STS NETWORK
CONSULENZA FISCALE, SOCIETARIA E MANAGERIALE

Circolare del 23 maggio 2018

OGGETTO:PRIVACY - COSA CAMBIA CON IL NUOVO REGOLAMENTO EUROPEO

Il presente documento si propone di fornire **uno strumento di ricognizione** per la verifica degli adempimenti in **materia di privacy a carico delle imprese e professionisti**, entro il **25 maggio 2018**, data in cui avrà definitiva attuazione il Regolamento UE (27.04.2016 n. 679) concernente la "*tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*", volto a disciplinare i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico, e destinato ad abrogare la Direttiva 95/46/CE2 ("**Direttiva 95/46**") che ha portato in Italia, all'adozione del vigente D.lgs. 30 giugno 2003 n. 196 ("**Codice Privacy**").

Vengono previste **maggiori tutele per cittadini e imprese**, in ragione dei grandi cambiamenti portati dalle tecnologie digitali adoperate per il **trattamento dei dati**.

A fronte delle continue evoluzioni degli strumenti utilizzati, diviene di fondamentale importanza, per le imprese che intendono migliorare o implementare il proprio assetto organizzativo, procedere per tempo ad effettuare **un'adeguata analisi dei rischi e una valutazione d'impatto sulla privacy**. Per fare ciò, occorrerà partire dall'attuale disciplina (**D.Lgs. n. 196 del 30.06.2003, c.d. "Codice della Privacy**") e cercare poi di prevedere **l'impatto della nuova normativa sulla realtà aziendale**, per comprendere se saranno sufficienti solo piccoli aggiustamenti o se invece occorrerà un mutamento organizzativo radicale.

In quest'ottica, dunque, quali sono i principali adempimenti cui le imprese sono già tenute e quali quelli che dovranno essere adottati in conformità al nuovo Regolamento UE?

FIGURE SOGGETTIVE

Per poter effettuare le verifiche necessarie in **materia di privacy**, occorre in primo luogo dotarsi di **un'organizzazione efficiente**, avvalendosi di professionisti specializzati e personale adeguatamente formato e preparato.

Accanto alle tradizionali figure del **Titolare** (*coincidente con il soggetto cui competono le decisioni in ordine ad un determinato trattamento*), del **Responsabile** (*ovvero il soggetto preposto dal Titolare ad un trattamento di dati*) e dell'**Incaricato** (*qualsiasi persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile*), il Regolamento UE ha introdotto all'*art. 35* la figura del **Responsabile della protezione dei dati personali** (***Data Protection Officer – DPO***), **obbligatorio per le aziende pubbliche e per tutte quelle realtà in cui i trattamenti presentano rischi specifici**.

Il **Responsabile della protezione dei dati personali** dovrà possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali; adempiere alle sue funzioni in piena autonomia e senza ricevere istruzioni.

Nello svolgimento dei suoi compiti, dovrà principalmente:

a) informare e consigliare il **titolare** o il **responsabile del trattamento**, nonché i **dipendenti**, in merito agli obblighi derivanti dal **Regolamento europeo**;

b) verificare l'attuazione e l'applicazione della **normativa**, compresi la sensibilizzazione e la formazione del **personale** e gli **audit relativi**;

c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla **protezione dei dati** e sorvegliare i relativi adempimenti;

d) fungere da punto di contatto per gli interessati in merito a **qualunque problematica** connessa al **trattamento dei loro dati** o all'esercizio dei loro diritti;

e) fungere da punto di contatto per il **Garante per la protezione dei dati personali** oppure, eventualmente, consultare il Garante di propria iniziativa.

Quanto alle figure tradizionali, si segnala fin d'ora che il nuovo impianto normativo e l'introduzione di nuovi principi (*quali quello di accountability e di privacy by design e by default, di cui si dirà nel prosieguo*) richiederà **un maggior grado di preparazione** e competenze specifiche (*si pensi, a titolo meramente esemplificativo, in ambito di conservazione digitale dei documenti*) a tutti i soggetti coinvolti, con la conseguenza che dovrà essere attuata un'adeguata e specifica formazione del personale.

INFORMATIVA

L'*art. 13 del* ***Codice della Privacy*** prevede l'obbligo, prima di effettuare qualsiasi **trattamento di dati personali**, di fornire all'interessato o alla persona presso la quale sono raccolti i dati una **informativa, orale o scritta**, circa:

- le finalità e le modalità del **trattamento**;
- la natura obbligatoria o facoltativa del loro **conferimento**;
- le conseguenze di un **eventuale rifiuto a rispondere**;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati, anche nella loro qualità di **responsabili o incaricati**;
- i diritti previsti dal Codice all'*art. 7* (*diritto di accesso e altri diritti*) e gli estremi identificativi del **Titolare** nonché del **Responsabile del trattamento**, se designato.

Analogo obbligo è previsto dal **Regolamento UE**, il quale, in applicazione del principio di trasparenza, stabilisce all'*art. 12* l'adozione di misure appropriate a fornire all'interessato tutte le informazioni necessarie e le comunicazioni relative al trattamento ***in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori***. Le informazioni dovranno essere fornite per iscritto o con altri mezzi, se del caso anche mediante strumenti elettronici. Se richiesto dall'interessato, le informazioni potranno essere fornite oralmente, purché l'identità dell'interessato sia comprovata con altri mezzi.

L'informativa continuerà a rivestire rilevanza fondamentale, prevedendo un contenuto più dettagliato e maggiori informazioni da fornire, come elencate agli *artt. 14 e 14 bis*.

La redazione della modulistica relativa all'assolvimento di quest'obbligo dovrà, quindi, essere in parte rielaborata e approfondita.

CONSENSO

In linea generale, l'*art. 23 del* ***Codice della Privacy*** indica le modalità con le quali deve essere acquisito il consenso e precisamente esso:

i) deve essere **espresso**;

ii) può riguardare **l'intero trattamento** ovvero una o più operazioni dello stesso;

iii) è validamente prestato solo **se è espresso liberamente e specificamente** in riferimento ad un trattamento chiaramente individuato, **se è documentato per iscritto** e se sono state rese all'interessato le informazioni di cui all'*art. 13*;

iv) è manifestato **in forma scritta** quando il trattamento riguarda dati sensibili.

Il successivo *art. 24* specifica, inoltre, i casi in cui il **trattamento dei dati può essere effettuato senza consenso**(*ad esempio, quando si tratta di dati "pubblici", informazioni relative ad attività economiche, adempimento di un obbligo di legge, ecc*.).

Particolari garanzie sono, poi, dettate per i **dati sensibili** (ovvero per "*i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*"), che possono essere oggetto di trattamento solo con il **consenso scritto dell'interessato** e **previa autorizzazione del Garante**, salvo specifiche deroghe indicate all'*art. 26*.

Quanto al **Regolamento UE**, di grande rilevanza è la nuova definizione di consenso: "*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*".

La richiesta di una manifestazione di volontà ***inequivocabile*** potrebbe avere un grosso impatto nella prassi, posto che, ad esempio, un semplice flag potrebbe non essere ritenuto più sufficiente per la manifestazione di consenso.

L'*art. 7* del **Regolamento** prevede, inoltre, che, qualora il trattamento sia basato sul consenso, il **responsabile del trattamento** debba essere in grado di dimostrare la volontà espressa dall'interessato. Se il consenso dell'interessato è manifestato nel contesto di una **dichiarazione scritta** che riguarda anche altre materie, la richiesta deve essere presentata in modo chiaramente distinguibile dalle altre materie, **in forma comprensibile e facilmente accessibile**, **utilizzando un linguaggio semplice e chiaro**. Il consenso reso in violazione al **Regolamento** non è vincolante, nemmeno in parte.

Anche per quanto concerne **il consenso**, la modulistica dovrà essere parzialmente rivista per essere resa più aderente a quanto prescritto dal legislatore europeo.

Quanto alle ***categorie particolari di dati personali*** (*pressoché coincidenti con la definizione sopra indicata di dati sensibili, salvo la novità riguardante l'orientamento sessuale*), l'*art. 9* sancisce il **divieto di trattamento**, che non si applica però quando ricorrono determinati casi espressamente elencati.

MISURE DI SICUREZZA

Come noto, lo **sviluppo tecnologico** e la maggiore attenzione rivolta alla **tutela della riservatezza** hanno determinato il legislatore a prestare maggiore attenzione all'aspetto della **sicurezza dei dati**, individuando gli strumenti volti a prevenire perdite e/o distruzione.

Il **Codice della Privacy** tratta il tema delle **misure di sicurezza** al Titolo V, operando una **distinzione tra misure idonee e misure minime**.

In particolare, l'*art. 31* del Codice specifica che i **dati personali** oggetto di trattamento debbono essere **custoditi e controllati** "*anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento in modo da ridurre al minimo, mediante* ***l'adozione di idonee e preventive misure di sicurezza****, i rischi di distruzione o perdita, anche se accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*".

Il Capo *II del Codice* (*artt. 33-36 ss.*) e l'*Allegato B* (*Disciplinare Tecnico in materia di misure minime di sicurezza*) fissano, poi, una soglia minima degli strumenti da adottare, distinguendo il caso in cui il trattamento avvenga mediante **strumenti elettronici** (*art. 34*) da quello in cui non vi sia l'uso di tali strumenti (art. 35).

La differenza tra **misure idonee e misure minime** può essere impercettibile da un punto di vista meramente tecnico; tuttavia, la loro distinzione è fondamentale sotto l'aspetto giuridico, dal momento che notevolmente diverse sono le **conseguenze derivanti dalla violazione dell'una o dell'altra prescrizione**.

Difatti, **l'inosservanza delle misure minime** configura reato come previsto dall'*art. 169* del Codice, che prevede l'arresto fino a due anni; **la mancata adozione delle misure idonee** rientra, invece, nel campo di applicazione dell'*art. 15*, integrando un'ipotesi di responsabilità civile ai sensi dell'*art. 2050 c.c.* (*Responsabilità per l'esercizio di attività pericolose*). Per evitare di incorrere nella predetta responsabilità, occorre, dunque, dare

la **prova liberatoria di avere adottato tutte le misure idonee**, così come esistenti alla luce del progresso tecnologico, ad evitare la causazione del danno.

Il **Regolamento UE** innalza ulteriormente il livello della sicurezza, introducendo **l'obbligo di segnalare all'Autorità competente** ed agli stessi utenti eventuali **violazioni dei dati personali (c.d. data breaches**, quali, ad esempio, accessi abusivi, utilizzo non consentito), entro un termine temporale prestabilito decorrente dal momento della scoperta della violazione.

Non si parla più di misure minime e idonee, ma di misure adeguate. In particolare l'*art. 30* stabilisce: "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il* ***titolare del trattamento*** *e il* ***responsabile del trattamento*** *mettono in atto* ***misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio****, che comprendono, tra le altre, se del caso*:

a) la ***pseudonimizzazione e la cifratura*** *dei* ***dati personali****;*

b) la capacità di assicurare su base permanente la ***riservatezza****,* ***l'integrità****, la* ***disponibilità*** *e la* ***resilienza*** *dei sistemi e dei servizi di trattamento;*

c) la capacità di ripristinare tempestivamente la ***disponibilità e l'accesso dei dati personali*** *in caso di incidente fisico o tecnico;*

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle ***misure tecniche e organizzative*** *al fine di garantire la sicurezza del trattamento*".

Le misure minime non verranno quindi ritenute sufficienti.

Per valutare l'adeguato livello di sicurezza occorrerà tenere conto dei **rischi di distruzione**, **perdita**, **modifica**, **divulgazione non autorizzata** o accesso accidentale o illegale a **dati personali** trasmessi, conservati o comunque trattati.

L'applicazione di un codice di condotta (*disciplinato all'art. 40*) o a un meccanismo di certificazione (*art. 42*) potranno essere utilizzati come elemento per dimostrare la conformità ai requisiti delle **misure di sicurezza**.

Per trattamenti che prevedono **rischi specifici**, è introdotta all'*art. 35* la necessità di effettuare, prima di procedere al trattamento, una **valutazione dell'impatto-privacy** all'interno dell'azienda.

Anche il **Regolamento UE** prevede la possibilità di reclamo e di ricorso giurisdizionale, prescrivendo altresì sanzioni amministrative pecuniarie per la mancata adozione di **misure di sicurezza inadeguate**; inoltre, sempre in analogia all'attuale impianto normativo, è possibile chiedere il **risarcimento dei danni al titolare o al responsabile del trattamento**, salvo che questi dimostrino (*fornendo una vera e propria probatio diabolica*) che l'evento dannoso non gli è in alcun modo imputabile.

ALTRE IMPORTANTI NOVITA'

Vi sono, inoltre, **ulteriori novità normative** che vanno tenute presenti nel percorso di adeguamento dell'assetto organizzativo aziendale in materia di privacy.

In particolare, il **Regolamento UE**:

- riconosce espressamente il **diritto all'oblio**, ovvero la possibilità per l'interessato di decidere che siano cancellati e non sottoposti ulteriormente a **trattamento i propri dati personali** non più necessari per le finalità per le quali sono stati raccolti, nel caso di revoca del consenso o quando si sia opposto al **trattamento dei dati personali** che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al **Regolamento**;
- stabilisce il **diritto alla portabilità dei dati**, in virtù del quale l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i **dati personali** che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo è necessario per l'esecuzione di un contratto;
- sancisce il principio di **accountability**, per cui il titolare dovrà dimostrare l'adozione di **politiche privacy** e misure adeguate in conformità al **Regolamento**;
- introduce il principio della **privacy by design** e quello della **privacy by default**. Dal primo discende l'attuazione di adeguate misure tecniche e organizzative sia all'atto della **progettazione che dell'esecuzione del trattamento**. Il secondo ricalca il principio di necessità di cui all'attuale disciplina, stabilendo che i dati vengano trattati solamente per le finalità previste e per il periodo strettamente necessario a tali fini.

SANZIONI

Da ultimo, preme segnalare che il **Regolamento UE** ha innalzato sensibilmente la misura delle sanzioni, che potranno arrivare fino ad un massimo di **€ 20.000.000,00 o fino al 4% del fatturato annuo**.

Considerazioni finali

Non v'è dubbio che il Nuovo Regolamento, così come è formulato, ponga obblighi di *compliance* particolarmente stringenti nei confronti degli operatori che trattano dati personali. D'altro canto però non può non rilevarsi come l'adozione di uno strumento normativo, quale, il Regolamento, comportante l'applicazione di un'unica disciplina in tutta l'UE, agevoli non poco l'esercizio del *business* di un'impresa che non si troverà più a dover fronteggiare quell'incertezza giuridica derivante da normative diverse per ogni Stato e i costi e la burocrazia a esse connesse. Anche la particolare attenzione che viene data alle piccole e medie imprese, esonerandole da alcuni obblighi, deve essere guardata con nota di merito in quanto faciliterà notevolmente il loro ingresso e affermazione sul mercato.

*****

Lo Studio STS NETWORK è a disposizione per qualsiasi chiarimento ed approfondimento, anche in relazione a fattispecie specifiche o offre i seguenti servizi:

a) l'analisi del trattamento dati e l'analisi dei potenziali rischi;

b) l'individuazione dei ruoli e dei responsabili, e la stesura delle relative lettere di nomina;

c) la stesura, la revisione e l'aggiornamento della documentazione sulla privacy (organigramma Privacy, Data Breach, Registro trattamenti ecc...), ivi comprese le varie informative per gli interessati al trattamento e le procedure operative;

d) l'identificazione di tutti quei casi in cui è necessario informare gli interessati del trattamento dati (es. iscrizione alla newsletter sul sito web);

e) l'eventuale stesura del Data Protection Impact Assessment (DPIA), ossia di quel documento contenente l'insieme di processi funzionali che si devono mettere in atto al fine di realizzare, attraverso lo studio delle modalità di trattamento dei dati, una seria e fattiva analisi

dei rischi. La valutazione dell'impatto del rischio consente di individuare i pericoli correlati al trattamento dati e le misure idonee a neutralizzarli o, almeno, gestirli;

f) le eventuali notifiche e comunicazioni al Garante della privacy;

g) l'eventuale redazione di un codice di condotta, da rendere effettivo in azienda;

h) la formazione presso la Vs. sede del personale.

Lo Studio rimane a disposizione per ogni ulteriore chiarimento.

Cordiali saluti.

STS NETWORK

CONTATTI

PISA
Sts Network
Via Matteucci, 38
Phone: +39 050 970628
Fax: +39 050 3137650
Mobile: +39 349-3672698
Email: ffacchini@stsnetwork.it
avirgili@stsnetwork.it

PISTOIA
Sts Network
Via E. Fermi, 93
Phone: +39 0573 935531
Fax: +39 0573 536691
Mobile: +39 348-8878425
Email: fgiommoni@stsnetwork.it

LUCCA
Sts Network
Via Muston, 117
Phone: +39 0583 050260
Fax: +39 0583 050715
Mobile: +39 339-1179619
Email: mbusico@stsnetwork.it

FIRENZE
Sts Network
Via delle Mantellate, 8
Phone: +39 055 462831
Fax: +39 055 4628332
Mobile: +39 348 2416449
Email fsalvadori@stsnetwork.it