GUIDA AL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

JONES DAY® | One Firm Worldwide℠

INDICE

INTRODUZIONE

Nel mese di maggio 2016 l'Unione Europea ("UE") ha pubblicato il Regolamento Generale dell'UE sulla Protezione dei Dati ("GDPR"). Questo strumento legislativo di primaria importanza rappresenta il cambiamento più significativo nell'ambito del diritto alla protezione dei dati a livello UE dal 1995. Sarà vincolante dal 25 maggio 2018 e da quella stessa data costituirà diritto applicabile in tutti gli Stati Membri.

Il GDPR e' uno strumento giuridico di vasta portata, destinato ad avere un impatto significativo su tutte le società che effettuano trattamento dei dati personali, molte delle quali situate al di fuori dell'UE. Il GDPR, peraltro, aumenta le sanzioni associate al difetto di *compliance*, prevedendo sanzioni amministrative pecuniarie fino a 20 milioni di euro, o fino al 4% del fatturato annuo mondiale della società che trasgredisce. Inoltre, un certo numero di poteri assai ampi saranno attribuiti alle autorità di vigilanza competenti.

E' quindi opportuno per tutte le società esaminare il GDPR e prepararsi ad adempiere alla nuova normativa in materia di protezione dei dati nell'UE.

Questa guida, oltre ad illustrare brevemente sia le nuove regole applicabili ai sensi e per gli effetti della normativa in oggetto, sia i cambiamenti principali che seguiranno, e' redatta alla scopo di assistere gli utenti nella fase di preparazione alla vigenza del GDPR. La guida include anche un glossario conciso contenente i termini tecnici utilizzati nel GDPR; in corrispondenza di ogni voce è anche predisposto un breve elenco degli "adempimenti da eseguire" ai fini della *compliance*. Inoltre, faranno seguito a questa guida, incontri di aggiornamento, invio di documentazione per la consultazione pratica ai sensi del GDPR e quant'altro necessario per prestare adeguata assistenza alle società interessate dalla normativa di cui si tratta.

Ci auguriamo che questa guida diventi per Voi un utile strumento di consultazione. Nel caso abbiate necessità di ulteriori informazioni, non esitate a contattare gli avvocati elencati a pagina 25 della guida.

FINALITA'

ARTICOLI 2 E 3

Quadro Generale di Sintesi

Il GDPR si applica al trattamento automatizzato dei dati personali o al trattamento di dati personali destinati ad essere contenuti in un archivio. Sia l'ambito di applicazione materiale, che l'ambito di applicazione territoriale del GDPR sono di più ampio respiro rispetto alle corrispondenti previsioni contenute nella Direttiva per la Protezione dei Dati ("Direttiva").

Ambito di Applicazione Materiale

- Il GDPR si applica sia ai titolari del trattamento, che ai responsabili del trattamento.
- Il GDPR non si applica in un numero limitato di casi, come per esempio al trattamento di dati per attività a carattere esclusivamente personale o domestico.

Ambito di Applicazione Territoriale

Il GDPR si applica al trattamento dei dati:

- nell'ambito delle attività di uno stabilimento nell'UE; e
- effettuato da un titolare del trattamento o da un responsabile del trattamento che *non* è stabilito nell'Unione e riguarda dati personali di soggetti interessati che si trovano nell'UE, quando le attività si riferiscono a:
  - offerta di beni o la prestazione di servizi ai suddetti interessati; o
  - monitoraggio del comportamento di suddetti interessati.

Attività di Verifica Suggerite

- ✓ Identificare il trattamento di dati personali effettuato.
- ✓ Confermare quali sono gli stabilimenti nell'UE che trattano dati personali e quando tale trattamento si riferisce a situazioni in cui i beni e i servizi sono offerti nel mercato UE o quando gli interessati sono soggetti a monitoraggio nel territorio UE.
- ✓ Valutare se il trattamento dei dati è svolto in qualità di titolare o di responsabile del trattamento.
- ✓ Stabilire se un rappresentante UE sia o meno necessario.

BASI GIURIDICHE PER IL TRATTAMENTO DEI DATI

ARTICOLI 6, 7 E 8

Quadro Generale di Sintesi

Le basi giuridiche su cui si fonda il trattamento dei dati personali ai sensi e per gli effetti del GDPR sono in gran parte coincidenti con quelle fornite dalla Direttiva. Tuttavia, il GDPR pone nuove limitazioni con riferimento al consenso, al trattamento fondato sull'interesse legittimo del titolare ed al trattamento dei dati per fini ulteriori.

Basi Giuridiche per il Trattamento dei Dati Personali

Le basi giuridiche per il trattamento dei dati personali ai sensi del GDPR sono soddisfatte:

- Quando i soggetti interessati prestano il loro consenso; e
- Quando il trattamento dei dati risulta necessario al fine di:
  - Dare esecuzione a, o negoziare, un contratto con un soggetto interessato;
  - Adempiere ad un obbligo di legge;
  - Proteggere gli interessi fondamentali per la vita del soggetto interessato o di un'altra persona fisica nel caso in cui il soggetto interessato non sia in grado di prestare il proprio consenso;
  - Portare avanti un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; e
  - Perseguire scopi connessi ad interessi legittimi (senza pregiudizio ad alcun diritto o libertà fondamentali).

Nuove limitazioni con riferimento al consenso, al trattamento fondato su "interessi legittimi" ed al trattamento dei dati per fini ulteriori

- Al fine del trattamento dei dati fondato sul consenso, il titolare del trattamento deve essere nella posizione di potere provare che il consenso è stato liberamente prestato dal soggetto interessato, posto che la richiesta di consenso deve essere chiaramente discernibile.
- Il GDPR fornisce chiarimenti su quando "l'interesse legittimo" possa costituire il fondamento giuridico per il trattamento dei dati (per esempio: marketing diretto, prevenzione frodi, condivisione di dati personali all'interno di un gruppo societario per finalità legate all'amministrazione interna, garantire la sicurezza di rete e delle informazioni), ed impone che il titolare del trattamento informi i soggetti interessati ogni qualvolta lo stesso stia trattando dati su una base giuridica che poggia su interesse legittimo.
- Il GDPR stabilisce una serie di criteri che debbono essere presi in considerazione quando si deve determinare se il trattamento dei dati ad un nuovo scopo sia compatibile con lo scopo originario per cui i dati sono stati inizialmente raccolti.

continua a pagina 4

Attività di Verifica Suggerite

- ✓ Valutare le basi giuridiche per il trattamento in corso dei dati e verificare che tali basi siano ancora valide e legittime ai sensi e per gli effetti del GDPR.
- ✓ Assicurarsi che il consenso sia stato prestato in osservanza dei nuovi requisiti di legge e che il titolare del trattamento possa effettivamente dimostrarlo.
- ✓ Quando il trattamento si fonda sull' "interesse legittimo", assicurarsi che:
  - Il bilancio del rapporto tra l' interesse e i diritti del soggetto interessato sia documentato; e
  - Quando il titolare del trattamento pone a fondamento del trattamento il suo interesse legittimo, questa specifica circostanza sia ricompresa tra le informazioni fornite al soggetto interessato.
- ✓ Assicurarsi che vengano adeguatamente documentate le ragioni poste a fondamento di determinate decisioni cosicché possano essere utilizzate per trattamenti successivi.

DIRITTI DELLE PERSONE FISICHE

ARTICOLI 12-17, 19, 20 E 21

Quadro Generale di Sintesi

Ai titolari del trattamento si richiede di essere particolarmente trasparenti con i soggetti interessati a cui sono conferiti ulteriori diritti di accesso ai dati, nonché nuovi importanti diritti tra cui domandare la rettifica o la cancellazione dei loro dati personali, così come limitare ulteriori trattamenti degli stessi dati di loro pertinenza.

Contenuto dell'Informativa

A ciascuna persona fisica devono essere fornite le informazioni relative alle modalità di trattamento dei dati a lui o lei riferiti, inclusi tutti i dettagli che riguardano:

- L'identità ed i contatti di riferimento del titolare del trattamento;
- Ciascun responsabile del trattamento dei dati;
- Lo scopo e la base giuridica per effettuare il trattamento;
- Qualsiasi "interesse legittimo" posto a fondamento del trattamento dei dati;
- Qualsiasi trasferimento internazionale e tutele applicabili;
- Il periodo di conservazione dei dati o i criteri per determinarlo;
- Il diritto ad avere dati portabili, nonché il diritto di obiettare al trattamento, di richiedere limitazioni e di revocare il consenso prestato al trattamento;
- Il diritto di dare corso a reclami innanzi ad una autorità di vigilanza; e
- Qualsiasi requisito previsto dalla legge o per accordo contrattuale che imponga di fornire dati e che stabilisca anche le conseguenze rilevanti nel caso in cui tali dati non siano forniti.

Suddette informazioni devono essere concise, conformi ai canoni di trasparenza ed intellegibili; devono essere redatte in formato facilmente accessibile; devono essere scritte con chiarezza e con un linguaggio semplice, in particolare quando sono indirizzate a bambini.

Quando i dati sono ottenuti in maniera diretta, il titolare del trattamento sarà chiamato sia a spiegare quali tra quelle informazioni devono essere obbligatoriamente fornite, sia a chiarire le conseguenze in caso di mancato adempimento. Quando i dati sono ottenuti in maniera indiretta, il titolare del trattamento deve rivelare la fonte di tali informazioni, incluse le fonti di comune accesso pubblico.

Diritto di accesso

Ai soggetti interessati è conferito il diritto di ottenere copie dei loro dati personali insieme ai dettagli più importanti relativi alle modalità di trattamento di tali dati. Le persone fisiche godono di un diritto più ampio di accesso ai loro dati.

continua a pagina 6

- I titolari del trattamento non possono addebitare alcuna tariffa, ma possono addebitare ragionevoli spese amministrative legate alle copie aggiuntive.
- Devono essere forniti alle persone fisiche tutti i dettagli relativi alla divulgazione internazionale dei dati; il periodo di conservazione degli stessi; i diritti di rettificare e cancellare i dati, le limitazioni al trattamento; i diritti di opporsi al trattamento e di dare corso a reclami innanzi ad una autorità di controllo.
- I titolari del trattamento devono rivelare qualsiasi fonte che sia una terza parte, nonché la portata significativa e le conseguenze legate ad ogni trattamento eseguito a mezzo di processi decisionali automatizzati.

Diritti dei Soggetti Interessati

Ai soggetti interessati sono ascritti importanti diritti in relazione ai loro dati personali, inclusi i seguenti:

- Il diritto di chiedere che i dati personali siano rettificati senza ritardo e il diritto che i dati personali incompleti vengano completati;
- Il dritto di ottenere la cancellazione dei dati personali ("diritto all'oblio") quando il Trattamento non risulti più necessario, o il consenso sia stato revocato, o vengano meno gli interessi legittimi da tutelare, o il trattamento dei dati sia illegittimo, o la cancellazione sia stabilita dalla legge. In tali casi, il titolare del trattamento deve adottare misure adeguate per informare altri titolari nel caso in cui abbia reso pubblici quei dati;
- Il diritto di prevenire ulteriori attività di trattamento dei dati personali ("limitazioni") quando sorge una controversia in merito all'accuratezza, o quando sia accertata una obiezione al trattamento, o quando il trattamento è illegittimo ed il soggetto interessato si oppone alla cancellazione, o quando i dati non sono più richiesti dal titolare del trattamento, ma il soggetto interessato richiede quei dati per l'esercizio di un suo diritto o di una sua difesa; e
- Il diritto di richiedere che i dati forniti ai fini del trattamento dai soggetti interessati che vi abbiano acconsentito, o siano vincolati da obbligazioni contrattuali, siano resi disponibili in un formato comunemente usato e leggibile da macchinari elettronici, cosicché possano essere trasmessi ad un altro titolare del trattamento ("portabilità dei dati").

I titolari del trattamento devono notificare ai destinatari dei dati ogni rettifica, cancellazione e limitazione, salvo che ciò sia impossibile o richieda sforzi eccessivi. In aggiunta, nel caso in cui sia loro richiesto, i titolari del trattamento debbono informare i soggetti interessati circa l'identità dei destinatari dei dati.

Attività di Verifica Suggerite

- ✓ Controllare le informative e le *policy* sulla *privacy*.
- ✓ Controllare le procedure di accesso dei soggetti interessati.
- ✓ Valutare le modalità di *compliance* con il requisito di portabilità dei dati e con le richieste degli interessati.
- ✓ Considerare le implicazioni per i sistemi IT derivanti dal diritto all'oblio.
- ✓ Considerare l'opportunità e le modalità attraverso cui fornire risposte automatizzate alle persone fisiche.

MECCANISMI DI *GOVERNANCE*

ARTICOLI 24, 25, 30, 32, 35, 37, 40 E 42

Quadro Generale di Sintesi: nuove norme

A differenza della Direttiva, il GDPR impone che i titolari del trattamento implementino programmi a garanzia della *compliance* che possano essere provati davanti alle autorità di vigilanza e ai soggetti interessati.

Misure Tecniche ed Organizzative Appropriate

I titolari del trattamento devono adottare misure tecniche ed organizzative appropriate. Queste possono includere:

- L'adozione di *policy* sulla protezione dei dati;
- L'adesione a codici di condotta approvati; e
- L'adesione a meccanismi di certificazione automatica.

Protezione dei dati sin dalla progettazione (*privacy by design* e *by default*)

I titolari del trattamento devono adottare misure tecniche ed organizzative appropriate, che siano progettate al fine di dare attuazione ai principi nell'ambito della protezione dei dati (come la pseudonimizzazione e la minimizzazione dei dati) da impiegarsi al momento della determinazione dei mezzi utilizzabili per il trattamento e durante il trattamento stesso. In via ordinaria, solamente i dati necessari al raggiungimento di obiettivi specifici dovrebbero essere trattati.

Valutazione dell'Impatto della Protezione dei Dati

Prima che il trattamento abbia luogo, i titolari del trattamento devono svolgere una valutazione sull'impatto di qualsivoglia attività che rappresenti una minaccia significativa per i diritti dei soggetti interessati (per esempio, decisioni basate su trattamenti o profilazioni automatizzati, trattamento di dati sensibili su larga scala e monitoraggio automatico su larga scala di un'area accessibile al pubblico).

Nomina di un Responsabile della Protezione dei Dati

I titolari ed i responsabili del trattamento sono tenuti, ciascuno, a nominare un un *data protection officer* ("DPO") nel caso in cui le loro attività caratteristiche prevedano un'attività di monitoraggio dei soggetti interessati che sia regolare, sistematica e su larga scala, oppure prevedano il trattamento su larga scala di dati sensibili. Anche le autorità o gli enti pubblici devono nominare un DPO. È possibile nominare un DPO anche su base volontaria, tenendo a mente che il diritto nazionale di ciascuno Stato Membro potrebbe imporre la designazione di un DPO in casi non specificamente previsti dal GDPR.

Documentazione (registri del Trattamento)

I titolari del trattamento devono tenere registri relativi alle attività trattate che contengano specifiche informazioni obbligatorie (inclusi: le finalità del trattamento, una descrizione delle categorie di soggetti interessati, i dati personali e i destinatari dei dati, le misure tecniche ed organizzative implementate, e qualsiasi trasferimento di dati verso paesi terzi).

Attività di Verifica Suggerite

- ✓ Attribuire le relative responsabilità e stabilire un *budget* per la *compliance* relativa alla protezione dei dati, nonché assicurarsi il supporto del *management*.
- ✓ Controllare il livello di *compliance* attuale (ciò include il controllo delle *policy* sulla protezione dei dati e sulla sicurezza informatica attualmente adottate, nonché l'identificazione delle attività di trattamento dei dati di riferimento).
- ✓ Verificare eventuali carenze nel sistema di *governance* dei dati.
- ✓ Aggiornare le procedure esistenti al fine di garantire la *compliance*, nonché sviluppare nuove procedure ove necessario.
- ✓ Determinare se la nomina di un DPO è, o meno, obbligatoria; altrimenti, prendere in considerazione una nomina su base volontaria.

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO E RELATIVI ACCORDI

ARTICOLI 28-33 E 37

Quadro Generale di Sintesi: nuove norme

Il GDPR specifica i requisiti applicabili agli accordi stipulati tra i titolari del trattamento ed i responsabili del trattamento di dati personali. Tali requisiti sono maggiormente dettagliati rispetto alle previsioni della Direttiva.

Inoltre, il GDPR stabilisce nuovi obblighi che vanno a gravare sul responsabile del trattamento.

Requisiti applicabili agli accordi stipulati tra i titolari ed i responsabili del trattamento

- I titolari del trattamento possono solo impiegare responsabili che forniscono quelle sufficienti garanzie tecniche e organizzative richieste dal GDPR.
- Ogni accordo tra il titolare ed il responsabile del trattamento deve essere in forma scritta.
- Gli accordi per il trattamento dei dati devono prevedere che:
  - Il responsabile tratti i dati personali esclusivamente sulla base delle istruzioni ricevute dal titolare;
  - Il responsabile deve garantire che i suoi dipendenti siano vincolati da obblighi di riservatezza;
  - Il responsabile deve attuare le misure tecniche ed organizzative appropriate per garantire un livello di sicurezza dei dati personali che sia adeguato al rischio;
  - Il responsabile non può subappaltare il trattamento dei dati personali senza la previa autorizzazione scritta del titolare;
  - Qualsiasi accordo tra il responsabile ed il *sub* responsabile deve sancire gli stessi obblighi relativi alla protezione dei dati personali che sono previsti dall'accordo con il titolare;
  - Il responsabile deve prestare assistenza al titolare nel momento in cui si garantisce la *compliance* con gli obblighi relativi alla sicurezza, la valutazione dell'impatto della protezione dei dati, e nel caso di consultazioni preventive con l'autorità di vigilanza competente ("Garante") per il trattamento di dati ad alto rischio;
  - Il responsabile deve cancellare o restituire i dati personali quando il trattamento e' stato completato; e
  - Il responsabile deve fornire al titolare tutte le informazioni necessarie a dimostrare la propria *compliance*, così da permettere lo svolgimento delle verifiche e contribuire alle stesse.

Obblighi Imposti direttamente al responsabile del trattamento

Ad eccezione di casi specifici, nelle imprese e nelle organizzazioni che impiegano meno di 250 persone:

- Il responsabile deve tenere un archivio scritto per tutte le categorie di dati trattati per conto di ogni titolare del trattamento; e
- Il responsabile deve mettere tale archivio a disposizione dell'autorità di vigilanza competente su richiesta.

In aggiunta, ciascun responsabile deve:

- Adottare appropriate misure tecniche ed organizzative al fine di garantire un adeguato livello di sicurezza;
- Compiere i passi necessari per garantire che i membri dello *staff* aventi accesso ai dati personali trattino tali dati solamente sulla base delle istruzioni ricevute dal titolare del trattamento;
- Notificare senza indugio al titolare ogni violazione dei dati personali, una volta appresa; e
- Designare, in casi specifici, un DPO, incluso quando: (i) il trattamento richiede regolare e sistematico monitoraggio dei soggetti interessati su larga scala, e (ii) i dati relativi a condanne penali e reati sono in corso di trattamento.

Attività di Verifica Suggerite

- ✓ I titolari debbono garantire che tutti gli accordi sottoscritti con i responsabili siano conformi alle disposizioni del GDPR.
- ✓ I responsabili devono determinare quali archivi in relazione al trattamento debbano essere tenuti per ciascun titolare.
- ✓ I responsabili devono adottare misure tecniche ed organizzative appropriate al fine di garantire un appropriato livello di sicurezza per i dati personali e devono anche adottare delle *policy* sul sistema di monitoraggio delle violazioni.
- ✓ I responsabili devono determinare quando e come un DPO sia necessario.

SICUREZZA DEI DATI E NOTIFICA RELATIVA ALLA VIOLAZIONE DEI DATI PERSONALI

PARAGRAFI 32–34 E 37

Quadro Generale di Sintesi: nuove norme

I titolari del trattamento e i responsabili sono d'ora in avanti soggetti all'obbligo di adottare un sistema di monitoraggio delle violazioni. Ove possibile, i titolari dovranno dare notizia di ogni violazione fondamentale nel giro di 72 ore.

Requisiti sulla Sicurezza dei Dati

- I titolari e i responsabili debbono, ciascuno, applicare le misure tecniche ed organizzative di sicurezza volte a garantire un adeguato livello di protezione dei dati personali.
- Ove opportuno, tra le misure di sicurezza debbono essere incluse la pseudonimizzazione e la criptazione, la possibilità di ripristinare i dati personali tempestivamente, nonché eseguire valutazioni e test su base regolare.
- I titolari e i responsabili che svolgono attività di trattamento o monitoraggio su larga scala devono nominare un DPO.

Regole Applicabili alla Notifica relativa alla Violazione di Dati Personali

I titolari del trattamento e i responsabili sono d'ora in avanti soggetti ad un regime di notifica relativa alla violazione di dati personali.

- I titolari devono riportare ogni violazione dei dati personali all'autorità di vigilanza competente, senza indugio (ove possibile, entro 72 ore dalla notizia della violazione), salvo la violazione non sia idonea a mettere a rischio i diritti e le libertà del soggetto interessato.
- I titolari devono notificare la violazione ai soggetti interessati su cui si ripercuotono gli effetti di tali violazioni della tutela dei loro dati personali nel caso in cui suddette violazioni pongano una minaccia significativa ai diritti e alle libertà dei soggetti interessati.
- In ogni caso, i responsabili debbono riportare ogni violazione dei dati personali ai titolari, senza indugio.

Attività di Verifica Suggerite

- ✓ Adottare procedure per identificare incidenti relativi alla sicurezza, rispondere ed eseguire le notifiche necessarie.
- ✓ Allocare le responsabilità relative alla sicurezza dei dati personali.
- ✓ Assicurarsi che i responsabili siano vincolati da un obbligo di riportare ogni violazione dei dati personali e di adottare le misure di sicurezza adeguate.
- ✓ Verificare la copertura dei rischi informatici.
- ✓ Stimare i *test* sulla sicurezza e sui comportamenti quotidiani.
- ✓ Valutare il livello di sicurezza e condurre costantemente verifiche.

CODICI DI CONDOTTA E CERTIFICAZIONI

ARTICOLI 40-43

Quadro Generale di Sintesi: nuove norme

Il GDPR prevede che, in particolare a livello europeo, l'approvazione dei rispettivi codici di condotta e l'accreditamento delle relative certificazioni siano di supporto ai titolari e ai responsabili del trattamento quando chiamati a dimostrare la loro *compliance* con le norme sulla protezione dei dati. I codici di condotta, nonostante siano richiamati dalla Direttiva, giocano un ruolo meno significativo nella Direttiva stessa rispetto al loro ruolo nel GDPR. Ai sensi del GDPR, le certificazioni sono regolate a livello pan-europeo per la prima volta.

Codici di Condotta

- Ai sensi del GDPR, le associazioni ed altri enti rappresentativi possono redigere, modificare o estendere la portata di un codice di condotta allo scopo di specificare come il GDPR si applichi in certi settori industriali.
- Ogni codice di condotta deve essere sottoposto all'attenzione dell'autorità di vigilanza competente ai fini dell'approvazione, registrazione e pubblicazione.
- Nel caso in cui ricorrano trattamenti transfrontalieri, il relativo codice di condotta deve essere sottoposto al Comitato Europeo per la Protezione dei Dati ("Comitato"), che rende un opinione a riguardo. La Commissione Europea ("Commissione") ha la facoltà di dichiarare che quel codice di condotta gode di generale validità all'interno dell'UE. Il Comitato si occuperà di collocare tutti i codici di condotta in un registro pubblicamente accessibile.
- La *compliance* con il relativo codice di condotta è soggetta a controlli da parte di enti accreditati. Nel caso in cui si verifichino violazioni, la società interessata potrebbe essere sospesa come soggetto che aderisce al codice, e segnalata all'autorità di vigilanza competente.
- L'adesione al codice di condotta è dimostrazione che i titolari ed i responsabili dei dati collocati al di fuori dello Spazio Economico Europeo ("SEE") hanno adottato tutele adeguate volte a rendere possibile il trasferimento di dati da paesi appartenenti allo SEE verso quelli all'esterno dello SEE.

Meccanismo di Certificazione

- La realizzazione di meccanismi di certificazione per la protezione dei dati è consigliata ai fini della dimostrazione dell'effettiva *compliance*.
- L'adesione a meccanismi di certificazione per la protezione dei dati è dimostrazione che i titolari ed i responsabili dei dati collocati al di fuori dello SEE hanno adottato tutele adeguate volte a rendere possibile il trasferimento di dati da paesi appartenenti allo SEE verso quelli all'esterno.

- L'autorità di vigilanza competente o il Comitato dovranno approvare i relativi criteri di certificazione. Il Comitato potrebbe elaborare criteri applicabili ad una certificazione comune, come per esempio il sigillo europeo per la protezione dei dati.
- Le certificazioni saranno emesse dagli enti accreditati per la certificazione. Gli accreditamenti per gli enti di certificazione saranno emessi per periodi di soli cinque anni e potranno essere rinnovati in costanza dei requisiti di accreditamento; altrimenti, saranno revocati. Le certificazioni saranno valide per periodi di tre anni al massimo e potranno essere rinnovate in costanza dei requisiti per la certificazione; altrimenti, saranno revocate.
- Il Comitato dovrà tenere un registro pubblicamente consultabile contenente tutti i meccanismi di certificazione.

Attività di Verifica Suggerite

✓ Identificare o costituire associazioni o enti rappresentativi in grado di sviluppare codici di condotta, con particolare riferimento ai trattamenti transfrontalieri dei dati.

✓ Monitorare gli enti di accreditamento e certificativi e prendere in considerazione l'ipotesi di richiedere le relative certificazioni.

✓ Acquisire familiarità con i vari schemi di certificazione ed informarsi debitamente circa le certificazioni, nel momento in cui si seleziona il prestatore del servizio.

Quadro Generale di Sintesi: nuove norme

Come nella Direttiva, il GDPR richiede di fornire adeguate motivazioni a giustificazione del trasferimento di dati verso paesi ubicati al di fuori dello SEE. Il GDPR ha ampliato il catalogo di possibili giustificazioni per il trasferimento dei dati includendo i codici di condotta ed i meccanismi di certificazione.

- La Commissione ha la facoltà di adottare decisioni di adeguatezza per mezzo delle quali specifici paesi terzi, o territori, o regioni all'interno di tali paesi, sono ritenuti idonei ad offrire un adeguato livello di protezione per i trasferimenti transfrontalieri. Trasferimenti verso tali paesi, territori, o regioni all'interno di quei paesi non richiedono alcuna autorizzazione specifica. Il catalogo esistente di paesi terzi che soddisfano i criteri di adeguatezza che è redatto dalla Commissione è tutt'ora in vigore ed include *il Privacy Shield Uniti* applicabile al trasferimento di dati dai paesi dello SEE agli Stati Uniti.
- In assenza di qualsivoglia decisione sull'adeguatezza, i dati personali possono essere trasferiti verso i paesi terzi ubicati al di fuori dello SEE solamente a condizione che vi siano adeguate tutele in essere. Tali tutele includono clausole *standard* per la protezione di dati che possono essere adottate o approvate dalla Commissione, così come Norme Vincolanti d'Impresa ("BCRs"), il cui contenuto è stato ora specificato e dettagliato nel GDPR. Gli altri trasferimenti soggetti a specifiche tutele sono quelli permessi quando sono adottati o un codice di condotta approvato, o un meccanismo di certificazione approvato o un accordo tra autorità pubbliche.
- In assenza di una decisione sull'adeguatezza o di tutele adeguate, i trasferimenti transfrontalieri sono possibili solo se almeno una delle seguenti condizioni è soddisfatta: (i) il soggetto interessato ha rilasciato consenso esplicito una volta reso edotto del possibile rischio associato a tali trasferimenti; (ii) il trasferimento è necessario ai fini di adempimenti contrattuali o di implementazione di misure pre-contrattuali intercorrenti tra il soggetto interessato e il titolare; (iii) il trasferimento è necessario per adempiere ad un contratto concluso con il titolare del trattamento nell'interesse del soggetto interessato; (iv) il trasferimento è necessario alla luce di importanti ragioni di interesse pubblico; (v) il trasferimento è necessario al fine di supportare o esercitare una pretesa giuridica o una difesa; (vi) il trasferimento è necessario a proteggere gli interessi fondamentali del soggetto interessato, o di altri individui, quando l'interessato non sia legalmente capace o fisicamente nella posizione di prestare consenso; e (vii) il trasferimento avviene da un registro pubblico.

- Il GDPR affronta anche il tema della raccolta di documenti in ottemperanza a un ordine di *discovery* in paesi terzi e a tal fine dispone che sentenze o decisioni di autorità amministrative di paesi terzi che richiedono il trasferimento di dati personali possono essere riconosciute ed avere esecuzione solamente nel caso in cui si basino su accordi internazionali, come per esempio trattati di mutua cooperazione internazionale esistenti tra il paese terzo che avanza la domanda di trasferimento e l'UE o uno Stato Membro, senza che ciò pregiudichi le basi di cui sopra per il trasferimento di dati ai sensi del GDPR.

Attività di Verifica Suggerite

- ✓ Tracciare mappe che indichino i flussi di dati.
- ✓ Valutare il fondamento di ogni trasferimento transfrontaliero esistente verso paesi al di fuori dello SEE.
- ✓ Riesaminare il contenuto delle BCRs al fine di garantire la *compliance* con i requisiti stabiliti dal GDPR.
- ✓ Prendere in considerazione nuove basi per effettuare il trasferimento dei dati, come per esempio codici di condotta e certificazioni.
- ✓ Seguire attentamente gli sviluppi legislativi in materia di decisioni di adeguatezza.

CONTROLLI EFFETTUATI DALLE DPA (*Data Protection Authorities*)

ARTICOLI 51-76

Quadro Generale di Sintesi: nuove norme

Il GDPR fornisce regole dettagliate ed armonizzate circa l'organizzazione ed i poteri delle autorità di vigilanza. Stabilisce anche meccanismi di cooperazione e coerenza al fine di affrontare questioni relative a procedure transfrontaliere.

Autorità per la protezione dei dati

In ciascun Stato Membro dell'UE dovrà essere presente almeno una DPA.

- L'indipendenza delle DPA sarà rafforzata a mezzo di regole sulla costituzione delle DPA, nonché sulla nomina e sulla rimozione dall'incarico dei loro componenti, tra gli altri strumenti messi a disposizione.
- I compiti e i poteri delle DPA saranno ampliati, includendo così il potere di condurre verifiche ed accedere alle strutture dei titolari e dei responsabili.
- Il GDPR stabilisce il meccanismo dello "sportello unico" a mezzo del quale le DPA designano il DPA *leader* (prima di tutto sulla base dello stabilimento principale del responsabile) e cooperano al fine di adottare decisioni con riguardo al trattamento transfrontaliero dei dati.

Il Comitato Europeo per la Protezione dei Dati

Il Comitato Europeo per la Protezione dei Dati andrà a sostituire il gruppo di lavoro ex art. 29.

- Il Comitato sarà costituito da ciascun capo della DPA per ogni Stato Membro e dal Garante Europeo per la Protezione dei Dati ("GEDP"). Si avvantaggerà di un segretariato permanente, fornito dal GEDP, con base a Bruxelles.
- Il Comitato rende pareri, fornisce linee guida ed assicura un'applicazione coerente del GDPR.
- Il Comitato ha il potere di rendere decisioni vincolanti nel caso vi sia divergenza di vedute tra diverse DPA nel corso della procedura dello "sportello unico" (per esempio, decidere quale DPA dovrebbe essere l'autorità *leader*, o determinare il contenuto di una decisione finale in occasione della risoluzione di una controversia).

Attività di Verifica Suggerite

- ✓ Seguire da vicino gli sviluppi del sistema giuridico nazionale che potrebbero modificare le strutture delle DPA.
- ✓ Comprendere la natura dell'ampliamento dei poteri investigativi delle DPA ai fine della *compliance* della struttura interna.
- ✓ Determinare quale sarà l'autorità *leader* di vigilanza per la Vostra società.
- ✓ Essere preparati all'eventualità di dovere comparire davanti al Comitato ed appellare le sue decisioni.

RIMEDI GIURIDICI, RESPONSABILITA' E SANZIONI

ARTICOLI 77-84

Quadro Generale di Sintesi: nuove norme

Il GDPR fornisce rimedi giuridici ai soggetti interessati e allo stesso tempo impone responsabilità in capo ai titolari e ai responsabili del trattamento, così come sanzioni più severe, incluse sanzioni pecuniarie amministrative assimilabili a quelle previste dal regime antitrust in UE. A differenza della Direttiva, il GDPR identifica in maniera dettagliata le condizioni per irrogare le sanzioni pecuniarie amministrative ed il loro ammontare massimo.

Rimedi Giuridici

Ai soggetti interessati sono attribuiti i seguenti diritti che possono essere azionati contro i titolari ed i responsabili del trattamento:

- Il diritto di reclamo (tra l'altro a mezzo di associazioni) davanti alla DPA dello Stato Membro di residenza del soggetto interessato, o dove lavora abitualmente, o dove la violazione ha avuto luogo, inclusi i ricorsi in appello nel caso in cui la DPA non sia in grado di gestire il reclamo;
- Il diritto di impugnare le decisioni vincolanti della DPA davanti alle corti nazionali; e
- Il diritto di iniziare procedimenti giuridici davanti alle corti nazionali dello Stato Membro dove il titolare o il responsabile sono stabiliti, o della residenza del soggetto interessato.

Risarcimento del Danno e Responsabilità

Ai sensi del GDPR, il titolare ed il responsabile hanno l'obbligo di risarcire interamente il soggetto interessato per tutti i danni materiali ed immateriali che siano il risultato di violazioni delle disposizioni del GDPR. Ciò si applica anche quando più di un titolare o più di un responsabile, o entrambi, sono parimenti responsabili dei danni cagionati dal trattamento ("responsabilità solidale").

Sanzioni

Le DPA hanno il potere di irrogare sanzioni amministrative.

- In base al tipo di violazione, le sanzioni amministrative pecuniarie possono arrivare fino a 20 milioni di euro, o nel caso di imprese, fino al 4% del fatturato mondiale totale annuo, e si applicano al maggiore tra i due valori.
- Le sanzioni pecuniarie amministrative devono essere determinate sulla base dei criteri elencati nel GDPR e sono soggette al controllo giudiziale.
- Gli Stati Membri dell'UE hanno la facoltà di prevedere sanzioni aggiuntive, ivi incluse sanzioni penali.

Attività di Verifica Suggerite

- ✓ Tenere in considerazione le nuove responsabilità e le nuove sanzioni imposte ai fini del piano per la *compliance*.
- ✓ Valutare la possibile esposizione a responsabilità alla luce dei contratti con clienti e fornitori.
- ✓ Accertare quale sia la giurisdizione cui si è probabilmente soggetti in caso di procedimenti legali.
- ✓ Seguire da vicino gli sviluppi legislativi che potrebbero imporre ulteriori sanzioni.

GLOSSARIO

Binding Corporate Rules ("BCRs")	Le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune. (Art. 4(20), GDPR)
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. (Art. 4(11), GDPR)
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri. (Art. 4(7), GDPR)
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. (Art. 4(8), GDPR)

Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. (Art. 4(9), GDPR)
Soggetto interessato	Una persona fisica identificata o identificabile della quale si trattano i dati personali. (Art. 4(1), GDPR)
Regolamento generale sulla protezione dei dati (GDPR)	Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. (Art. 4(1), GDPR)

Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. (Art. 4(2), GDPR)
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica. (Art. 4(4), GDPR)
Terzo	Una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile. (Art. 4(10), GDPR)

CONTATTI

Dr. Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Elizabeth A. Oberle-Robertson
London
+44.20.7039.5204
erobertson@jonesday.com

Paloma Bru
Madrid
+34.91.520.3985
pbru@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Dr. Jörg Hladjk
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Giuseppe Mezzapesa
Milan
+39.02.7645.4001
gmezzapesa@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

POINTS OF CONTACT OUTSIDE EUROPE

Daniel J. McLoon
Los Angeles
+1.213.243.2580
djmcloon@jonesday.com

Richard J. Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Jeff Rabkin
San Francisco
+1.415.875.5850
jrabkin@jonesday.com


JONES DAY
One Firm Worldwide℠