare dal legale rappresentante e inviata entro 30 giorni all'Autorità nazionale. Nella notifica il titolare del trattamento deve stimare la durata delle operazioni di trattamento dei dati; inoltre ha l'obbligo di comunicare, entro limiti di tempo definiti, anche tutti quei cambiamenti che modificano i dati precedentemente forniti.

	Per il trattamento di categorie particolari di dati (es. i dati sensibili) occorre che l'Autorità rilasci un'autorizzazione specifica sulla base di una serie di documenti specifici che il titolare deve presentare in cui sia chiaro lo scopo del trattamento, i soggetti coinvolti, le categorie di dati trattati, la data stimata della fine delle operazioni, la fonte dei dati, la descrizione delle condizioni in cui sono trattati i dati e l'eventuale motivo dell'urgenza.
TRASFERIMENTO DEI DATI	I trasferimenti di dati personali devono sempre essere notificati all'Autorità nazionale. Le regole sono diverse a seconda della sede del destinatario: - se i dati personali sono trasferiti a un altro paese UE, non sono previsti ulteriori passaggi; - in caso trasferimento verso un paese che secondo l'Autorità nazionale garantisce un adeguato livello di protezione dei dati (USA, Argentina, Canada, Svizzera, Jersey, Guernsey, Isle of Man), occorre indicare il paese di destinazione nella lista online del modulo di notifica; - in caso di trasferimento a paesi che non rientrano nelle ca-

	tegorie precedenti, il titolare del trattamento deve trasmettere all'Autorità nazionale un accordo di trasferimento sottoscritto tra l'operatore e il destinatario. L'accordo deve comprendere delle regole standard che sono ritenute minime per assicurare un livello di protezione adeguato. - Per il trasferimento di dati verso gli USA, fa fede l'adesione ai principi del programma Safe Harbor.
SICUREZZA	I responsabili devono prendere misure tecniche e organizzative adeguate contro l'accesso non autorizzato, la perdita, il danneggiamento o la distruzione illegali dei dati. Le misure devono assicurare un livello di sicurezza coerente con la natura dei dati.
NOTIFICA DI VIOLAZIONE	Non è previsto l'obbligo di notifica in caso di violazione.
APPLICAZIONE	L'autorità nazionale può investigare ex officio oppure in seguito a un ricorso individuale presentato per violazione dei diritti individuali. L'Autorità nazionale può richiedere al responsabile del trattamento qualsiasi informazione relativa al trattamento e può verificare qualsiasi documento o notifica relativa.

SLOVENIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita il 15 luglio 2004 con la Legge sulla Protezione dei Dati Personali (Zakon o Varstvu Osebnih Podatkov o ZVOP).
DEFINIZIONE DI DATI PERSONALI	Qualsiasi dato attraverso cui è possibile identificare un soggetto, indipendentemente dalla forma in cui è espresso.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati che possono rivelare l'origine razziale, nazionale o etnica, le convinzioni politiche, religiose o filosofiche, l'appartenenza sindacale, lo stato di salute, la vita sessuale, le tendenze criminali, le caratteristiche biometriche.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Information Commissioner
NOTIFICAZIONE DEL TRATTAMENTO	I responsabili devono registrare i trattamenti fornendo numerosi dati tra cui: - dati del titolare del trattamento; - base legale del trattamento; - categorie di individui a cui si riferiscono i dati; - tipo di dati trattati; - scopo e durata del trattamento; -eventuali limitazioni di diritti e

	relative basi legali, - destinatari dei dati, - eventuali destinatari di un trasferimento, - descrizione generica delle misure di sicurezza adottate.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Le organizzazioni non hanno l'obbligo di nominare al loro interno il DPO.
RACCOLTA E TRATTAMENTO DEI DATI	Il trattamento di dati personali può essere effettuato soltanto se l'interessato ha dato il proprio consenso in maniera inequivocabile oppure se il trattamento è necessario per: - l'esecuzione di un contratto concluso con l'interessato; - l'adempimento da parte del titolare del trattamento di un obbligo legale; - salvaguardare l'interesse vitale dell'interessato; - l'esecuzione di un'attività di interesse pubblico; - perseguire un interesse legittimo del titolare del trattamento a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata.

TRASFERIMENTO DEI DATI	È possibile trasferire i dati verso tutti i paesi dell'area UE o verso altri paesi solo se è garantito un livello di protezione adeguato. Tuttavia, il trasferimento di dati personali verso paesi che non garantiscono una tutela adeguata è possibile se: - l'interessato ha manifestato il proprio consenso; - è necessario per l'esecuzione di un contratto tra l'interessato ed il titolare del trattamento; - è necessario per la conclusione o l'esecuzione di un contratto a favore dell'interessato; - è necessario, o previsto dalla legge, per la salvaguardia di un interesse pubblico rilevante oppure per constatare, esercitare o difendere un diritto per via giudiziaria; - è necessario per tutelare l'interesse vitale dell'interessato; - viene avviato a partire da un registro accessibile al pubblico.
SICUREZZA	I titolari e i responsabili del trattamento devono adottare tecniche e misure appropriate per proteggere i dati personali contro la distruzione o la perdita sia intenzionale che accidenta -

	le e contro l'apertura e l'accesso non autorizzati alle banche dati.
NOTIFICA DI VIOLAZIONE	In caso di violazione, c'è l'obbligo di notifica all'Autorità nazionale.
APPLICAZIONE	In caso di violazione sono previste multe tra i 4000€ e i 13000€.

SPAGNA

LEGGE	La Spagna ha formalmente recepito la Direttiva UE 95/46/EC nel novembre 1999 con il Special Data Protection Act (LOPD), che ha emendato il precedente LORTAD del 1992. L'applicazione della legge spetta all'Agenzia spagnola per la protezione dei dati (AEPD).
DEFINIZIONE DI DATI PERSONALI	Qualsiasi informazione (tra cui numeri, testi, disegni, immagini, video o audio) attraverso cui è possibile identificare le persone.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati attraverso cui è possibile risalire all'orientamento politico e religioso, l'appartenenza sindacale, l'origine etnica, la salute e la vita sessuale. Ogni categoria di informazione sensibile richiede un diverso livello di protezione.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Agencia Española de Protección de Datos (AEPD)
NOTIFICAZIONE DEL TRATTAMENTO	In Spagna, a differenza degli altri paesi, non esiste un registro dei titolari del trattamento o dei trattamenti dei dati. Presso l'Autorità nazionale esiste un registro dei database in cui sono raccolte le informazioni personali. La notificazione del trattamento, che avviene utilizzando un software messo a disposizione dall'Autorità stessa, è mol-

	to dettagliata e identifica non solo il titolare ma anche gli addetti al trattamento. Contiene una chiara descrizione dei contenuti dei database, le fonti dei dati, gli scopi per cui sono stati raccolti, trattati e trasferiti, così come l'identità dei destinatari delle informazioni, con particolare attenzione ai trasferimenti internazionali. Qualsiasi modifica nel database comporta un emendamento nella notificazione del trattamento.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	La legge non prevede la nomina di un DPO. Nonostante ciò, le organizzazioni che svolgono trattamenti per i quali è richiesto un livello di protezione medio o alto, devono nominare un Capo per la Sicurezza dei Dati, che deve occuparsi esclusivamente delle misure di sicurezza da applicare alle basi di dati.
RACCOLTA E TRATTAMENTO DEI DATI	I dati possono essere raccolti e trattati nel rispetto di una delle seguenti condizioni: - l'interessato dà il proprio consenso; - il trattamento è necessario affinché il titolare possa concludere o eseguire un contratto di cui è parte l'interessato; - i dati sono raccolti da registri

	pubblici e il trattamento è necessario per proteggere un interesse legittimo del titolare del trattamento o di una parte terza a cui sono comunicati i dati, posto che i diritti costituzionali dell'interessato siano garantiti; - il trattamento protegge gli interessi vitali del titolare del trattamento; - il trattamento è previsto dalla legge o nel pubblico interesse. Per il trattamento dei dati sensibili occorre il consenso scritto e esplicito dell'interessato. In ogni caso, il titolare del trattamento deve fornire al soggetto tutte le informazioni relative al trattamento.
TRASFERIMENTO DEI DATI	I titolari del trattamento possono trasferire dati personali a terzi nei seguenti casi: -l'interessato dà il proprio consenso; - il trasferimento è previsto dalla legge; - i dati sono raccolti da registri pubblici; - il trasferimento è indispensabile per l'esecuzione di un contratto di cui l'interessato è liberamente e legittimamente parte;

	- il trasferimento è fatto per il difensore civico nazionale o regionale, per il pubblico ministero, giudici e corti; - il trasferimento avviene tra enti pubblici ed è finalizzato a scopi di ricerca storica, statistica o scientifica; - il trasferimento è urgente e necessario per proteggere la salute dell'interessato o di altri individui. L'interessato ha la facoltà di revocare in qualsiasi momento il proprio consenso. Il consenso sarà ritenuto nullo se l'interessato, attraverso le informazioni ricevute, non sarà in grado di identificare gli scopi per cui i propri dati sono stati trattati. Questi principi si applicano al trasferimento dei dati all'interno della Spagna o dell'EEA. Il trasferimento dei dati personali a paesi non UE/EEA è consentito solo se è garantito un adeguato livello di protezione per la sicurezza dei dati (es.: Argentina), o se vi è il consenso inequivocabile dell'interessato o in altri specifici casi, tra cui: trattati internazionali; cooperazione giudiziaria; motivi di salute;

	trasferimenti monetari internazionali; protezione di un interesse pubblico; ecc. In qualsiasi altro caso, il trasferimento all'estero a paesi che non sono ritenuti adeguati deve essere autorizzato in anticipo dall'Autorità nazionale. Per i trasferimenti di dati agli USA, si fa riferimento al UE/US Safe Harbor Principles.
SICUREZZA	I titolari e i responsabili del trattamento devono adottare adeguate misure tecniche e organizzative contro l'accesso o il trattamento non autorizzato o illegale, la perdita accidentale, la distruzione o il danneggiamento dei dati. Le misure prese devono assicurare un livello di sicurezza appropriato alla natura de dati.
NOTIFICA DI VIOLAZIONE	In caso di violazione del sistema di protezione dei dati, la legge non prevede un obbligo di notifica né all'Autorità nazionale, né agli interessati. Ciononostante, le organizzazioni hanno l'obbligo di registrare qualsiasi violazione in un apposito registro a cui l'Autorità può accedere in qualsiasi momento. Tuttavia, la consuetudine vuole che le forze di polizia o gli uffici pubblici inviino immediatamente una notifica all'AEPD nel mo-

	mento in cui ricevono un reclamo per una violazione.
APPLICAZIONE	L'Autorità nazionale è responsabile dell'applicazione della legge. Può agire sia ex officio, sia sulla base di un ricorso presentato dall'interessato o da una pubblica autorità che ha ricevuto l'esposto dal soggetto interessato. L'Autorità nazionale può avviare: - un'indagine per raccogliere informazioni; - una procedura per la protezione dei diritti di privacy, quando il titolare del trattamento impedisce al soggetto interessato di esercitare i propri diritti di accesso, rettifica, cancellazione o opposizione; - una procedura disciplinare a carico del titolare del trattamento in caso di violazione della legge. In Spagna il diritto alla privacy è un diritto costituzionale e la negligenza o l'errore non sono considerati una ragione valida per limitare le sanzioni, che sono essenzialmente pecuniarie. Le multe possono andare dai 900 ai 40.000€ per infrazioni minori, dai 40.001 € ai 300.000 € per infrazioni ritenute serie e dai 300.001 € ai 600.000 € per infrazioni molto serie.

SVEZIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita nel 1998 con il Personal Data Act (Sw. Personuppgiftslagen) SFS 1998:204.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi tipo di informazione attraverso cui è possibile risalire direttamente o indirettamente a una persona fisica viva.
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Dati che rivelano l'origine etnica o razziale di una persona, le sue opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute e la vita sessuale.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	Data Inspection Board (Sw. Datainspektionen)
NOTIFICAZIONE DEL TRATTAMENTO	Tutti i trattamenti, eccetto quelli per cui la legge prevede eccezioni, devono essere notificati all'Autorità nazionale.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	La legge non obbliga le aziende a nominare un DPO. Nel caso in cui un'azienda decida di prevedere tale figura, deve comunicarlo all'Autorità nazionale e, automaticamente, ricade tra i casi eccezionali per cui non è richiesta la notificazione del trattamento. Compito del DPO è di tenere un registro dei trattamenti effettuati.

RACCOLTA E TRATTAMENTO DEI DATI	I titolari possono raccogliere e trattare dati personali qualora: - l'interessato fornisca il proprio consenso; - il trattamento venga effettuato da un'autorità pubblica; - il trattamento sia necessario per concludere un contratto di cui l'interessato è parte; - il trattamento sia necessario affinché il titolare adempia un obbligo legale; - il trattamento sia necessario per proteggere gli interessi vitali dell'interessato; - il trattamento sia necessario per l'interesse pubblico; - l trattamento sia necessario per il perseguimento dell'interesse legittimo del titolare oppure di terzi a cui i dati sono comunicati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata che sono suscettibili di tutela; Nel caso di trattamento di dati personali sensibili, la legge prevede ulteriori obblighi oltre a quelli sopra menzionati. In ogni caso, il titolare del tratta-

	mento deve fornire all'interessato alcune informazioni, tra cui l'identità del titolare del trattamento, lo scopo del trattamento, se i dati saranno trasferiti e a chi e qualsiasi altra informazione che consenta all'interessato di esercitare i propri diritti.
TRASFERIMENTO DEI DATI	In linea di principio, è proibito trasferire i dati personali a paesi fuori dall'UE/EEA che non offrono un adeguato livello di protezione. Il trasferimento può in ogni caso essere autorizzato anche verso un paese che non offre un adeguato livello di protezione, solo se l'interessato ha dato il proprio consenso, o in alcuni casi previsti dalla legge (es. protezione degli interessi vitali dell'interessato). Il trasferimento di dati personali è permesso anche verso uno stato che ha aderito alla Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione degli individui nel trattamento di dati automatico. Il trasferimento di dati personali a paesi terzi è permesso se questi forniscono un'adeguata protezione dei dati o se il trasferimento è coperto dalle clausole contrattuali approvate dalla Commissione Europea, o sog-

	getto alle Binding Corporate Rules di un'organizzazione. Per i trasferimenti verso gli USA si fa riferimento al Programma US/UE Safe Harbor.
SICUREZZA	Il titolare del trattamento è responsabile delle misure tecniche e organizzative per la protezione dei dati personali che devono assicurare un adeguato livello di sicurezza. Se il titolare individua degli addetti al trattamento, questi ultimi devono rispettare le norme e le misure di sicurezza, anche se in ultima istanza è il titolare che risponde di eventuali violazioni. In casi particolari, l'Autorità nazionale può decidere speciali misure di sicurezza.
NOTIFICA DI VIOLAZIONE	In caso di violazione non c'è un obbligo di notifica all'Autorità nazionale. Le violazioni sono valutate caso per caso. Tuttavia, in seguito all'attuazione della Direttiva sulla e-Privacy, la legge svedese sulle comunicazioni elettroniche del luglio 2011 (Sw. lag om elektronisk kommunikation, SFS 2003:389) dispone che il gestore del servizio di comunicazione pubblica debba immediatamente notificare a Swedish Post a Telecom

	Authority (Sw. Post-och Telestyrelsen) incidenti che violano dati personali, specificando se questi hanno conseguenze su abbonati o utenti. Solo nel caso in cui il provider abbia adottato misure di sicurezza che rendono i dati illeggibili ai non autorizzati, la notifica di violazione non è richiesta.
APPLICAZIONE	L'Autorità nazionale, nel suo ruolo di supervisore, ha il diritto di accesso ai dati personali trattati, alle informazioni e alla documentazione riguardante il trattamento dei dati. Contro le decisioni dell'Autorità si può ricorrere in appello alla Corte amministrativa generale. L'Autorità può però decidere che la decisione contro la quale è stato presentato ricorso deve comunque essere applicata. In caso di violazione della legge, sono previste sanzioni pecuniarie o detentive per un periodo che va da 6 mesi a 2 anni. Inoltre in caso di trattamenti non conformi il titolare può essere obbligato a obbligato al risarcimento danni.

UNGHERIA

LEGGE	La direttiva europea sulla protezione dei dati 95/46/EC è stata recepita con la legge n. CXII del 2011 "Informational Self-Determination and Freedom of Information", entrata in vigore il 1 gennaio 2012 che istituisce anche l'Autorità Nazionale per la Protezione dei Dati e la Libertà di Informazione ("Authority"), a cui spetta l'applicazione della legge.
DEFINIZIONE DI DATI PERSONALI	Qualsiasi dato relativo al soggetto (in particolare nome, numero di identificazione, uno o più fattori specifici dell'identità fisica, fisiologica, mentale, economica, culturale o sociale) e qualsiasi riferimento che possa essere ricavato da tali dati. Durante il trattamento, tali dati devono essere trattati come dati personali fino a quando da tali dati è possibile risalire al soggetto attraverso l'uso di tecnologia adeguata fornita dal titolare del trattamento. Diversamente tali dati non dovranno essere considerati "dati personali".
DEFINIZIONE DI DATI PERSONALI SENSIBILI	Si tratta di dati che: - rivelano l'origine razziale, nazionale o etnica, le opinioni politiche e qualsiasi appartenenza a partiti politici e sindacati, le con-

	vinzioni religiose o filosofiche, la vita sessuale; - rivelano lo stato di salute, le dipendenze o le tendenze criminali.
AUTORITA' NAZIONALE PER LA PROTEZIONE DEI DATI	National Authority for Data Protection and Freedom of Information: Nemzeti Adatvédelmi és Információszabadság Hatóság – NAIH
NOTIFICAZIONE DEL TRATTAMENTO	Il titolare del trattamento, prima di iniziare qualsiasi trattamento, deve richiede l'autorizzazione all'Autorità nazionale che provvede a registrare la richiesta addebitando un costo (di cui non si conosce ancora l'entità) al titolare. La notifica deve includere le seguenti informazioni: - lo scopo del trattamento; - i tipi di dati e le basi legali del trattamento; - le categorie dei soggetti dei dati; - la fonte; - le categorie dei dati trasferiti, i destinatari e le basi legali del trasferimento; - il nome e l'indirizzo del titolare e dell'addetto al trattamento, il luogo in cui i dati verranno conservati e trattati e le attività che

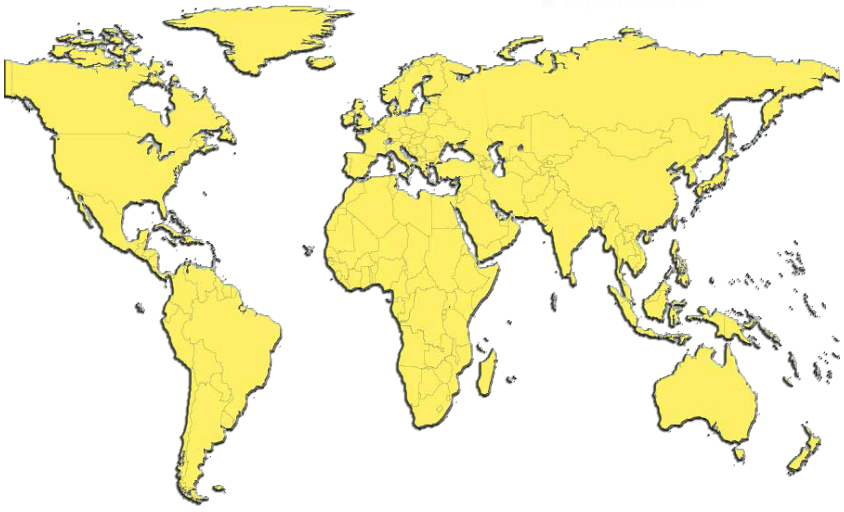
	svolgerà l'addetto in relazione al trattamento; - la tecnologia utilizzata per il trattamento.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – Data Protection Officer)	Alcuni titolari del trattamento (istituzioni finanziarie, provider di servizi di comunicazione e di pubblica utilità e autorità che accedono ai dati dei registri nazionali del lavoro e della giustizia) hanno l'obbligo di nominare un DPO che deve essere in possesso di una laurea in legge, in economia o in informatica e che risponde direttamente al capo dell'organizzazione.
RACCOLTA E TRATTAMENTO DEI DATI	I dati possono essere raccolti e trattati se l'interessato dà il proprio consenso e se il trattamento è previsto per legge o per decreto emesso da una municipalità locale sulla base di una legge nazionale. I dati personali possono essere trattati anche senza il consenso dell'interessato qualora il trattamento sia necessario affinché il titolare adempia un obbligo legale o per soddisfare gli interessi legittimi di una terza parte o del titolare del trattamento stesso. I dati sensibili possono essere trattati se:

	- l'interessato ha dato il proprio consenso per iscritto; - è necessario per l'applicazione un trattato internazionale, o di un diritto costituzionale o per la salvaguardia di un interesse pubblico o della sicurezza nazionale.
TRASFERIMENTO DEI DATI	Il trasferimento all'interno dei paesi EEA è considerato come se avvenisse all'interno dell'Ungheria, per cui non occorre il consenso. La legge ammette il trasferimento dei dati a paesi terzi non EEA se le condizioni (basi legali) del trattamento sono soddisfatte e il livello di protezione è adeguato. Spetta all'Authority decidere se sono queste condizioni sono soddisfatte oppure no.
SICUREZZA	I titolari devono adottare tutte le misure tecniche e organizzative affinché sia rispettato il livello di protezione richiesto. I dati devono essere protetti contro l'accesso, l'alterazione, il trasferimento e la diffusione non autorizzati e il deterioramento.
NOTIFICA DI VIOLAZIONE	La legge non prevede un obbligo di notifica né all'autorità né ai soggetti interessati. Tuttavia, come regola speciale, i provider di servizi di comunicazione elettronica devono riportare

	immediatamente le violazioni al National Media and Infocommunications Authoriy secondo la legge No. 100 del 2003 sulle comunicazioni elettroniche.
APPLICAZIONE	L'Autorità nazionale è un ente amministrativo istituito con la legge di recepimento della Direttiva europea, è guidata da un Presidente proposto dal primo ministro e nominato dal presidente della Repubblica per un periodo di 9 anni. L'Autorità ha tutti i poteri necessari per dare attuazione e fare osservare la legge verificando che i trattamenti dei dati si svolgano rispettando i diritti dei soggetti interessati. In particolare l'Authority può: - ordinare la correzione di dati non conformi; - ordinare il blocco, l'eliminazione o la fine del trattamento non conforme alla legge; - proibire il controllo o il trattamento illegale dei dati; - proibire il trasferimento dei dati a paesi stranieri; - ordinare al titolare del trattamento di notificare eventuali violazioni alla parte lesa; - imporre multe il cui importo può variare dai 350€ ai 35.000€ circa.

TERZA PARTE

...E NEL RESTO DEL MONDO?



...E NEL RESTO DEL MONDO?

In questa sezione è possibile farsi un'idea di come il diritto alla riservatezza sia tutelato in 32 paesi del "resto del mondo".

ARGENTINA

In Argentina i riferimenti legislativi sono:

- Legge sulla protezione dei dati personali n. 25326 del 2000

- Regolamento approvato con Decreto n. 1558/2001

L'Argentina è stato il primo paese del Sud America la cui legislazione è stata ritenuta dalla Commissione Europea adeguata rispetto al livello di protezione garantito ai dati personali.

AUSTRALIA

In Australia la protezione dei dati personali è disciplinata oltre che dal Federal Privacy Act del 1988 (Cth), che si applica alle aziende private e alle agenzie governative dell'area di Canberra (Australian Capital Territory), anche dalla legislazione statale e territoriale che si applica alle agenzie governative dei vari stati. I riferimenti legislativi sono i seguenti:

- Information Act 2002 (Northern Territory)

- Privacy and Personal Information Protection Act 1998 (New South Wales)

- Information Privacy Act 2009 (Queensland)

- Personal Information and Protection Act 2004 (Tasmania)

- Information Privacy Act 2000 (Victoria)

A livello statale e federale inoltre vi sono ulteriori disposizioni legislative sulla protezione dei dati personali in ambiti specifici, per esempio: Telecommunications Act 1997, National Health Act 1953, Health Records and Information Privacy Act 2002 (NSW),

Nei prossimi 12-24 mesi è attesa una significativa riforma del Federal Privacy Act.

BRASILE

In Brasile diverse fonti disciplinano la protezione dei dati personali:la Costituzione, che contiene i principi e le disposizioni generali, il Codice Civile, le leggi e i regolamenti che fanno invece riferimento a specifici ambiti (Codice di protezione dei consumatori e diritto de lavoro), settori di attività (finanziario, sanità, telecomunicazioni, ecc.) e professioni (medici e avvocati). Inoltre esistono leggi che salvaguardano la riservatezza delle informazioni gestite dalle istituzioni governative.

CANADA

In Canada la protezione dei dati personali nel settore privato, pubblico e sanitario è regolata a livello federale, provinciale e territoriale da ben 27 leggi che, nel loro insieme costituiscono, il "Canadian Privacy Statutes".

Nel settore pubblico le leggi di riferimento sono:

- Privacy Act del 1983,

- Access to Information Act del 1985

- Freedom of Information Act del 1996.

Nel settore privato invece si fa riferimento a:

- Personal Information Protection and Electronic Documents Act ("PIPEDA"), Legge federale

- Personal Information Protection Act ("PIPA Alberta"), Legge della Provincia di Alberta

- Personal Information Protection Act ("PIPA BC"), Legge della Provincia della British Columbia

- Act Respecting the Protection of Personal Information in the Private Sector ("Quebec Privacy Act"), Legge della Provincia del Qubec

CILE

In Cile la protezione dei dati personali è disciplinata dalle seguenti disposizioni legislative e regolamentari:

- Legge n. 19628 per gli archivi di dati personali c/o istituzioni pubbliche e private;

- Decreto n. 779/2000 del Ministero della Giustizia con il quale è stato emanato il regolamento per gli archivi di dati personali c/o gli enti pubblici

- Legge n. 20285 che regola la libertà di informazione

- Decreto n. 13/ 2009 del Ministro generale della Presidenza con il quale è stato emanato il regolamento per la L. 20285.

CINA

In Cina varie legge e regolamenti contengono clausole relative alla protezione dei dati personali, ma mai si ritrova una chiara definizione della portata del diritto alla tutela della privacy. Da molti anni il governo sta lavorando su un disegno di legge per la protezione dei dati personali, ma non vi sono indicazioni se e quando questa legge sarà approvata. Recentemente il Ministro dell'informazione e dell'Industria ha pubblicato una bozza di progetto su "Tecnologie per la Sicurezza dell'informazione – Guida per la protezione dei dati personali". Qualora questo documento dovesse essere approvato e reso esecutivo, il suo impatto sulle modalità di gestire e trattare i dati personali sarebbe significativo

COLOMBIA

L'art. 15 della Costituzione colombiana include tra i diritti fondamentali il diritto alla riservatezza e alla tutela dei dati personali.

Recentemente, il 17 ottobre 2012, la Corte Costituizonlae Colombiana ha approvato, una nuova e innovative legge sulla protezione dei dati personali (Statutory Act No 1581) che risente profondamente dell'influenza europea.

E' in vigore anche La Legge 1266/08 che regola invece la raccolta, l'uso e il trasferimento di dati nell'ambito del settore creditizio e finanziario.

COREA DEL SUD

La legge per la protezione dei dati personali è entrata in vigore il 30 settembre 2011. Esistono inoltre delle leggi di settore come, per esempio:

-Act on Promotion of Information and Communication Network Utilization and Information Protection ("IT Network Act"), che regola la raccolta e l'uso dei dati personali da parte dei provider di servizi di telecomunicazione;

- Act on Real Name Financial Transactions and Guarantee of Secrecy ("ARNFTGS") per le informazioni ottenute da istituzioni finanziarie.

DUBAI

Nell'Emirato di Dubai la legge di riferimento per la protezione dei dati personali è la n. 1 del 2007, emendata dalla Legge n. 5 del 2012. La legge si applica alle persone giuridiche e fisiche che operano nell'ambito della sfera giuridica regolata dal Centro Finanziario Internazionale di Dubai (Zona Franca Finanziaria) (Dubai International Financial Centre - DIFC).

EGITTO

In Egitto il diritto alla riservatezza è riconosciuto a livello costituzionale, anche se non esiste una specifica legge per la protezione dei dati personali. Nelle disposizioni del Codice Civile, Penale e all'interno di varie disposizioni legislative e regolamenti si ritrovano alcune clausole che disciplinano la protezione dei dati in differenti settori (lavoro, sanitario, bancario e creditizio ...).

EMIRATI ARABI (United Arab Emirates - UAE)

A livello federale non c'è una legislazione per la protezione dei dati personali. La materia è disciplinata dalla Costituzione degli Emirati (Federal Law 1 of 1971, Article 31) e da varie disposizioni contenute nelle seguenti leggi e regolamenti:

- Penal Code (Federal Law 3 of 1987 e successive modifiche)

- Cyber Crime Law (Federal Law 2 of 2006);

- Regulating Telecommunications (Federal Law by Decree 3 of 2003 e successive modifiche tra cui alcuni regolamenti attuattivi emessi da Telecommunications Regulatory Authority per la tutela dei consumatori.

FILIPPINE

Attualmente nelle Filippine non esiste una legge specifica per la protezione dei dati personali e, nonostante la Costituzione garantisca il diritto alla privacy nella comunicazione e il diritto di accesso alle informazioni governative, sono numerose le cause per la violazione di tali diritti costituzionali.

All'interno di testi legislativi e regolamentari vi possono ritrovare disposizioni relative alla protezione dei dati personali, ad esempio:

- Codice Civile, art. 32 e 723

- Legge sul commercio elettronico che prevede l'obbligo di riservatezza

- Regolamento del Dipartimento amministrativo (Department Administrative Order No.08 - Series of 2006) che individua delle linee guida per la protezione dei dati personali nel settore della comunicazione e informazione.

GIAPPONE

In Giappone la legge che disciplina la Protezione dei dati personali (Act on the Protection of Personal Information - "APPI") è la n. 57 del 30 maggio 2003, entrata in vigore il 1 aprile 2005, il cui contenuto è molto simile a quanto disposto dalla Direttiva Europea 95/46/EC.

HONG KONG

La protezione dei dati personali è regolata dalla legge n. 18 del 2012 ("Ordinance no. 18") che ha profondamente modificato la legge precedente, la n. 486 del 1995 ("Ordinance no. 486) e successivi emendamenti.

INDIA

In India la tutela della privacy è disciplinata dalla legge 21 del 2000 (Information Technology Act), alla quale è stata data attuazione solo nel 2011 con il regolamento "Clarification on the Privacy Rules" emesso dal Ministero per la comunicazione e informazione.

INDONESIA

In Indonesia non c'è una legge specifica sulla Protezione dei dati. Nella Costituzione è riconosciuto il diritto al rispetto e alla dignità e all'interno del codice civile e penale ci sono diverse disposizioni che disciplinano l'obbligo alla riservatezza nel trattare informazioni. Inoltre esistono leggi che disciplinano il tema della protezione dei dati personali in ambiti specifici del diritto (diritti umani, diritto del lavoro, diritto sanitario, ecc.).

MALESIA

Dopo numerose consultazioni e dibattiti, in Malesia il 1 gennaio 2013 è entrata in vigore la prima legge sulla Protezione dei dati personali (Personal Data Protection Act 2010 – "PDPA") che sostituisce

la precedente consuetudine di trattare il diritto alla riservatezza inserendo apposite clausole nei documenti e contratti.

MAURITIUS

Nella Repubblica di Mauritius la materia della protezione dei dati è disciplinata dal Data Protection Act 2004 ("MU DPA"), entrato in vigore nel Febbraio 2009.

MESSICO

In Messico c'è una Legge Federale sulla protezione dei dati personali trattati da persone fisiche o giuridiche private (Ley Federal de Protección de Datos Personales en Posesión de Particulares) che è entrata in vigore il 6 luglio 2010 e un regolamento dall'esecutivo (Reglamento de la Ley Federal de Protección de Datos en Posesión-de Particulares) entrato in vigore il 22 dicembre 2011.

NORVEGIA

La Norvegia, pur non facendo parte dell'Unione Europea, ha sottoscritto l'accordo che il 1 gennaio 1994 ha dato vita alla Area Economica Europea. Per questo, nell'aprile 2000 ha adottato la direttiva europea sulla protezione dei dati personali approvando il Personal Data Act 2000 la cui applicazione è in carico al Data Inspectorate.

NUOVA ZELANDA

In Nuova Zelanda la Legge sulla privacy è del 1993 e disciplina la raccolta, l'uso, la divulgazione, l'archivio dei dati personali, nonché le modalità di accesso. Al Commissario per la protezione di dati personali la legge conferisce il potere di emettere dei codici procedurali in relazione a specifiche industrie, agenzie, ttività o tipi di dati personali che modificano il contenuto della legge stessa. Al 31 gennaio 2012 i codici in essere sono quelli relativi al settore del credito, della sanità; della giustizia, della previdenza e delle telecomunicazioni.

PAKISTAN

Attualmente in Pakistan non esiste una legislazione per la protezione dei dati personali. Nel 2005 il Ministro per l'informazione elaborò un progetto di legge sulla protezione dei dati elettronici che il Governo però non ha mai reso esecutivo.

PRINCIPATO DI MONACO

Nel Principato, la materia è disciplinata dalla Legge n. 1.165 del 23 December 1993, modificata dalla Legge n° 1.353 del 4 December 2008 ("DPL"). Inoltre, essendo il Principato di Monaco membro del Consiglio d'Europa, ha aderito alla Convenzione n. 108 del Consiglio sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

RUSSIA

In Russia la protezione dei dati personali è garantita da più fonti:

- Convenzione di Strasburgo sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e ratificata dalla Russia nel 2006;

- Costituzione Russa che agli articoli 23 e 24 afferma il diritto alla privacy per ogni individuo

- Legge sulla protezione dei dati personali n. 152 FZ del 27 luglio 2006 e relativi regolamenti

- Legge sulla libertà di informazione in tutte le sue forme n. 149 FZ del 27 luglio 2006, emendata con la legge n. 139-FZ del 28 luglio 2012 per la protezione dei con la quale la Duma ha introdotto delle misure di protezione dei minori dai pericoli della rete, individuando una "black-list" di siti internet considerati pericolosi;

- Codice del lavoro in cui nella parte XIV sono contenute disposizioni sulla protezione dei dati personali dei lavoratori dipendenti.

SINGAPORE

La legge per la protezione dei dati personali (Personal Data Protection Act n. 26 del 2012) è recentissima: è stata infatti approvata il 15 ottobre 2012, dopo una lunga serie di consultazioni pubbliche, ed è entrata in vigore il 2 gennaio 2013.

STATI UNITI

Negli Stati Uniti ci sono circa 20 leggi a livello nazionali che disciplinano la materia nell'ambito di settori più o meno specifici, oltre a un centinaio di altre leggi all'interno dei singoli stati (solo in California ci sono più di 25 leggi sulla privacy e la protezione dei dati personali). Inoltre gioca un ruolo molto importante anche la Federal Trade Commission (FTC) che ha il potere di perseguire quelle aziende che non applicano le misure minime di sicurezza e non rispettano le politiche di riservatezza.

SUD AFRICA

In Sud Africa attualmente non esiste una legge per la protezione dei dati personali, ma il Parlamento sta lavorando già da tempo sul Protection of Personal Information Bill.

I riferimenti legislativi al momento sono:

- Costituzione della Repubblica del Sud Africa che garantisce il diritto alla privacy;

- Electronic Communications and Transactions Act che contiene alcune disposizioni relative alla raccolta di dati personali attraverso sistemi elettronici, che però non ha carattere obbligatorio.

SVIZZERA

Il trattamento dei dati personali è regolato principalmente dal Federal Act on Data Protection del 19 giugno 1992 e dai suoi regolamenti attuativi (Ordinance to the Federal Act on Data Protection e Ordinance on Data Protection Certification). In ogni caso nel settore pubblico e dei mercati regolati vengono applicate disposizioni legislative più restrittive.

TAIWAN

Il 1 ottobre 2012 è entrata in vigore la nuova legge per la protezione dei dati personali (Personal Data Protection Act).

THAILANDIA

In Thailandia al momento non c'è una legge che regola la protezione della privacy. Nella recente Costituzione, approvata nel 2007, sono sanciti alcuni diritti alla privacy, tra cui quello alla protezione dei dati personali. Per il resto esistono leggi che regolano la materia in specifiche aree (telecomunicazioni, servizi bancari e finanziari, protezione dei minori e dei consumatori) in modo da impedire raccolte, trattamenti, divulgazioni e trasferimenti di dati non autorizzati. Il Parlamento sta lavorando su un progetto di legge coerente e complessivo che si presume sarà basato sugli standard europei al fine di facilitare il trasferimento dei dati da e verso l'Unione Europea.

TURCHIA

In Turchia non esiste una specifica legge sulla protezione dei dati personali. Vi sono numerose leggi e regolamenti che disciplinano la materia in specifici ambiti.

Il Parlamento sta attualmente lavorando su un progetto di legge di carattere complessivo che si avvicina molto nei contenuti alla direttiva europea 95/46/EC.

URUGUAY

Le fonti legislative che disciplinano la protezione dei dati sono:

- Data Protection Act Law No. 18.331 (11 August 2008)

- Decree No. 414/009 (31 August 2009)

Per la legislazione della Repubblica Uruguaiana il diritto alla protezione dei dati personali è uno dei diritti fondamentali della persona.

Recentemente la Commissione Europea ha approvato la legislazione uruguaiana ritenendola come "adeguata" rispetto al livello di protezione garantito nel caso di trasferimento di dati personali. E' il secondo stato dopo l'Argentina ad ottenere questo riconoscimento dalla Commissione europea.

FONTI - SITOGRAFIA

• Comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati. Bruxelles 07.03.2007, COM (2007) 87 def.

• Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

• Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

• Relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE) (COM(2003)265 – C5-0375/2003 – 2003/2153(INI)). Parlamento europeo, 24 febbraio 2004.

• Working document 2 on the protection of individuals with renard to the processing of personal data and on the free movement of such data. Committee on Civil Liberties, Justice and Home Affairs. European parliament, 08.10.2012

• Working document 3 on the protection of individuals with renard to the processing of personal data and on the free movement of such data. Committee on Civil Liberties, Justice and Home Affairs. European parliament, 19.10.2012

• Data protection laws of the world. DLA Piper (Global Law Firm, London), March 2012

• http://www.garanteprivacy.it

• http://hub.coe.int/

• www.privacyinternational.org

• www.legalweeklaw.com

• www.huntonprivacyblog.com

• www.huntonprivacyblog.com

• www.filodiritto.com

• https://secure.edps.europa.eu

settembre 2013

Stampa : Centro Stampa Regione Emilia-Romagna

Impaginazione: Antonella Pascale, Francesca Mezzadri

Copertina e immagini da European Commission Data Protection
(http://ec.europa.eu/justice/data-protection/minisite/)