CSA SERVICE SRL
Via Brusade, 81 - 30027 San Donà di Piave (Ve)
Tel. 0421 592411 - Fax 0421 592417 - E-mail segreteria.sandona@articom.it
Via Einaudi, 62 - 30174 Venezia-Mestre
Tel. 041 961624/954958 – Fax 041 5055188 E-mail segreteria.mestre@articom.it

San Donà di Piave, 16.05.2018

PRIVACY

Nuova disciplina in materia di protezione dei dati personali
Regolamento UE n. 679/2016

Gentile Cliente,
Il 25.5.2018 troverà applicazione la nuova disciplina in materia di Protezione dei dati Privacy contenuta nello specifico Regolamento UE n. 679/2016, che sostituirà buona parte del "Codice della privacy".
Premesso che ogni trattamento di dati deve rispettare i fondamenti di liceità, correttezza e trasparenza, anche nella nuova disciplina assume particolare importanza l'Informativa all'interessato ed il consenso dello stesso.
La nuova disciplina, improntata sulla "responsabilizzazione" del Titolare/Responsabile del trattamento dei dati, introduce, la nuova figura del Responsabile della protezione dei dati (RPD / DPO).

LE PRINCIPALI NOVITA'

Le modifiche più significative introdotte dal Regolamento UE n. 679/2016 riguardano:

- l'introduzione di un sistema armonizzato di Privacy in ambito comunitario, allo scopo di uniformare la normativa dei singoli stati;
- il diritto all'oblio dell'interessato (cioè la cancellazione definitiva dei dati trattati e conservati dal Titolare del trattamento) e alla portabilità dei dati su richiesta degli interessati;
- l'introduzione di un "approccio basato sulla riduzione del rischio" da parte del Titolare/Responsabile del trattamento il quale deve effettuare costantemente (prima, durante e al termine del trattamento) delle valutazioni sulla correttezza dell'operato;
- l'introduzione del Registro dei trattamenti per particolari fattispecie;
- l'introduzione della figura del Responsabile della protezione dei dati (cd. "*DPO*" - *Data protection officer*) per gli enti pubblici/privati che trattino dati di natura particolare o effettuino un trattamento dei dati su larga scala e/o in maniera sistematica;
- inasprimento del regime sanzionatorio.

ENTRATA IN VIGORE E ABROGAZIONI

Il Regolamento UE n. 679/2016

- entrerà in vigore a far data dal **25/05/2018** e sarà direttamente applicabile in ogni stato membro;
- non abroga le discipline nazionali, ma ne sostituisce automaticamente le disposizioni in contrasto.

NOTA: Il Codice della Privacy, contenuto nel D.lgs. 196/2003, resterà in vigore per quanto non difforme dal Regolamento fintantoché il Governo non approverà una nuova disciplina. Attualmente è stato formulato in bozza uno schema di Decreto, approvato in via preliminare dal Consiglio dei ministri in data 21/03/2018. Con l'approvazione in via definitiva, il Codice Privacy sarà abrogato e spetterà al nuovo decreto il compito di armonizzare l'ordinamento interno alla nuova disciplina europea.

QUALI DATI SONO INTERESSATI DAL REGOLAMENTO (AMBITO APPLICATIVO)

Il Regolamento UE si applica al trattamento dei dati effettuato dal Titolare o Responsabile del trattamento relativamente ai dati delle **persone fisiche** come:

Dati personali comuni: nome , indirizzo, nazionalità e numeri di previdenza sociale;

Dati personali particolari:

- Informazioni personali: origine raziale ed etnica, opinioni politiche, credo, appartenenza sindacale e orientamento sessuale;
- informazioni Web: posizione, indirizzo IP, cookie e tag RFID;
- informazioni sulla salute e la documentazione genetica;

Dati giudiziari: relativi a condanne penali.

NB: Sono **esclusi** dal Regolamento UE

- Dati delle persone giuridiche (es: società), compresi il nome, la forma della persona giuridica e i suoi dati di contatto;
- le informazioni anonime e i dati anonimizzati.

APPROCCIO BASATO SUL RISCHIO

Il nuovo Regolamento UE pone l'accento sulla "responsabilizzazione" dei Titolari e dei Responsabili del trattamento dei dati. Mentre nel Codice della privacy la protezione dei dati si limitava al rispetto formale e all'adozione di misure minime, il nuovo approccio impone al Titolare o al Responsabile del trattamento di valutare e successivamente dimostrare di aver adottato misure realmente efficaci.

NOTA: Titolari e Responsabili del trattamento sono liberi di decidere le modalità ed i limiti del trattamento dei dati (il Regolamento non prevede delle specifiche modalità di elaborazione o conservazione dei dati), ma per poter **risultare conformi alla** normativa, saranno tenuti a dimostrare nel corso del tempo di aver valutato i rischi relativi al trattamento dei dati e di aver posto in essere misure organizzative e tecniche adeguate alla riduzione di tale rischio.

CONSENSO ED INFORMATIVA

QUANDO E' POSSIBILE TRATTARE I DATI

Il Regolamento conferma che ogni trattamento dei dati deve trovare fondamento in un idonea base giuridica, rispettando i fondamenti di liceità del trattamento indicati all'art. 6 del Regolamento.
Il trattamento è lecito solo nel caso in cui ricorra una delle seguenti condizioni:

- CONSENSO: l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- CONTRATTUALE: il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- LEGALE: il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- INTERESSE VITALE: il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- PUBBLICO INTERESSE: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- LEGITTIMO INTERESSE: il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

CONSENSO

Il consenso per essere valido deve essere espresso in modo libero, specifico, informato e in modo tale che la volontà dell'interessato risulti inequivocabile per ogni singolo trattamento dei dati.

Il Regolamento non prevede una specifica forma per il Consenso, ma il Titolare è tenuto a dare prova che l'interessato ha prestato il proprio consenso, specialmente per i dati particolari (es: ex dati sensibili) e per il trattamento automatizzato dei dati, per i quali il consenso deve essere espresso.

Per garantire la prova del Consenso è **consigliato raccogliere il consenso in forma scritta**.
L'interessato potrà in qualsiasi momento **revocare il proprio consenso**, ma la revoca non pregiudica la liceità del trattamento basata sul consenso in precedenza prestato.

INFORMATIVA

Il Regolamento UE prevede che l'Informativa all'interessato debba rispettare un contenuto minimo, previsto dagli artt. 13, par. 1 e 14, par. 1.

In particolare, l'Informativa deve obbligatoriamente indicare:

- L'identità e i dati di contatto del Titolare del trattamento e del suo Rappresentante;
- i dati di contatto del Responsabile della protezione dei dati - DPO, se nominato;
- le finalità e la base giuridica del trattamento;
- il periodo di conservazione dei dati personali, oppure i criteri utilizzati per determinare tale periodo;
- qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal Titolare del trattamento o da terzi;
- i destinatari o le eventuali categorie di destinatari dei dati personali, interni o esterni;
- se i dati sono trasferiti in paesi terzi al di fuori del territorio UE e con che modalità sono trasferiti;
- i diritti dell'interessato: diritto d'accesso e aggiornamento, diritto all'oblio, diritto alla portabilità dei dati, diritto ad una corretta informativa, diritto di limitazione all'elaborazione, diritto di opporsi.

FIGURE DEL TRATTAMENTO

TITOLARE E RESPONSABILE DEL TRATTAMENTO

In modo analogo a quanto già previsto nel Codice della privacy, il Regolamento definisce le caratteristiche soggettive e le responsabilità del Titolare e del Responsabile del trattamento.

Il Regolamento introduce le seguenti novità:

- **designazione del Responsabile del trattamento**: si tratta di un contratto che evidenzi che il Responsabile presenti garanzie sufficienti (quali la natura, durata e finalità del trattamento, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal Titolare e delle disposizioni del regolamento). Contitolarità del trattamento: prevede la possibilità di trattamento congiunto, imponendo ai contitolari di definire l'ambito delle rispettive responsabilità;
- **sub-responsabili del trattamento**: il Responsabile può nominare terzi per specifiche attività di trattamento per conto del Titolare del trattamento;
- **specifici obblighi per i Responsabili del trattamento**: viene introdotta, in determinati casi:
  - ➔ la tenuta del registro delle attività di trattamento;
  - ➔ la designazione di un Responsabile della protezione dei dati (DPO).

Atti formali: il Titolare dovrà predisporre un atto formale di nomina del Responsabile del trattamento; allo stesso modo quest'ultimo sarà tenuto ad un atto di nomina formale nel caso in cui nomini dei sub-responsabili del trattamento (per specifiche attività) o nomini il Responsabile della protezione dei dati (DPO).

RESPONSABILE PROTEZIONE DATI (DPO)

Il Regolamento UE prevede che il Titolare/Responsabile del trattamento possa nominare la figura del Responsabile della protezione dei dati "Data Protection Officer – DPO". Tale figura può essere sia interna all'azienda (es: dipendente non in conflitto d'interessi) e sia esterna (es: persona fisica, professionista o persona giuridica). Successivamente alla nomina, il Titolare/Responsabile del trattamento sarà tenuto a comunicare al Garante della Privacy i dati di contatto del DPO.

La nomina del DPO generalmente è volontaria, diventa obbligatoria sono nei seguenti casi:

- se le attività principali del Titolare/Responsabile del trattamento consistono in trattamenti "su larga scala":
    - che "per loro natura, ambito di applicazione e/o finalità "richiedono un monitoraggio "regolare e sistematico" di dati anche non sensibili (es: sondaggi di opinione, analisi epidemiologiche);
    - di "dati sensibili" o di dati relativi a condanne penali e a reati
- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;

La nomina del DPO **non è obbligatoria** nei casi diversi dalla "elaborazione su larga scala", ad esempio:

- liberi professionisti, imprese individuali o familiari;
- agenti, rappresentanti e mediatori operanti su larga scala;
- PMI per trattamenti di dati connessi alla gestione dei rapporti con fornitori/dipendenti.

NOTA: Il Garante della privacy italiano ha pubblicato sul proprio sito internet le risposte alle FAQ, fornendo ulteriori chiarimenti sui soggetti obbligati alla nomina del Responsabile della protezione dei dati - DPO.
Sono tenuti alla nomina ad esempio: istituti di credito, imprese assicurative, società finanziarie, società di revisione controllo, CAF e patronati, società operanti nel settore della cura della salute, della prevenzione / diagnostica / diagnostico sanitaria.

La figura del DPO avrà funzioni di controllo e supporto, dovrà essere indipendente e autonomo nello svolgimento dei propri compiti, sarà esperto di normativa e prassi in materia di privacy e ricoprirà i seguenti compiti:

- Informare e consigliare il Titolare/Responsabile del trattamento circa gli obblighi derivanti dal Regolamento e vigilare sul loro effettivo adempimento;
- fornire, su richiesta, un parere sulle valutazioni d'impatto sulla protezione dei dati raccolti;
- cooperare con l'autorità di controllo per le questioni riguardanti il trattamento (e per questo il suo nominato è oggetto di comunicazione al Garante).

REGISTRO DEI TRATTAMENTI

Il Regolamento UE all'art. 30 prevede che i Titolari e i Responsabili del trattamento dei dati possano volontariamente tenere un apposito registro dei trattamenti svolti.
La tenuta del Registro è **obbligatoria** in presenza di almeno una delle seguenti condizioni:

- impiego di più di 250 dipendenti;
- trattamenti che presentino un rischio per i diritti fondamentali e le libertà dell'interessato;
- trattamenti che riguardano categorie particolare di dati (art. 9);
- dati giudiziari (art. 10).

Il Registro dei trattamenti tenuto dal Titolare del trattamento dovrà obbligatoriamente avere un contenuto minimo secondo quanto individuato all'art. 30 del Regolamento UE:

- il nome e i dati di contatto del Titolare del trattamento;
- il nome e i dati di contatto del Responsabile della protezione dei dati – DPO;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali trattati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi UE, con separata indicazione dei destinatari di paesi terzi EXTRA-UE e delle modalità di trasmissione;
- i termini per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate per la protezione dei dati.

Allo stesso modo, il Registro dei trattamenti tenuto dal Responsabile del trattamento dovrà obbligatoriamente contenere:

- il nome e i dati di contatto del Responsabile e di ogni Titolare del trattamento per conto del quale agisce;
- le categorie di trattamenti effettuati per conto del Titolare del trattamento;
- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate per la protezione dei dati.

REGIME SANZIONATORIO

La misura delle sanzioni pecuniarie varia in relazione alla natura, gravità e durata della violazione, al suo carattere doloso/colposo, nonché alle misure concretamente adottate dal Titolare o dal Responsabile del trattamento per attenuare il danno arrecato.

L'art. 83 del Regolamento UE 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.

NOTA: Merita sottolineare che con la futura approvazione del Decreto attuativo al Regolamento UE, di cui attualmente è disponibile solamente una bozza, accanto alle sanzioni amministrative si affiancheranno quelle penali, la cui misura sarà determinata da ogni stato membro.

DEFINIZIONI

L'art. 4, Regolamento UE fornisce tra l'altro le seguenti 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.
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.