Ai sigg.ri CLIENTI LORO SEDI

Le novità in materia di privacy applicabili dal 25 maggio 2018

Gentile cliente, con la presente desideriamo informarLa che **in data 25.05.2018 entrano in vigore le nuove disposizioni in materia di protezione dei dati contenuta nel regolamento UE n. 679/2016** (con legge n. 163/2017 è stata conferita delega al Governo all'emanazione di un Decreto di adeguamento del quadro normativo nazionale al contenuto del regolamento UE).

La disciplina introdotta prevede la **responsabilizzazione del titolare e del responsabile del trattamento dei dati**, nonché **l'introduzione della nuova figura del responsabile della protezione dei dati** (RPD/DPO).

Al fine di ridurre nella maggior misura possibile l'utilizzo improprio dei dati, viene introdotto un sistema che prevede la **responsabilizzazione e la rendicontazione delle misure intraprese per essere coerenti con il nuovo impianto legislativo.**

Viene prevista una più specifica disciplina relativa all'informativa con particolare riferimento alla sua **predisposizione** (concisa e scritta con un linguaggio chiaro e semplice, di facile comprensione). Con riferimento all'ambito di applicazione, si segnala che **la nuova disciplina si estende al trattamento dei dati personali effettuato**:

1) **nell'ambito delle attività di uno stabilimento** da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento avvenga nell'Unione europea o meno;

2) da un titolare del trattamento o da un responsabile del trattamento **non stabilito** nell'Unione, **per dati di interessati che si trovano nell'Unione,** quando le attività di trattamento riguardano:

   a) **l'offerta di beni o la prestazione di servizi** ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;

   b) il **monitoraggio del loro comportamento** nella misura in cui tale comportamento ha luogo all'interno dell'Unione;

3) daun titolare del trattamento non stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Premessa

Con il **regolamento UE n. 679/2016**, **applicabile a partire dal 25.05.2018**, viene introdotta una **nuova disciplina in materia di privacy**. Le novità, in particolare, sono le seguenti:

- **responsabilizzazione:** il titolare/responsabile del trattamento dovrà dimostrare, non solo formalmente, di aver adottato interventi e misure efficaci a contrastare l'utilizzo fraudolento dei dati. Si passa quindi da un sistema di **"regolarità formale"** ad un sistema di **"regolarità fattuale"**;
- **nuove figure professionali:** viene inoltre introdotta la figura del Responsabile della protezione dei dati;
- **informativa e consenso al trattamento**: al fine di poter garantire un effettivo consenso al trattamento dei dati personali, vengono previste nuove disposizioni relativamente alla modalità espositiva dell'informativa al trattamento. Le informative dovranno, infatti, essere accessibili, concise e scritte con un linguaggio chiaro e semplice. Viene richiesto il consenso esplicito sui dati sensibili;
- **figure del trattamento:** la catena di custodia del trattamento dei dati personali deve essere tracciata attraverso la definizione di un organigramma e dei ruoli all'interno della struttura del titolare;
- **regime sanzionatorio:** viene prevista la definizione di un regime sanzionatorio in misura percentuale sul volume di fatturato, in misura diversa a seconda della gravità della violazione.

Al fine di favorire la maggiore comprensione di quanto segue, forniamo le principali definizioni fornite dal Regolamento UE circa i soggetti interessati e l'oggetto del provvedimento:

DEFINIZIONI	
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.
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.

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.
Resp. 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**.

Di seguito illustriamo le **principali novità applicabili a decorrere dal prossimo 25.05.2018**.

Ambito di applicazione

Il reg. UE 679/2016 trova applicazione con riferimento ai seguenti **trattamenti:**

1) **automatizzato**, in maniera parziale o totale, **di dati personali**;

2) **non automatizzato** di dati personali contenuti in un archivio o destinati ad essere ivi inclusi.

Sono esclusi, in particolare, i **trattamenti di dati personali effettuati** da una persona fisica **per l'esercizio di attività a carattere esclusivamente personale o domestico.**

Il reg. UE 679/2016 (art. 3) si estende al trattamento dei dati personali effettuato:

- nell'ambito delle **attività di uno stabilimento** da parte di **un titolare del trattamento o di un responsabile del trattamento nell'Unione**, indipendentemente dal fatto che il trattamento avvenga nell'Unione europea o meno;
- da un titolare del trattamento o da **un responsabile del trattamento non stabilito nell'Unione**, per dati di interessati che si trovano nell'Unione, quando le attività di trattamento riguardano:
- **l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione**, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
- il **monitoraggio del loro comportamento** nella misura in cui tale comportamento ha luogo all'interno dell'Unione;
- da un **titolare del trattamento non stabilito nell'Unione**, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

La responsabilizzazione del titolare del trattamento

Al fine di evitare l'uso improprio di dati e informazioni, il legislatore ha introdotto il principio di accountability, ovvero di **responsabilizzazione del titolare del trattamento**, introducendo inoltre un obbligo di rendicontazione delle misure intraprese per essere coerenti con il nuovo impianto normativo.

Attraverso l'obbligo di rendicontazione delle misure adottare, quindi, si passa da un sistema di regolarità formale ad un **sistema di regolarità sostanziale**, in quanto il titolare avrà la necessità di dimostrare l'adozione nel corso del tempo di misure realmente efficaci.

Si segnala, inoltre, che alla luce delle nuove disposizioni, **coloro che entrano in contatto con i dati personali devono essere autorizzati al loro trattamento.**

Novità in materia di informativa e consenso al trattamento

Secondo quanto previsto dalle previgenti disposizioni, **l'informativa** non doveva possedere particolari requisiti, ma solamente il contenuto specifico elencato nell'articolo 13 del D.Lgs. n. 196/2003. Il Regolamento UE, oltre ad averne ridefinito il contenuto, ha **fissato anche le regole necessarie a rendere effettiva la comprensione ed efficacia dell'informativa.**

Viene ora imposto, infatti, che il titolare del trattamento deve predisporre **informative accessibili, concise e scritte con un linguaggio chiaro e semplice, di facile comprensione**. Il fine di tale ulteriore specificazione dell'informativa contenuta nella nuova disciplina consiste nel **garantire la possibilità di decidere con cognizione di causa se concedere o meno il proprio consenso**

L'informativa deve inoltre specificare la **base giuridica del trattamento, il trasferimento dei dati in stati terzi e, in caso positivo, tramite quali canali, il periodo di conservazione dei dati, i diritti dell'interessato e le finalità del trattamento.**

Con riferimento al consenso, **per il trattamento dei dati sensibili è previsto il consenso esplicito** (libero, specifico, informato e inequivocabile). Non viene richiesta necessariamente la documentazione del consenso per iscritto, né è richiesta la forma scritta ma solamente l'adozione di una modalità idonea a garantire l'inequivocabilità dello stesso.

Le figure del trattamento

Al fine di garantire una struttura di protezione efficiente il regolamento prevede un **tracciamento della catena di custodia ed utilizzo dell'informazione attraverso la definizione di ruoli e compiti all'interno della struttura del titolare** (con specifica indicazione dei soggetti interni ed esterni all'attività del titolare del trattamento).

RESPONSABILE DEL TRATTAMENTO DATI

Può essere designato dal titolare del trattamento tramite contratto, ove sono indicati gli specifici obblighi distinti da quelli di pertinenza del titolare. Il responsabile deve:

1. **tenere il registro dei trattamenti svolti** (solo nel caso di soggetti con almeno 250 dipendenti o qualora i trattamenti siano a rischio) contenente un quadro aggiornato dei trattamenti in essere all'interno dell'azienda;
2. **adottare misure tecniche e organizzative necessarie per garantire la sicurezza dei trattamenti;**
3. designare, nel caso in cui sia necessario, il **responsabile per la protezione dei dati.**

RESPONSABILE DELLA PROTEZIONE DEI DATI

Rappresenta una nuova figura non prevista dalla previgente disciplina, incaricata di **funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del regolamento UE n. 679/2016.**

Tale figura è obbligatoria per i **soggetti la cui attività consiste in trattamenti che necessitano di un monitoraggio costante / permanente degli interessati su larga scala** (es. banche, istituti di credito, imprese assicurative, società finanziarie, CAF e patronati, società del settore sanitario), o **trattamenti su larga scala di categorie di dati personali particolari** (come i dati relativi a condanne penali e reati).

Osserva

Secondo chiarimenti forniti dal Garante, **tale figura non è prevista per i liberi professionisti operanti in forma individuale, agenti, rappresentanti e mediatori, imprese individuali, familiari, PMI con riferimento ai trattamenti dei dati connessi alla gestione corrente dei rapporti con fornitori e dipendenti.**

I diritti degli interessati

Oltre a confermare i diritti previsti dalla precedente disciplina, viene definito a favore degli interessati:

- il **diritto alla portabilità**, al fine di consentire all'interessato di disporre e controllare il proprio dato utilizzandolo per scopi diversi ed evitando pratiche scorrette tese a creare una fidelizzazione forzata dell'utente di un servizio;
- il **diritto all'oblio**, volto a tutelare l'interessato quando la circolazione di informazioni che lo riguardano, essendo venuto meno l'interesse pubblico a conoscerle, diventa lesiva della sua onorabilità.

Sanzioni

La nuova disciplina prevede, **in caso di violazione del regolamento UE, l'applicazione di sanzioni differenziate a seconda della gravità dell'evento**. In particolare, si segnalano le seguenti sanzioni:

- **sanzione fino al 2%** del fatturato calcolato sull'esercizio precedente per le sanzioni relative agli obblighi in capo al titolare o responsabile del trattamento, all'organismo di certificazione e di controllo;
- **sanzione fino al 4%** del fatturato calcolato sull'esercizio precedente nel caso in cui le violazioni siano riferite ai principi base del Trattamento tra cui le condizioni di consenso, il trasferimento dei dati ad uno stato terzo o un'organizzazione internazionale, qualsiasi obbligo adottato dalla legislazione nazionale, il mancato rispetto di un ordine, di una limitazione provvisoria o definitiva al trattamento dei dati, la negazione di un accesso alle autorità di controllo.

Lo Studio rimane a disposizione per ogni ulteriore chiarimento e approfondimento di Vostro interesse.

Cordiali saluti