TAR DIVEL &ASSO CIATI
gestione integrata d'impresa
Via XX Settembre, 57 - Conegliano 31015 TV - T. 0438.35355 / 0438.22109 F. 0438.22810 - info@studiotardivel.it - www.studiotardivel.it

Con il regolamento 27.04.2016 n. 679 GDP) il Legislatore comunitario ha "uniformato" la disciplina sulla Privacy applicabile negli Stati membri **a decorrere dal 25.05.2018**. Entrerà quindi in vigore la nuova disciplina sulla Privacy. Il nuovo decreto prevede l'abrogazione del D.Lgs n. 196/2003.

Ecco alcune specifiche:

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.
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.
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.
Violazione dei dati personali	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o

	comunque trattati
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

L'introduzione del citato Regolamento UE n. 679/2016 sul trattamento dei dati ha, come scopo principale, uniformare il trattamento dei dati in tutta l'Unione Europea.
Questo regolamento impone ai Titolari del trattamento, anche residenti al di fuori dell'UE, il rispetto del Regolamento e quindi garantirà un maggior grado di protezione ai cittadini quandanche dovessero utilizzare beni e servizi offerti da soggetti non comunitari.

La nuova impostazione, in riferimento all'utilizzo di dati ed informazioni, si basa sostanzialmente su un approccio che vuole arrivare alla **massima riduzione del rischio per la libertà e la dignità del cittadino**.
Per ottenere questo scopo, il Legislatore ha introdotto il **principio di accountability**, inteso quale "**responsabilizzazione**" e di un concomitante obbligo di rendicontazione delle misure intraprese per essere coerenti con il nuovo impianto normativo. corso del tempo, l'adozione di misure realmente efficaci.

Il Regolamento UE n. 679/2016, definisce e fissa anche le regole necessarie a rendere effettiva la comprensione ed efficacia dell'Informativa.
I requisiti di validità del consenso rimangono sostanzialmente invariati anche nella formulazione dell'art. 4. par. 11, Regolamento UE n. 679/2016, ma viene aggiunto il **requisito di validità**. Il consenso sarà **valido** solo se la volontà dell'interessato è **espressa in modo inequivocabile** per ogni singolo trattamento.

Per consentire un'efficace catena di protezione del dato personale durante le attività di trattamento è necessario procedere ad un tracciamento della catena di custodia e utilizzo dell'informazione attraverso la

Via XX Settembre, 57 - Conegliano 31015 TV - T. 0438.35355 / 0438.22109 F. 0438.22810 - info@studiotardivel.it - www.studiotardivel.it

definizione di ruoli e compiti all'interno della struttura del Titolare. Il D.Lgs. n. 196/2003 aveva già introdotto l'obbligo di individuare **l'organigramma** dei soggetti coinvolti nelle attività di trattamento del dato.

Una novità importante dal punto di vista organizzativo viene introdotta dalla possibilità di **nomina di sub responsabili** che consentirà una migliore mappatura dei flussi di dati esterni all'organizzazione del Titolare.
Sempre nell'ottica della tracciabilità dei flussi di dati (GDO).

È designato dal Titolare del trattamento, **tramite contratto** nel quale dovranno essere specificate tassativamente almeno le materie di cui all'art. 28, par. 3, Regolamento UE n. 679/2016. Allo stesso sono imputabili **specifici obblighi** distinti da quelli di pertinenza del Titolare.

Il responsabile della protezione dei dati assolve **funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento UE n. 679/2016**.
È una **figura obbligatoria** per i soggetti le cui attività consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala** o un trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.
Il ruolo di responsabile della protezione dei dati può essere ricoperto **da un dipendente del Titolare o del Responsabile** (non in conflitto di interessi) che conosce la realtà operativa in cui avvengono i trattamenti;
L'incarico può essere affidato **anche a soggetti esterni**, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento UE n. 679/2016 assegna a tale figura.

La migrazione verso i nuovi concetti di tutela e riduzione del rischio può essere laboriosa ed onerosa sia dal punto di vista organizzativo che economico.
Dando per scontata la necessaria conoscenza della normativa, la prima attività da compiere è una **ricognizione ed identificazione** dei trattamenti di dati personali, che potrà, poi sfociare nella predisposizione del registro dei trattamenti svolti.
L'operazione più importante sarà l'individuazione dei **rischi che incombono sui dati**, che potrà eventualmente sfociare nella predisposizione di una valutazione di impatto dei trattamenti (DPIA) e la conseguente adozione di contromisure adeguate.
Inoltre non sarà quindi più sufficiente intendere la protezione del dato come sistema statico, ma sarà necessario procedere a **valutazioni periodiche** dell'esistente e ad analisi preventive in caso di introduzione di nuove tipologie di trattamento.

Via XX Settembre, 57 - Conegliano 31015 TV - T. 0438.35355 / 0438.22109 F. 0438.22810 - info@studiotardivel.it - www.studiotardivel.it

Ciò implica non solo una costante attenzione e verifiche periodiche dell'efficacia delle misure individuate, ma anche una costante valutazione del contesto in cui avviene il trattamento perché non è necessariamente detto che ciò che andava bene prima debba andare bene anche dopo.
Sarà necessario dotarsi di **procedure interne organizzate e standardizzate** che consentano il monitoraggio di ogni fase di trattamento nell'ottica della riduzione del rischio e l'organizzazione di momenti formativi per i soggetti autorizzati.

REGIME SANZIONATORIO

L'art. 83, par. 3 e 4, Regolamento UE n. 679/2016 prevede 2 distinte categorie di sanzioni amministrative pecuniarie a seconda della natura della violazione. In particolare, sono previste le seguenti sanzioni:

- **fino al 2% del fatturato** dell'esercizio precedente per le sanzioni relative agli obblighi:
  - del Titolare / Responsabile del trattamento;
  - dell'Organismo di certificazione;
  - dell'Organismo di controllo;
- **fino al 4% del fatturato** dell'esercizio precedente per le violazioni relative:
  - ai principi base del Trattamento, comprese le condizioni di consenso;
  - ai diritti degli Interessati;
  - ai trasferimenti dei dati personali a un destinatario di uno Stato terzo o un'organizzazione
  - internazionale;
  - a qualsiasi obbligo ai sensi della legislazione nazionale adottata a norma del Capo IX;
  - all'inosservanza di un ordine, di una limitazione provvisoria / definitiva di trattamento o di un ordine di sospensione dei flussi di dati all'Autorità di controllo o il negato accesso.

TAR DIVEL &ASSOCIATI
gestione integrata d'impresa
Via XX Settembre, 57 - Conegliano 31015 TV - T. 0438.35355 / 0438.22109 F. 0438.22810 - info@studiotardivel.it - www.studiotardivel.it

Principio / Requisito / Organi	Art.	Adempimento
Trattamento dei dati personali	5	*OBBLIGATORIO* Liceità, correttezza, trasparenza del rattamento dati sono princìpi fondamentali che incombono su chiunque
Condizioni di liceità del trattamento	6	*OBBLIGATORIO* Le condizioni previste dalla norma garantiscono l'effettività dei principi generali
Consenso	7	*OBBLIGATORIO salvo ECCEZIONI* (una è rappresentata dal trattamento dati necessario alla stipula e gestione del rapporto di lavoro)
Informativa	12 - 14	*OBBLIGATORIO* Chiunque tratti dati personali deve informare gli interessati dei suoi diritti secondo le indicazioni del Regolamento
Registro attività di trattamento	30	*NON OBBLIGATORIO* per le realtà che occupano meno di 250 addetti *L'obbligo prescinde dal requisito dimensionale* nel caso in cui i dati oggetto del trattamento possano presentare un rischio per i diritti e le libertà degli interessati, il trattamento non sia occasionale o includano dati sensibili, genetici, biometrici, giudiziari
Predisposizione, verifica, aggiornamento sistema di adeguatezza misure adottate	24 – 26	*OBBLIGATORIO* È la conseguenza logico-attuativa del principio di responsabilizzazione o *accountability*
Valutazione d'impatto sulla protezione dei dati	35 - 36	*CONNESSO* alla specificità di determinate tipologie di dati
Responsabile interno	28	*FACOLTATIVO*
DPO	37	*FACOLTATIVO*
Data – Breach	35	*OBBLIGATORIO* L'adempimento nel rispetto dei termini previsti dal regolamento è un obbligo che incombe su tutti i titolari di trattamento dati