STUDIO VENTURATO
Commercialisti e Consulenti per le imprese e gli enti locali

TUTTI I CLIENTI
- LORO SEDI -

Circolare n. 005/18
Legnago, 17/05/2018

PRIVACY

REGOLAMENTO EUROPEO 2016/679 - GDPR

(GENERAL DATA PROTECTION REGULATION)

NUOVE REGOLE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

SINTESI

A partire dal 25 maggio 2018 sarà operativo il Regolamento (UE) 2016/679 (più comunemente definito GDPR - General Data Protection Regulation) che, **in materia di PRIVACY**, prevede nuovi obblighi, una nuova figura professionale e un nuovo e pesantissimo trattamento sanzionatorio.
Come detto il Regolamento, che è entrato in vigore il 24.5.2016 ma sarà operativo dal prossimo 25.5.2018, si applica a tutte le aziende aventi almeno uno stabilimento nell'UE che trattano in modo integrale o parziale, automatizzato o non, i dati personali, indipendentemente dal fatto che il trattamento sia effettuato all'interno dell'Unione.
Il GDPR disciplina la protezione dei dati delle persone fisiche con riferimento sia al trattamento sia alla libera circolazione di tali dati. Persegue due principali finalità: sensibilizzare e rendere consapevoli gli "interessati" (le persone fisiche) nel momento in cui rendono disponibili i propri dati personali; responsabilizzare sia le imprese private sia le autorità pubbliche che utilizzano i dati personali nell'ambito delle loro attività.
Il regolamento prevede:

- **maggiori diritti dell'interessato in termini di privacy personale**. I titolari devono dichiarare agli interessati, in modo trasparente, le finalità del trattamento e le misure di protezione dei dati;
- **maggiori doveri in capo al**le organizzazioni. Il regolamento conferma che ogni trattamento di dati personali deve trovare fondamento in un'idonea base giuridica. I titolari del trattamento dei dati sono tenuti a seguire un percorso di adeguamento alle norme, nel rispetto dei fondamenti di liceità del trattamento, che coincidono, in linea di massima, con quelli già previsti dal Codice privacy d.lgs. 196/2003 (consenso, adempimento obblighi contrattuali, obblighi di legge cui è soggetto il titolare, ecc.). Il titolare deve sempre poter dimostrare che è stato fatto tutto il possibile per evitare e prevenire la diffusione non autorizzata di informazioni sensibili, fino anche all'autodenuncia se dovessero verificarsi violazioni o furti di archivi contenenti dati sensibili;
- **obblighi del titolare:**
    - fornire informazioni chiare agli interessati della raccolta dei dati;
    - evidenziare gli scopi dell'elaborazione e i casi di utilizzo;
    - definire i criteri di conservazione e di eliminazione dei dati;
    - proteggere i dati personali con misure di sicurezza appropriate;
    - avvalersi di un responsabile della protezione dei dati (per le organizzazioni di grandi dimensioni);
    - segnalare alle autorità eventuali violazioni;
    - conservare la documentazione dettagliata;
    - formare personale e dipendenti.

Novità del regolamento:

- la protezione dei dati personali e l'uso per il quale si raccolgono le informazioni devono essere dichiarate ed organizzate in modo chiaro; non sarà possibile raccogliere o gestire dati senza specificarne la finalità, nel rispetto della norma;
- diritto all'oblio degli interessati: non possono essere detenute le informazioni una volta venuto meno lo scopo;
- principio di responsabilità (accountability): occorre dimostrare di aver fatto il possibile per proteggerli in base ai mezzi disponibili;
- sanzioni fino a 20 milioni di euro o fino al 4% del fatturato, comminate dall'autorità garante della privacy, e controlli da parte di Guardia di Finanza e tutte le forze di polizia.

Le modifiche introdotte in materia di privacy, per le quali si fornisce una breve sintesi con la presente circolare, presentano elementi di una certa complessità che possono rendere necessario, soprattutto in determinate situazioni, l'intervento di un esperto specializzato in materia.

Ambito di applicazione

Le disposizioni contenute nel regolamento UE 679/2016 si applicano a tutte le imprese e le pubbliche amministrazioni e riguardano la protezione delle persone fisiche. In particolare:

a. sono relative al trattamento dei dati personali;
b. alla libera circolazione di tali dati;
c. trovano applicazione con riferimento sia al trattamento automatizzato sia a quello non automatizzato di dati personali.

Soggetti responsabili

Oltre al titolare del trattamento dei dati e il responsabile del trattamento dati è introdotta la nuova figura del Responsabile per la protezione dei dati (RDP).
Nello specifico:

- il **titolare del trattamento** è il soggetto che singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali, mette in atto misure tecniche e organizzative per garantire che il trattamento sia conforme al Regolamento, tiene conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche e aggiorna e riesamina le misure ed è in grado di dimostrare la conformità al Regolamento;
- il **responsabile del trattamento** è il soggetto che tratta i dati personali per conto del titolare del trattamento e che deve avere garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate (incarico disciplinato da un contratto o da un altro atto giuridico, stipulato in forma scritta, anche in formato elettronico);
- il **responsabile per la protezione dei dati (RDP)** può essere sia un dipendente della società titolare del trattamento o, in alternativa, un professionista esterno competente in tema di protezione dati. La nomina di tale figura è obbligatoria nei seguenti casi:
  a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
  b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;
  c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

I casi concreti in cui si rende necessaria la nomina dell'RDP non sono di facile individuazione, tuttavia, si può ritenere che tra le aziende private rientrino le seguenti: istituzioni finanziarie e istituti di credito, società di recupero crediti, istituzioni e compagnie assicurative, aziende sanitarie

private/cliniche, poliambulatori, laboratori analisi cliniche e diagnostiche e altri istituti sanitari, società di servizi e consulenza, centri elaborazione dati e Internet provider, società di trasporti, agenzie di viaggio, strutture alberghiere e ricettive in genere, società commerciali e industriali allorquando trattino una mole di dati personali dei propri dipendenti, clienti, fornitori, consulenti esterni, tale da far ritenere soddisfatto uno dei fattori che connota il trattamento su larga scala, studi professionali associati, società di revisione, società tra professionisti.
Tra i compiti svolti dall'RDP si evidenziano i seguenti:

- informare e fornire consulenza al titolare e al responsabile del trattamento nonché ai dipendenti che eseguono i trattamenti;
- sorvegliare l'osservanza del Regolamento;
- fornire pareri in merito alla "Valutazione d'impatto sulla protezione dei dati";
- cooperare con l'Autorità di controllo e fungere da punto di contatto con essa.

Adempimenti

In capo al titolare del trattamento e al responsabile del trattamento sono stati:

- dettagliati e/o modificati alcuni adempimenti già previsti, ad esempio in materia di modalità di trattamento dei dati, di acquisizione del consenso e di rilascio dell'informativa;
- introdotti nuovi compiti, fra i quali tenere un registro delle attività di trattamento ed effettuare una valutazione di impatto sulla protezione dei dati.

Tra gli adempimenti da effettuare, parte rilevante è il trattamento dei dati che deve avvenire sulla base di determinati principi stabiliti dal regolamento quali la liceità (art. 6 del Regolamento), la correttezza e la trasparenza nei confronti dell'interessato, la limitazione delle finalità, la minimizzazione dei dati che devono essere adeguati, pertinenti e limitati a quanto necessario, l'integrità e la riservatezza.

Misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.
Tuttavia, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Notifica delle violazioni di dati personali

A partire dal 25 maggio 2018, tutti i titolari, e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi, dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle menzionate nell'art. 32-bis dell'attuale Codice Privacy. I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del regolamento.

Suggerimenti
Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, dell'attuale Codice Privacy. Si raccomanda, pertanto, ai titolari del trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

NEW **- Responsabile della protezione dei dati**
Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: *Data Protection Officer*) riflette l'approccio responsabilizzante che è proprio del regolamento (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35. La sua designazione è obbligatoria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: si vedano artt. 38 e 39).

NEW **- Registro dei trattamenti** - Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti, ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.
Suggerimenti
La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche, ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Fatto una breve disamina generale del Regolamento 679/2016, cerchiamo di capire più nel dettaglio alcuni punti specifici, dicendo cosa cambia e cosa rimane invariato e, ove possibile, dando dei suggerimenti (condivisi dallo stesso Garante della Pivacy).

Consenso
E' qualsiasi manifestazione di volontà che i propri dati personali siano oggetto di trattamento.
Cosa cambia:

a. Per i dati "sensibili" (si veda art. 9 Regolamento) il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione);
b. Non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare inequivocabilmente il consenso e il suo essere "esplicito" (per i dati sensibili). Inoltre, il titolare (art. 7.1) deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento (per questo si consiglia di avere sempre la prova scritta);

c. Il consenso dei minori è valido a partire dai 16 anni (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci;

Cosa non cambia:

a. Deve sempre essere, in tutti i casi, libero, specifico, informato ed inequivocabile e non è ammesso il consenso tacito o presunto (es. no a caselle precompilate su un modulo);
b. Deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile";

Suggerimenti

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica. In particolare, occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. E' bene prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2).

Informativa

Deve essere concisa, trasparente, intelligibile per l'interessato; occorre utilizzare un linguaggio chiaro e semplice.

L'informativa è data per iscritto e preferibilmente in formato elettronico. Il regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa.

Casa cambia:

a. Contenuti dell'informativa
   I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto all'attuale Codice Privacy. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati-Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.
   Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.
   Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.
b. Tempi dell'informativa
   Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).
c. Modalità dell'informativa
   Il regolamento specifica molto più in dettaglio rispetto all'attuale Codice Privacy le caratteristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice e, per i minori, occorre prevedere informative idonee.
   L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente.

Sono inoltre parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato.

Cosa non cambia:

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato prima di effettuare la raccolta dei dati (se raccolti direttamente presso l'interessato, art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

Suggerimenti.

E' opportuno che i titolari di trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento.

Diritti degli interessati e loro modalità di esercizio

Chi è interessato al trattamento dei dati ha dei diritti specificamente tutelati. Sono il diritto di accesso, di rettifica, di oblio, di limitazione al trattamento, di portabilità e di opposizione.

Casa cambia:

a. Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego;
b. Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive - art. 12.5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, dell'attuale Codice Privacy, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato, di regola, deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3);
c. sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici.

Suggerimenti.

E' opportuno che i titolari del trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati che, a differenza di quanto attualmente previsto, dovrà avere per impostazione predefinita forma scritta (anche elettronica).

Diritto di accesso

Il soggetto interessato può consultare (anche in remoto) e/o ottenere gratuitamente una copia dell'informativa sul trattamento di dati personali che viene effettuato.

Cosa cambia:

a. Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento;
b. Fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri

utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

NEW **- Diritto di cancellazione (diritto all'oblio)**

Rappresenta il diritto alla cancellazione celere dei dati personali dell'interessato.

Cosa cambia:

a. Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione";
b. Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), dell'attuale Codice Privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.

Diritto di limitazione del trattamento

a. Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), dell'attuale Codice Privacy: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare);
b. Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Suggerimenti.

Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

NEW **- Diritto alla portabilità dei dati**

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Cosa cambia:

a. Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare.
b. il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Suggerimenti

Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un formato interoperabile.

NEW **- Titolare, responsabile, incaricato del trattamento**

Cosa cambia:

a. il regolamento disciplina la contitolarità del trattamento (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;
b. il regolamento fissa più dettagliatamente (rispetto all'attuale Codice Privacy) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" quali, in particolare, la natura, la durata e la finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;
c. il regolamento consente la nomina di sub-responsabili del trattamento da parte di un responsabile per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile";
d. il regolamento prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un RPD-DPO, nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento, diversamente da quanto prevedeva l'art. 5, comma 2, dell'attuale Codice Privacy.

Cosa non cambia:

a. Il regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). Pur non prevedendo espressamente la figura dell'incaricato del trattamento (ex art. 30 Codice), il regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

NEW **- Approccio basato sul rischio e misure di *accountability* (responsabilizzazione) di titolari e responsabili**

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (*accountability* nell'accezione inglese) di titolari e responsabili, ovvero, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Cosa cambia:

a. Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by default and by design*" (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di

procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

b. Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative, anche di sicurezza, che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento, avendo adottato le misure idonee a mitigare sufficientemente il rischio, ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

c. L'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia, con eventuale successiva consultazione dell'Autorità, tranne alcune specifiche situazioni di trattamento (vedi art. 36, paragrafo 5 del regolamento). Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

Videosorveglianza

L'installazione di adeguati impianti di video-sorveglianza deve rispettare i principi indicati dal Garante della Privacy e dalla normativa vigente.

Le attuali norme del Governo hanno riformato la disciplina del controllo a distanza dei lavoratori e stabilito che l'installazione degli apparecchi è ammessa solo:

- previo accordo con le rappresentanze sindacali aziendali;
- previa autorizzazione della Direzione Territoriale del Lavoro (D.T.L.), nelle aziende con minori dimensioni, ove mancano le rappresentanze sindacali.

L'accordo con le Rappresentanze sindacali o l'autorizzazione della D.T.L. devono in ogni caso essere preventivi rispetto alla installazione delle apparecchiature.

Si ricorda che la violazione delle norme è punita con sanzioni pecuniarie e costituisce un illecito di natura penale.

Sanzioni

Come già anticipato, con il Regolamento è stato introdotto un nuovo "sistema sanzionatorio" che prevede un aumento delle sanzioni amministrative pecuniarie fino ad un massimo di 20 milioni di Euro o, per le imprese, fino al 4% del fatturato totale annuo dell'esercizio precedente, se superiore.

CONCLUSIONI

Dal prossimo 25.05.2018, imprese e professionisti dovranno porre in essere una serie di adempimenti, differenziati a seconda della tipologia di attività esercitata e della dimensione della realtà aziendale, al fine di adeguarsi al nuovo regolamento europeo sulla privacy.
Il Garante della Privacy ha già fatto sapere, tenuto conto delle novità rispetto al precedente Codice Privacy e allo sforzo anche economico ed organizzativo che il nuovo impianto normativo può comportare, che non saranno comminate sanzioni in riferimento al primo periodo di operatività della norma. Ciò non toglie, che le imprese, i professionisti e gli altri soggetti economici interessati, devono prepararsi ed organizzarsi per rispettare le nuove normative.
In sintesi, quindi, gli step che l'impresa, il professionista o gli altri soggetti economici interessati, possono essere tenuti a seguire consistono:

a. nella revisione dell'organizzazione interna dell'impresa conformandola al protocollo privacy;
b. nella contrattualizzazione dei rapporti tra Titolare e Responsabile del trattamento dati, specificando le rispettive responsabilità;
c. nella revisione della modulistica con i clienti/utenti che si realizza con la riformulazione delle informative sulla privacy e la raccolta del nuovo consenso al trattamento dati;
d. nella programmazione e l'attuazione di sistemi di sicurezza nella protezione dei dati;
e. nella predisposizione della documentazione dimostrativa della propria conformità alle regole previste nel Regolamento;
f. nella formazione obbligatoria del personale;
g. nell'eventuale adesione a codici di correttezza e a sistemi di certificazione.

Le modifiche introdotte in materia di privacy, per le quali si fornisce una breve sintesi con la presente circolare, presentano elementi di una certa complessità che possono rendere necessario, soprattutto in determinate situazioni, l'intervento di un esperto specializzato in materia.

SCADENZIARIO MAGGIO – GIUGNO 2018

GIORNO	SCADENZA
25 maggio 2018	**APPLICAZIONE REGOLAMENTO EUROPEO 2016/679 - GDPR**
	Presentazione modelli INTRASTAT per operatori con obbligo mensile
31 maggio 2018	**Comunicazione dei dati delle liquidazioni periodiche IVA**
	Comunicazione dei dati delle fatture emesse e ricevute relativi al primo trimestre 2018 per coloro che non optano per la trasmissione dei dati semestrale
18 giugno 2018 (il 16 è un sabato)	Versamento dell'IVA dovuta per i contribuenti mensili
	Versamento delle ritenute sui redditi di lav. Autonomi, dipendenti e su provvigioni
	Versamento contributi INPS per collaboratori coordinati e continuativi e per i lavoratori dipendenti
	Versamento della prima rata dell'Imposta municipale propria (IMU) e TASI dovuta per l'anno in corso
	Versamento seconda ed ultima rata imposta sostitutiva assegnazione e cessione agevolata beni immobili o beni mobili iscritti a pubblici registri
25 giugno 2018	Presentazione modelli INTRASTAT per operatori con obbligo mensile
2 luglio 2018 (il 30 è un sabato)	Versamento imposta sostitutiva sulle rivalutazioni di terreni e partecipazioni
	Presentazione della dichiarazione IMU per l'anno 2017
	Versamento di imposte e contributi risultanti dalle dichiarazioni Redditi ed Irap 2018 (senza maggiorazione) per contribuenti persone fisiche, società di persone e società di capitali
	Versamento del diritto annuale dovuto alle Camere di Commercio di competenza

Le circolari precedenti possono essere consultate sul Ns. sito al seguente link:
http://www.studioventurato.it/circolari.htm

CORDIALI SALUTI **STUDIO VENTURATO**