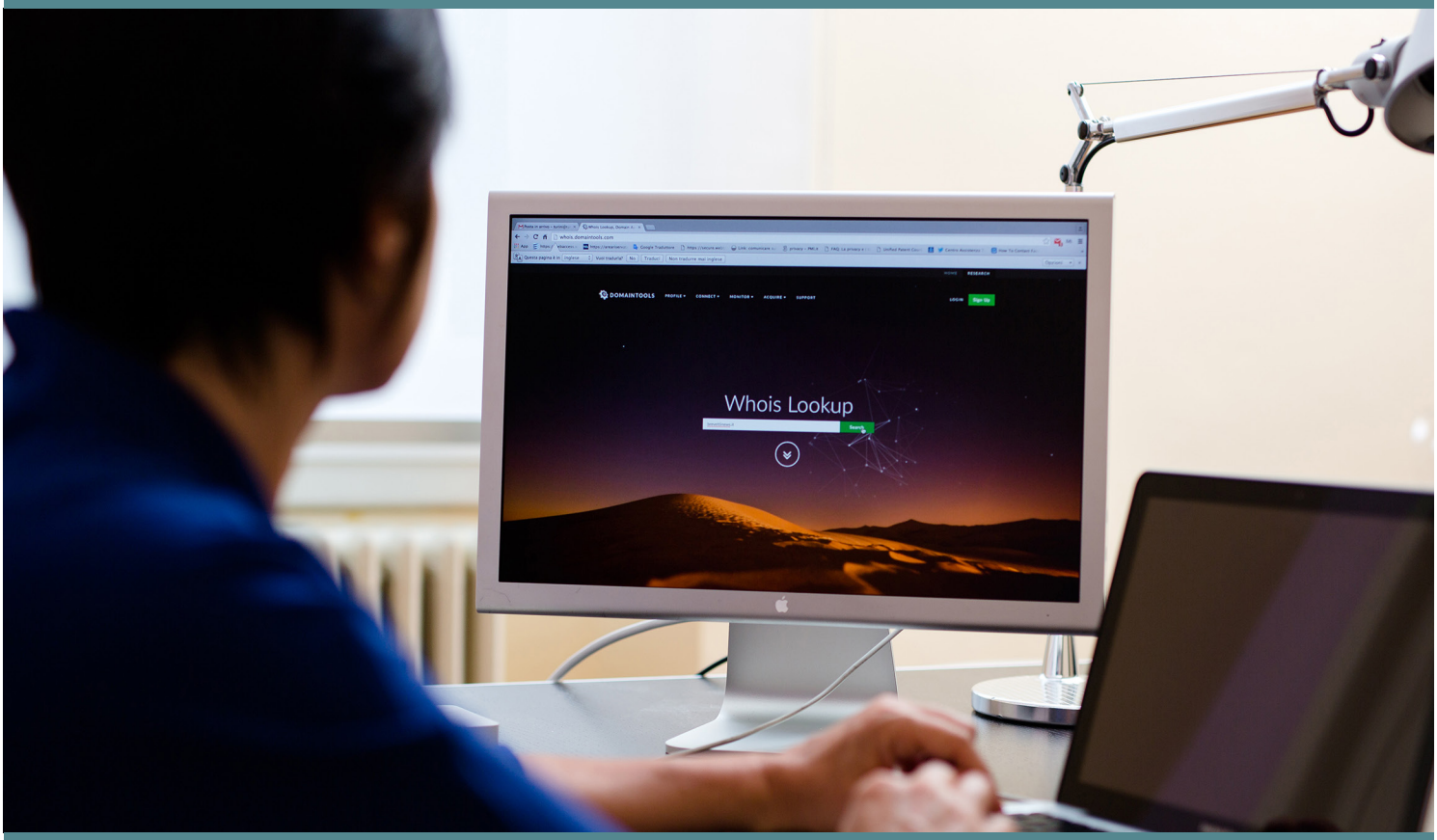
TURINI

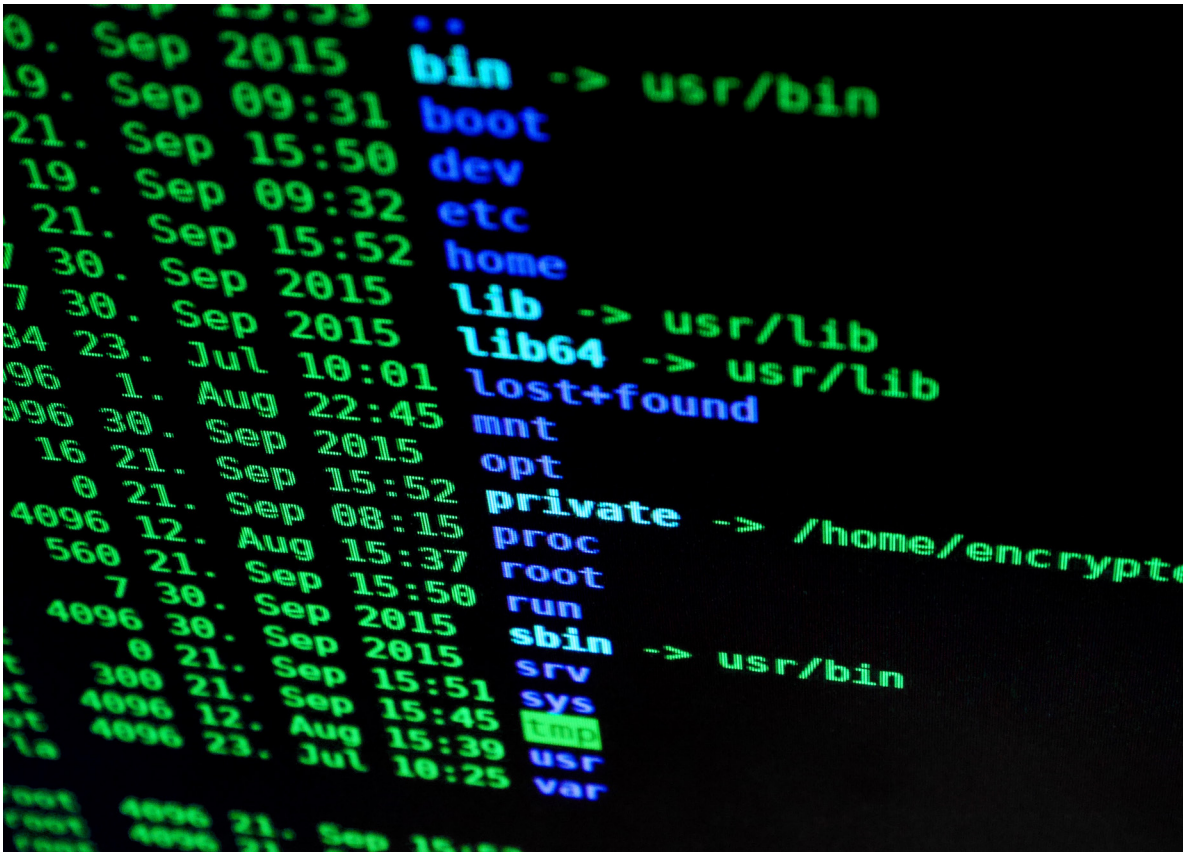
Dal 1993 tuteliamo le vostre ***idee***

www.turinigroup.com



Privacy e Data Protection

Il trattamento di dati personali in Europa:
il nuovo Regolamento sulla privacy



Privacy e Data Protection

Da oltre dieci anni ci occupiamo di Privacy. La nostra esperienza al vostro servizio.

Il 24 Maggio 2016 è entrato in vigore il **Regolamento Europeo sulla Privacy 2016/679.** Le GDPR, **General Data Protection Regulations**, in esso contenute si applicano sia alle **imprese europee** sia alle **imprese extra-UE** che offrono beni e servizi nell'Unione o che hanno uno stabilimento o un rappresentante nell'Unione.

Le imprese che trattano affari con l'Unione Europea dovranno adeguare la loro struttura aziendale in modo conforme al Regolamento entro il 25 Maggio 2018.

Vi raccomandiamo di chiedere una valutazione preliminare della vostra struttura aziendale per valutare tempestivamente gli interventi necessari per la compliance che possono comportare revisioni importanti.

L'adeguamento non può mai essere "standardizzato" ma **disegnato su misura caso per caso** per ogni singola realtà.


devise :database_
:validatab
validates :email,
before_validation
after_initialize
has_many :photos,
has_many :orders_
has_many :orders_
has_many :ratings
has_many :message
has_many :message
accepts_nested_att
avatar attach

IL TRATTAMENTO DI DATI PERSONALI IN EUROPA: **IL NUOVO REGOLAMENTO PRIVACY**

1. A chi si applica 6
2. A chi non si applica 7
3. Cosa sono i dati personali 8
4. Cosa è un trattamento di dati 9
5. Chi è il titolare del trattamento 10
6. L'informativa e i diritti dell'interessato 11
7. La "base legale" del trattamento e il consenso 12
8. La responsabilità del titolare 13
9. Data protection e sicurezza informatica 14
10. Le sanzioni 15

1 A chi si applica

Per stabilire se un'impresa è soggetta al Regolamento Europeo sulla Privacy è necessario conoscere i suoi **stabilimenti** e la sua organizzazione interna (art. 3).

Il Regolamento si applica ad un'impresa che ha:

- uno **stabilimento nell'Unione** se il trattamento riguarda l'attività che viene svolta nello stabilimento. In questo caso non conta la nazionalità dell'interessato del trattamento né importa che vengano offerti servizi o beni nell'Unione; oppure
- uno stabilimento **fuori dall'Unione**, se svolge un'attività (ad esempio monitoraggio o profilazione) o **un'offerta di beni e servizi nell'Unione**, destinata a soggetti che si trovano, anche in via temporanea, nell'Unione. Non conta invece la nazionalità di questi ultimi.

È importante considerare che ai sensi del Regolamento lo *"stabilimento"* è anche la presenza di un rappresentante nell'Unione o lo svolgere alcune attività nell'Unione, come il tracciamento dei consumatori (Google Spain C-131/12; Weltimmo C-230/14).

Non è considerato *"stabilimento"* avere un sito Internet accessibile dall'Unione o avere il server nell'Unione.

L'ubicazione del server e della struttura che tratta i dati (c.d. *equipment*) è irrilevante ai fini dell'applicazione del Regolamento.

A chi non si applica

Il Regolamento **non si applica ad alcuni specifici trattamenti di dati.**

In particolare non si applica al trattamento di dati fatto per attività che **non rientrano nell'applicazione del diritto dell'Unione**, ad esempio per la sicurezza nazionale. È escluso il trattamento di dati fatto dagli Stati per la politica estera, per le indagini penali, per la prevenzione e per motivi di sicurezza pubblica.

Il Regolamento non si applica al trattamento di dati effettuato **in modo interamente manuale e non strutturato**, al trattamento di dati di **persone decedute**, al trattamento di **informazioni anonime** (art. 2, par. 1).

Il Regolamento non si applica al trattamento di dati effettuato da una persona fisica **per finalità esclusivamente domestiche o personali**.

Sono considerate personali le attività svolte anche *online* all'interno di un social network e la tenuta di una rubrica personale. Non è invece considerata personale l'attività di inserire foto o informazioni personali su Internet in modo che possa avervi accesso un numero indeterminato di persone, in quanto esula dall'ambito domestico e privato.

La videosorveglianza di un'abitazione privata esula dall'ambito privato e domestico se la telecamera visualizza immagini anche su una parte di strada pubblica per cui in questo caso si applica il Regolamento.

3

Cosa sono i dati personali

È dato personale **«qualsiasi informazione riguardante una persona fisica identificata o identificabile»** che nel Regolamento prende il nome di *"interessato"* del trattamento.

Il Regolamento **si occupa solo di dati relativi a persone fisiche** e non anche delle persone giuridiche.

Il concetto di dato personale è molto ampio e riguarda qualsiasi informazione che sia in qualche modo collegabile ad una persona fisica. Quest'ultima può essere identificata attraverso il nome o in altro modo, ad esempio attraverso una foto.

Sono dati personali anche quelle informazioni che possono consentire di identificare una persona in via indiretta, ad esempio un numero di telefono, una targa automobilistica, un codice fiscale.

Sono soggetti al Regolamento anche i dati *"pseudonimizzati"*, ovvero quei dati resi anonimi ma per i quali vi è la ragionevole probabilità che possano essere ricollegati ad una persona fisica utilizzando altre informazioni, tenuto conto dei costi e del tempo necessario per risalirvi.

Per il trattamento di dati di massa (c.d. **big data**) si può ricorrere alla pseudonimizzazione in modo da poterli trattare in forma anonima per dati statistici o per ricerche scientifiche, ma sono soggetti comunque all'applicazione del Regolamento.

In particolare per il trattamento di queste masse di dati sono richieste cautele particolari, ad esempio i codici che consentono di risalire alla persona *"anonimizzata"* (c.d. **singling out**) devono essere conservati in sede separata e protetti con particolari accorgimenti tecnici.

Gli unici dati che non sono trattati dal Regolamento sono i **dati anonimi**, ovvero quelli che non possono essere ricollegati in modo irreversibile ad una persona fisica.

I dati personali possono essere **generici o sensibili** e per questi ultimi è previsto un **trattamento particolare.**

I dati sensibili sono quelli che si rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, biometrici, i dati relativi alla salute, alla vita sessuale o all'orientamento sessuale.

Le informazioni relative alla situazione economica di una persona sono dati generici e non sensibili.

Un trattamento particolare hanno poi i dati giudiziari relativi alle **condanne penali.**

Cos'è un trattamento dei dati

È un trattamento dei dati **qualsiasi operazione venga svolta in relazione a dati personali** incluso anche il solo **accesso** o la sola **visione**.

Si ha trattamento di dati anche se si utilizza un impianto di videosorveglianza o un drone con cui si visualizzano immagini di persone anche se non si effettua alcuna registrazione.

Il trattamento deve essere **lecito, corretto e trasparente.** L'informativa sul trattamento dei dati deve essere chiara e semplice in modo da fare capire senza difficoltà quali dati si stiano trattando e come.

Il trattamento deve avvenire per **finalità determinate, esplicite e legittime.** Quando si devono trattare dati per un certo scopo che viene indicato nell'informativa (ad esempio per inviare informazioni), quegli stessi dati non possono essere utilizzati per scopi diversi da quelli indicati che non potessero essere prevedibili per l'interessato.

I dati richiesti devono essere **pertinenti, adeguati e non eccedenti rispetto alla finalità.** Se si richiedono dati per inviare un prodotto acquistato online è eccedente chiedere informazioni sull'attività sportiva praticata o sui luoghi in cui si trascorrono le vacanze.

I dati devono essere **esatti** e **aggiornati.**

Il trattamento deve avvenire per lo **stretto tempo necessario** a svolgere l'attività per cui sono richiesti, salvo che la normativa nazionale non preveda un tempo più lungo.

Principio fondamentale nel trattamento dei dati è che esso deve avvenire con una **adeguata sicurezza.** Per sicurezza si intende la capacità di una rete o di un sistema informatico di resistere ad un evento imprevisto anche doloso che possa compromettere i dati.

Prima di iniziare un trattamento è quindi necessario effettuare la Valutazione d'impatto sulla protezione dei dati (DPIA o **Data Protection Impact Assessment**) per comprendere quali sono i rischi e come si possono evitare.

Nel caso in cui ci si renda conto che i rischi sono alti e non si riesce a contenerli, può essere necessario consultare in via preventiva l'**Autorità di controllo.**

La sicurezza è un requisito fondamentale perché possa avvenire il trasferimento di dati tra aziende dello stesso gruppo e affinché possano essere approvate le **Binding Corporate rules** (BCR).

Chi è il titolare del trattamento

Il titolare del trattamento è colui che **determina le finalità e le modalità del trattamento.** Nel caso di una società il titolare è la società stessa e non la persona che la rappresenta o che è incaricata di gestire la privacy.

Il titolare può nominare **uno o più responsabili esterni** a cui affidare alcune attività particolari (manutenzione informatica, gestione dati in cloud, hosting, ecc..) nel qual caso essi dovranno agire secondo le indicazioni date dal titolare ma potranno avere una certa autonomia dei mezzi usati per il trattamento vista la loro competenza specifica.

Il Regolamento prevede che il responsabile deve essere incaricato con un **contratto scritto.** Altra novità è che il responsabile può a sua volta nominare un altro responsabile per attività specifiche che a sua volta può delegare.

Il titolare resta sempre responsabile per la violazione della privacy, in alcuni casi in via solidale con il responsabile del trattamento nominato.

Possono esistere contitolari del trattamento, quando più soggetti trattano dati per uno stesso fine e concordano i relativi mezzi. In tal caso dovrà essere predisposto un accordo che stabilisca i compiti e le responsabilità.

A fianco del titolare e dei responsabili ci sono poi i dipendenti dell'azienda che devono essere istruiti sulle modalità del trattamento.

L'azienda è tenuta ad effettuare regolari **corsi di formazione** per i dipendenti.

Il Regolamento introduce poi la nuova figura del DPO **Data Privacy Officer**, che è una sorta di **consulente interno o esterno all'azienda** che consiglia il titolare sulle misure di sicurezza da adottare e che si interfaccia con gli interessati e le autorità Garanti della Privacy.

Il DPO deve essere **nominato obbligatoriamente solo in alcuni casi** (trattamento di dati fatto da autorità pubblica, oppure attività di monitoraggio regolare degli interessati su larga scala, oppure trattamento di dati sensibili o giudiziari su larga scala), mentre può sempre essere nominato in via facoltativa.

Le imprese **extra-UE** devono nominare un **Rappresentante nell'Unione** che le rappresenta e si occupa di ogni questione che possa comportare obblighi in capo all'impresa estera derivanti dal Regolamento.

La nomina di un Rappresentante nell'Unione è obbligatoria per le imprese extra-UE quando ricorrono tutte le seguenti condizioni: il titolare non è un soggetto pubblico; si applica l'art. 3.2 (offerta di beni o servizi nell'Unione anche senza richiesta di un pagamento); il trattamento non è occasionale; riguarda su larga scala dati sensibili o giudiziari; vi è un probabile rischio per gli interessati.

L'informativa e i diritti dell'interessato

Presupposto fondamentale di un trattamento lecito è che venga fornita all'interessato una **adeguata informativa sul trattamento dei suoi dati** prima che egli presti il consenso o comunque nel momento in cui sono raccolti se il consenso non è previsto come necessario.

L'informativa deve contenere le seguenti indicazioni:
- identità dell'interessato;
- finalità del trattamento;
- base giuridica del trattamento;
- eventuali obblighi di legge o di contratto e conseguenze del rifiuto;
- ambito di circolazione dei dati per destinatari;
- durata del trattamento;
- eventuale processo decisionale bastato unicamente su un trattamento automatizzato;
- i diritti dell'interessato.

L'informativa non deve essere necessariamente scritta anche se è opportuno che lo sia perché **deve essere fornita la prova del suo contenuto** e del fatto di averla data.

È consigliabile che l'informativa venga resa in due parti: una **sintetica** che indica il contenuto minimo della stessa ed una più **estesa**, a cui la prima rimanda, che sia invece più ampia.

L'informativa deve essere **chiara**. Meglio usare espressioni colloquiali semplici che un linguaggio tecnico-giuridico troppo articolato.

I diritti dell'interessato sono:
- diritto di accesso ai dati che lo riguardano;
- diritto di rettifica e integrazione dei dati;
- diritto di limitazione del trattamento alla sola conservazione;
- diritto di revoca del consenso;
- diritto di cancellazione dei dati e diritto di oblio (right to be forgotten);
- diritto di opposizione al trattamento, ma solo nei casi previsti;
- diritto alla portabilità dei dati (data portability) trattati in modo strutturato.

Il consenso deve essere **informato, libero, specifico, inequivocabile e espresso.**

Non importa che sia scritto ma **deve risultare in modo chiaro la volontà dell'interessato di acconsentire al trattamento.** Il consenso deve essere prestato per ogni tipo di trattamento per cui il consenso ottenuto per l'archiviazione dei dati fiscali non è idoneo a consentire di utilizzare quegli stessi dati per finalità di marketing.

Il consenso deve poi essere *"esplicito"* nel caso di trattamento di dati sensibili, per attività decisionali basate su trattamenti automatizzati e nel caso di trasferimento di dati verso un paese terzo o un'organizzazione internazionale non adeguati.

7 La “base legale” del trattamento e il consenso

Il Regolamento muove dal presupposto che **il trattamento dei dati è illecito se non vi è una base legale che lo consente.**

Il consenso non è più l’unica base legale ma ve ne sono altre poste tutte sullo stesso piano del consenso. La base legale è diversa a seconda che si trattino dati comuni o dati sensibili.

La base legale per i dati comuni può essere rappresentata da uno dei seguenti elementi (art. 6.1):

- consenso dell’interessato;
- trattamento necessario per l’esecuzione di un contratto o di misure precontrattuali (ad es. invio preventivi);
- trattamento necessario per adempiere ad un obbligo legale;
- trattamento necessario per la salvaguardia degli interessi vitali dell’interessato o di altra persona fisica;
- trattamento necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri;
- trattamento necessario per un legittimo interesse del titolare se non prevalgono gli interessi e i diritti dell’interessato.

Tra i trattamenti che possono ritenersi **leciti** per esercizio di un legittimo interesse viene incluso anche il **marketing diretto** se effettuato a favore di clienti che possano attendersi un tale tipo di comunicazione in ragione del rapporto intercorso tra le parti. In ogni caso l’interessato deve essere sempre informato del suo **diritto di opporsi** a questo trattamento esercitando l’**opt-out**.

La base legale per i dati sensibili può essere rappresentata da uno dei seguenti elementi (art. 9.2):

- consenso esplicito dell’interessato;
- trattamento necessario per adempiere obblighi o esercitare diritti in materia di diritto del lavoro e della sicurezza sociale nella misura in cui è autorizzato dal diritto dell’Unione;
- trattamento necessario per tutelare interessi vitali dell’interessato o di altra persona fisica;
- trattamento effettuato nelle sue legittime attività e con adeguate garanzie da una fondazione, associazione o ente senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali se riguarda membri, ex membri o persone che hanno contatto con l’ente stesso.

Nel caso in cui l’art. 6.1 preveda garanzie maggiori rispetto all’art. 9.2, si applicheranno al trattamento dei dati sensibili anche le previsioni del primo articolo che si cumulano alle seconde.

NORMATIVA DI RIFERIMENTO
Regolamento dell'Unione Europea 2016/679

La responsabilità del titolare

Il Regolamento si basa sul principio di **responsabilizzazione del titolare** del trattamento.

Il principio di **Accountability** prevede che il titolare debba adottare le misure che garantiscano un trattamento conforme al Regolamento e che debba **dimostrarne la concreta attuazione e l'oggettiva efficacia.**

Il principio era già noto all'interno dell'Ordinamento giuridico italiano per ciò che concerne la normativa sulla Responsabilità delle Persone Giuridiche e delle Società, contenuta nel D.Lgs. 8 giugno 2001 n.31.

Per fare questo non sono previste delle misure specifiche da adottare, per cui spetta al titolare fare una valutazione per capire quale siano le più idonee apparendo, comunque, imprescindibile l'impostazione, in Azienda, di un vero e proprio *"Modello"* volto ad assicurare l'adeguamento e la conformità dei trattamenti effettuati alla normativa vigente.

Quindi il titolare dovrà prima di tutto effettuare una analisi preventiva delle misure da adottare per rendere i nuovi servizi ed i nuovi prodotti conformi al Regolamento (c.d. **Privacy by design**). In questo contesto potrebbe essere utile ricorrere a specialisti che potrebbero assumere il ruolo di **Data Protection Designer.**

Inoltre dovrà fare in modo che il rispetto delle previsioni del Regolamento avvenga il più possibile in modo automatico ed entri a fare parte del flusso informativo per evitare che non sia rispettato (c.d. **Privacy by default**).

La Privacy by design e la Privacy by defalut servono per **attuare** e per **dimostrare l'attuazione** del Regolamento ma anche per **delimitare il perimetro della responsabilità** del titolare.

Tra le misure che il titolare deve necessariamente attuare rientrano la DPIA, la nomina del DPO se ricorrono le condizioni di cui all'art. 37.1, l'adozione delle BCR per il trasferimento di dati extra-UE tra società infragruppo e, non ultimo, il **Registro dei trattamenti** (art. 30) in cui il titolare deve indicare tutti i trattamenti.

Il Registro dei trattamenti, la DPIA, gli archivi di nomine e incarichi sono poi strumenti essenziali per fornire la prova dell'attuazione delle misure previste.

Possono essere adottate anche misure volontarie, quali i meccanismi di gestione dei reclami e dei **data breach**, gli audit interni o esterni.

In caso di data breach il titolare è tenuto entro 72 ore ad avvisare l'Autorità di controllo ed anche l'interessato in caso di violazioni che possono comportare danni nella sua sfera personale.

9 Data protection e sicurezza informatica

L'adozione di misure efficaci di protezione dei dati personali ha un effetto importante anche per la **tutela di tutto il patrimonio informativo di un'impresa** che rappresenta un **valore inestimabile.**

Impostare un sistema di sicurezza informatica è quindi necessario non solo per **adempiere ad un obbligo di legge** ma per **difendersi da possibili fughe** o **furto di informazioni.**

La data protection è un'esigenza sempre più forte in funzione dello sviluppo tecnologico.

L'**Internet of Things**, IoT, immette sul mercato prodotti e servizi che acquisiscono informazioni senza che la persona spesso se ne renda conto. I **robot** a loro volta acquisiscono informazioni sulla vita delle persone che assistono.

Non a caso il 9 Maggio 2018 entra in vigore la Direttiva 2016/1148/UE NIS, **Network and Information systems security**, sulla cybersecurity che ha molti punti di contatto con il Regolamento privacy.

Il Regolamento deve poi coordinarsi con altre normative tra cui la Dir. 2000/31/CE sul commercio elettronico, la Convenzione CoE 108/1981 sul trattamento automatizzato di dati a carattere personale, l'art. 7 e 8 della Carta dell'Unione Europea che tutelano la vita privata e familiare ed il rispetto dei dati di carattere personale.

Protezione dei dati e privacy sono sempre più due facce della stessa medaglia tanto che è stato coniato il nuovo termine di ***"data protecy"*** per indicare la protezione dei dati anche dal punto di vista privacy.

È necessario che un'impresa adotti tutte le misure necessarie per tutelare se stessa ed i dati che tratta.

Per tutte le persone giuridiche operanti od intenzionate ad operare sul territorio italiano, siano esse appartenenti a paesi UE che extra-UE, è necessario valutare l'adeguamento, tramite l'adozione di un apposito **Modello organizzativo**, alla normativa contenuta nel **D.Lgs.231/2001** al fine di contrastare il rischio di incorrere nelle pesantissime sanzioni dalla stessa previste.

Tale normativa emanata in attuazione della Convenzione OCSE sulla corruzione di pubblici ufficiali stranieri nelle operazioni commerciali internazionali firmata a Parigi il 17 dicembre 1997, recepisce la dottrina del ***"respondeat superior"*** già vigente negli USA per effetto della disciplina del **Foreign Corrupt Practise Act** successivamente ampliata e precisata dalle **Federal Sentencing Guidelines** statunitensi del 1991 e dalle **Ad hoc Advisory Group in the Organizational Sentencing** che fanno riferimento, là a soli fini attenuanti della responsabilità, ai concetti di efficacia del modello organizzativo e di culpability of the organization attenuata da *"existence of an effective compliance and ethics program; self-reporting, cooperation, or accemptance of responsibility."*

Normative similari si ritrovano, a livello mondiale, in Canada (sez.22.1 e 732.1 -3.1- Codice Penale canadese) nel Regno Unito (Mousell Bros v London and North Western Rly Co [1917] 2 KB 836; Griffiths v Studebakers Ltd [1924] 1 KB 102; Ltd v Woodward[1972] AC 824; Supermarkets v Nattrass [1972] AC 153), in Giappone, in Germania (Ordnungswidrigkeiten del 24 maggio 1968 solo per i profili amministrativi), in Russia (art.2.10 del codice degli illeciti amministrativi del 20.12.2001) ed in Francia (art.121-2 Codice Penale francese del 1994).

Tale normativa, che in Italia riguarda una

vasta serie di **gravi illeciti** (tra i quali i reati ambientali, i reati societari in materia di bilancio, di comunicazioni sociali e di utilizzo di informazioni sociali privilegiate, i reati contro la Pubblica Amministrazione… etc.), include anche i reati strettamente correlati al **settore della sicurezza e dell'attività informatica aziendale** ed al trattamento, *latu sensu*, di dati, informazioni e beni immateriali in ambito aziendale.

Proprio con riguardo a tale specifico settore il corretto adeguamento alla normativa privacy con l'efficace attuazione delle prescrizioni normative previste, costituisce il minimo ed imprescindibile presidio e punto di partenza nell'adozione di un Modello 231 a contrasto del rischio di incorrere nella responsabilità 231 per i reati informatici e per la violazione del diritto d'Autore

Le sanzioni

10

Il Regolamento prevede le **violazioni che devono essere sanzionate** e gli importi massimi applicabili.

Per valutare gli importi adeguati si dovrà tenere conto di **diversi parametri** ma hanno grande importanza le misure adottate dal titolare.

Nel comminare la sanzione amministrativa si tiene conto tra l'altro proprio delle misure tecniche e organizzative adottate dal titolare, del rispetto della privacy by-design e by-default, dell'entità del pregiudizio arrecato, dell'eventuale colpa o dolo del titolare.

È quindi evidente che **una buona organizzazione della privacy è indispensabile** anche per ridurre il rischio di vedersi comminare sanzioni ed anche per ridurre la loro quantificazione.

La misura massima applicabile è infatti altissima:

a. massimo di **€ 10.000.000** o, per le imprese, fino al **2% del fatturato mondiale** annuo se superiore (art. 83.4) in caso ad esempio di violazione dei seguenti obblighi:
- misure di protezione by-design, by-defualt;
- nomina del rappresentante del titolare o dei responsabili non stabiliti nell'UE;
- accordo tra contitolari per le responsabilità;
- consenso dei minori in merito a servizi della società dell'informazione;
- tenuta del Registro dei trattamenti;
- adozione di misure di sicurezza adeguate;
- comunicazione di data breach;
- DPIA;
- designazione del DPO.

b. massimo di **€ 20.000.000** o, per le imprese, fino al **4% del fatturato mondiale** annuo se superiore (art. 83.6, 83.6) in caso ad esempio delle seguenti violazioni:
- principi generali del trattamento dei dati;
- violazione condizioni di liceità, per il consenso o per la revoca;
- violazioni norme per il trattamento di dati particolari, sensibili o giudiziari;
- mancato rispetto diritti dell'interessato;
- mancato rispetto principi per il trasferimento di dati extra-UE;
- violazione di norme nazionali in materia di rapporti di lavoro, archivi storici, ricerca scientifica.

Le sanzioni amministrative irrogate dall'**Autorità di Controllo** sono sottoposte al ricorso giurisdizionale ed al giusto processo (art. 78).

Le sanzioni saranno applicate al titolare, ma potrebbero riguardare anche il responsabile, il DPO o altri soggetti coinvolti nel trattamento.

La Compliance al Regolamento

Vi aiutiamo ad adeguarvi e a non correre rischi

Adeguarsi al Regolamento non è semplice ma è un lavoro necessario che può comportare molti benefici all'impresa.

I DATI PERSONALI RAPPRESENTANO UN VALORE E PROTEGGERLI È IMPORTANTE

Il nostro studio **progetta la privacy compliance** in combinazione con impegni di segretezza e con misure tecniche adeguate per ridurre il rischio di perdere informazioni preziose magari a vantaggio di concorrenti.
L'adeguamento tecnico e contrattuale devono avvenire contestualmente per fornire le massime garanzie.
Valutiamo spesso l'introduzione del **Modello organizzativo 231/2001** per evitare o ridurre il rischio di responsabilità derivante dalla commissione di alcuni reati presupposto.

> **La nostra *esperienza* al vostro *servizio***

IL NOSTRO METODO PRIVACY FULL CONSENTE UN ADEGUAMENTO RAPIDO ED EFFICIENTE

È modulare e può essere parzializzato ma la perfetta compliance si ottiene adottando il metodo in modo integrale.

SCOPRI TUTTE LE SUE CARATTERISTICHE

Privacy Full

Le caratteristiche del nostro metodo, punto per punto

1. VALUTAZIONE PRELIMINARE

- Esame dell'attività svolta dal Cliente e dei suoi stabilimenti
- Valutazione dell'applicabilità del Regolamento

2. VALUTAZIONE SPECIFICA

- Individuazione dei prodotti e servizi offerti e del tipo di dati trattati
- Individuazione degli obiettivi del cliente
- Esame della struttura aziendale del Cliente
- Esame delle misure di sicurezza attualmente adottate dal Cliente

3. PROGETTAZIONE DELLA PRIVACY COMPLIANCE

- Elaborazione prospetto dati, modalità, soggetti incaricati.
- Studio degli adempimenti e delle misure di sicurezza da adottare
- Impostazione della **Privacy by design** per i prodotti/servizi
- Impostazione della **Privacy by default** per i prodotti/servizi
- Impostazione della Privacy Policy per i siti Internet e l'e-commerce
- Elaborazione del DPIA **Data Protection Impact Assessment**

4. ATTUAZIONE DELLA PRIVACY COMPLIANCE

- Individuazione delle cariche e delle nomine
- Predisposizione dei contratti necessari
- Predisposizioni informative privacy e moduli di consenso se necessari
- Adozione del Registro dei trattamenti
- Adozione delle misure di sicurezza concordate
- Eventuale individuazione e nomina del DPO **Data Privacy Officer**
- Eventuale individuazione e nomina del **Responsabile della Privacy nell'Unione**

5. PREDISPOSIZIONE MODELLO 231/2001

- Adozione ed efficace attuazione del modello organizzativo per evitare o limitare la responsabilità derivante da alcuni reati (ad esempio reati informatici, ambientali, reati societari, reati contro la violazione del diritto d'autore, reati di frode informatica e reati contro la P.A.)
- A livello pratico l'adozione di un Modello 231 consiste, previa attività preliminare di analisi dei rischi di reato concretamente riguardanti la persona giuridica (c.d risk assestment), nella redazione e predisposizione di una serie di documenti, protocolli e procedure interne in grado di ridurre i rischi di illecito tenendo l'Azienda esente dalla specifica responsabilità.
- L'attività si suddivide in tre distinte fasi:

a. Fase preliminare (analisi dei rischi).
b. Fase di adozione del modello (introduzione protocolli).
c. Fase di efficace attuazione del modello (concreta esecuzione delle procedure, comunicazione formale e pubblica del Modello 231 ai vari soggetti interessati).

Contatti

Turini Group

-

Viale Giacomo Matteotti, 25 – 50121 Firenze (Italy)
Tel: +39 055 5520647 | Fax: +39 055 4089025
info@turinigroup.com | www.turinigroup.com

Avv. Laura Turini

-

Intellectual Property Lawyer - Founding Partner
Responsabile del settore Internet & Software
turini@turinigroup.com

TURINI

Legale | Brevetti | Marchi & Design | Internet & Software