

LA NUOVA PRIVACY EUROPEA: LEGAL COMPLIANCE

tempistiche e attività per le aziende



Le novità

introdotte dal Regolamento Europeo n° 679 del 2016



Lo studio SILS offre un team di professionisti per assistervi nella revisione della documentazione relativa al trattamento dei dati personali, al fine di essere conformi al nuovo Regolamento.

Il 24 maggio 2016 è stato approvato il Regolamento Europeo n° 679/2016 relativo alla tutela delle persone fisiche con riferimento al trattamento dei dati personali e la libera circolazione dei dati. Questo Regolamento sarà direttamente applicabile in Italia e in tutti gli altri Stati Membri dell'Unione Europea a partire dal 25 maggio 2018, termine del periodo transitorio di due anni concesso per l'attuazione.

Le principali novità introdotte dal Regolamento sono:

1

l'applicazione del Regolamento anche alle imprese situate fuori dell'Unione Europea, che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione Europea (Art. 3);

2

l'esclusione di ogni forma di consenso tacito oppure ottenuto proponendo all'interessato una serie di opzioni già selezionate (Art. 7);

3

l'obbligo per i fornitori di servizi internet e i social media di chiedere il consenso ai genitori per trattare i dati personali dei minori di 16 anni (Art. 8);

4

la maggior chiarezza, completezza, trasparenza, brevità e accessibilità dell'informativa sul trattamento dei dati personali (Artt. da 13 a 21);

5

il diritto all'oblio, cioè la possibilità per gli interessati di ottenere la cancellazione dei propri dati personali, anche on-line, qualora ricorrano alcune condizioni (Art. 17);

6

il diritto alla portabilità dei dati personali per trasferirli da un titolare del trattamento all'altro (Art. 20);

7

i criteri di "privacy by default" e "privacy by design", con riferimento alla valutazione degli strumenti e dei rischi in cui l'impresa può incorrere nel trattamento dei dati personali per prevenire ipotesi di "data breach" (Art. 25);

8

l'obbligo per il titolare del trattamento dei dati, entro 72 ore dall'evento di violazione dei dati personali di inviarne comunicazione all'Autorità Nazionale per la Protezione dei Dati personali e al soggetto interessato (Artt. 33-34);

9

la figura professionale e il ruolo del Data Protection Officer, nuovo responsabile che l'impresa deve nominare per la corretta gestione dei dati personali (Artt. da 37 a 39);

10

l'autorizzazione per legge al trasferimento di dati personali fuori dall'Unione Europea solo in presenza di garanzie contrattuali o valutazioni di adeguatezza (il cd. Privacy Shield) oppure di consenso esplicito dei soggetti interessati purché previamente informati di tutti i rischi (Artt. da 44 a 50);

11

lo sportello unico, cioè la possibilità per le imprese stabilite o che offrono servizi in più Stati Membri dell'Unione Europea di rivolgersi all'Autorità per la Protezione dei Dati Personali del Paese dove si trova la propria sede principale (Art. 56);

12

le sanzioni che, a seconda delle violazioni, possono comportare multe sino a Euro 20.000.000 o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

Le imprese dovranno rivedere le attuali informative per il consenso al trattamento dei dati (sia per i dipendenti che per i clienti), nonché nominare un Data Protection Officer, al fine di essere conformi al nuovo Regolamento. Inoltre, il tema del trasferimento dei dati personali dall'I-

talia verso le organizzazioni presenti negli Stati Uniti aderenti allo "Scudo o Privacy Shield" pubblicato dal dipartimento del commercio degli Stati Uniti, è ancor più di attualità data la recente autorizzazione dell'Autorità Garante Privacy del 27 ottobre 2016.

Nuove regole

per le aziende ai fini della protezione dei dati personali



NORMATIVA • ENTRATA IN VIGORE • APPLICABILITÀ

Come sopra indicato, il 24 maggio 2016 è entrato in vigore il Regolamento Europeo n° 679 del 27 aprile 2016 relativo alla tutela delle persone fisiche con riferimento al trattamento dei dati personali e la libera circolazione dei dati.

Il Regolamento 679/2016 sarà applicabile in tutti gli Stati Membri dell'Unione Europea a partire dal 25 maggio 2018, al termine del periodo transitorio di due anni concesso per l'attuazione.

INFORMATIVA

Nell'informativa sarà necessario avere:

ICONE

- Una nuova forma grafica con icone per attrarre l'attenzione degli interessati sui punti fondamentali dell'informativa.

CHIAREZZA

- Una maggior chiarezza, completezza, trasparenza e brevità.

Nell'informativa sarà necessario indicare:

CONTATTI

- I dati di contatto:
 - (a) Titolare del trattamento dei dati;
 - (b) Rappresentante del Titolare del trattamento dei dati;
 - (c) Responsabile del trattamento dei dati.

TRATTAMENTO

- Le finalità di trattamento dei dati personali;
- La base giuridica del trattamento;
- I legittimi interessi perseguiti dal titolare del trattamento qualora il trattamento rientri nell'art. 6, comma 1, lettera f)

DESTINATARI E TRASFERIMENTI

- Gli eventuali destinatari o le categorie di destinatari dei dati personali;
- L'intenzione di trasferire i dati personali a un paese terzo (fuori dall'Unione Europea)

CONSERVAZIONE E CANCELLAZIONE

- Il periodo di conservazione dei dati personali o, se non possibile, i criteri utilizzati per la determinazione di tale periodo;
- Il diritto dell'interessato all'accesso ai propri dati, alla rettifica, alla cancellazione, alla limitazione del trattamento e all'opposizione al trattamento;

REVOCA E OBBLIGATORietà

- Il diritto alla revoca del consenso;
- L'obbligatorietà legale o contrattuale della comunicazione dei dati o la facoltà dell'interessato di fornire i dati;

PORTABILITÀ E RECLAMO

- Il diritto alla portabilità dei dati;
- Il diritto di proporre reclamo alle autorità;

PROFILAZIONE E MARKETING

- L'esistenza di un processo decisionale automatizzato compresa la profilazione, informazioni sulla logica usata, l'importanza e le conseguenze previste di tale trattamento;
- La descrizione dei singoli trattamenti dei dati personali che esulano dagli obblighi contrattuali. In particolare, dovrà essere predisposto un singolo articolo descrittivo per ogni singolo trattamento (fini contrattuali, marketing, sondaggi, offerte personalizzate)

MODULO DI CONSENSO

Le regole per l'elaborazione del modulo di consenso prevedono:

CONSENSO ESPlicito E SEPARATO

- L'esclusione di ogni forma di consenso tacito oppure ottenuto proponendo all'interessato una serie di opzioni già selezionate;
- L'obbligo di un consenso singolo e separato: dovrà essere predisposto un singolo articolo descrittivo per ogni singolo trattamento (fini contrattuali, marketing, sondaggi, offerte personalizzate) e il modulo di consenso dovrà contenere una checkbox, che preveda l'opt-in o l'opt-out del cliente finale.

CONSENSO GENITORI

- L'obbligo per i fornitori di servizi internet e i social media di chiedere il consenso ai genitori per trattare i dati personali dei minori di 16 anni.

COMPETENZA

L'applicazione del Regolamento 679/2016 anche alle imprese situate fuori dell'Unione Europea, che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione Europea.

DATA BREACH

L'obbligo per il titolare del trattamento dei dati, entro 72 ore dall'evento di violazione dei dati personali, di inviare comunicazione all'Autorità Nazionale per la Protezione dei Dati personali e al soggetto interessato.

SPORTElLO UNICO

Lo sportello unico, cioè la possibilità per le imprese stabilite o che offrono servizi in più Stati Membri dell'Unione Europea di rivolgersi all'Autorità per la Protezione dei Dati del paese dove si trova la propria sede principale.

DATA PROTECTION OFFICER

Il Data Protection Officer è la nuova figura professionale aziendale con il compito di assicurare una gestione corretta dei dati personali degli interessati.

NUOVE SANZIONI

Le nuove sanzioni previste a seconda delle violazioni possono comportare multe sino a Euro 20.000.000 o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.



I. Normativa e orientamenti del Garante per la Protezione dei Dati Personali

Il *Data Protection Officer* (di seguito “DPO”) -- figura introdotta dal Regolamento Europeo n° 679 del 27 aprile 2016 (il “Regolamento”), che diverrà applicabile in Italia e in tutti gli altri Stati Membri dell’Unione Europea a partire dal 25 maggio 2018 -- ha il ruolo di verificare e attuare l’applicazione del Regolamento da parte del Titolare del trattamento dei dati che, normalmente è l’impresa di cui il DPO è dipendente o incaricato. Il DPO è anche incaricato di mantenere i contatti fra il Titolare (l’impresa di cui sopra) e il competente ente pubblico italiano, ovvero l’Autorità Garante per la Protezione dei Dati Personali (“Garante”).

Il DPO deve possedere diversi requisiti: (i) competenze informatiche (anche relative al processo aziendale di raccolta e trattamento del dato personale) e giuridiche; (ii) qualità caratteriali volte all’equilibrio e alla diploma-

zia, indispensabili per corretto ed efficace dialogo con il Garante; (iii) indipendenza ed autonomia nello svolgimento delle proprie mansioni, in assenza di conflitti di interessi rispetto al Titolare.

L’art. 37 del Regolamento prevede la nomina obbligatoria del DPO in tre casi: (a) quando il trattamento dei dati è svolto da un organismo pubblico; (b) quando le attività principali del Titolare determinino trattamenti su larga scala basati sul monitoraggio regolare e sistematico degli interessati; (c) quando le attività principali del Titolare comportino trattamenti di categorie particolari di dati personali (ad esempio, l’origine razziale o etica, le opinioni politiche, le convinzioni religiose o filosofiche, appartenenza sindacale, i dati genetici, i dati relativi a condanne penali e a reati ai sensi degli artt. 9 e 10 del Regolamento), anche in questo caso su larga scala.

II. Chi è il DPO: possibili soluzioni pratiche

(1) Una prima ipotesi potrebbe identificare il DPO con un software che funga da DPO “digitale”, con compiti di gestione del data breach o delle altre violazioni portate alla sua attenzione tramite una specifica linea di comunicazione utilizzabile da dipendenti, clienti e fornitori (ad esempio una ethic hotline). Tale soluzione, pur avendo l’indubbio vantaggio di essere uno strumento totalmente dedicato ai controlli in materia di protezione dei dati personali e poco costoso (al netto dell’investimento iniziale), sembra in realtà identificare solo uno strumento a supporto di un DPO “analogico” (o, se si preferisce, in carne e ossa) dotato dell’equilibrio e diplomazia necessari a individuare le criticità nella valutazione d’impatto sulla protezione dei dati, sorvegliare l’osservanza del Regolamento, informare e sensibilizzare il titolare del trattamento e i suoi dipendenti e, infine, cooperare ai fini che precedono con il Garante.

(2) Una seconda ipotesi identifica il DPO in un dipendente già presente all’interno dell’impresa, cui il ruolo assorbirebbe la maggior parte del proprio orario lavorativo. In questo scenario, si porrebbe la questione del possesso da parte del candidato delle soft skill necessarie (come sopra identificate) nonché l’adeguata conoscenza della normativa e della prassi della gestione dei dati personali, con riferimento anche alle misure tecniche o organizzative per garantire la sicurezza dei dati. Tali profili critici sembrerebbero indirizzare la scelta delle imprese verso un candidato facente parte della funzione legale, favorito nelle attività che precedono dalla propria formazione lavorativa. Tuttavia, anche tale soluzione rischierebbe di sollevare delle criticità, sotto forma di inevitabile conflitto di interesse che si creerebbe in capo ad un medesimo dipendente, contemporaneamente tenuto a

Protection Officer

gli elementi di certezza sui quali possiamo contare

difendere l'impresa e a valutarne oggettivamente il comportamento e le prassi ai fini del trattamento dei dati personali.

(3) Una terza ipotesi affida il ruolo di DPO ad un legale esterno. La soluzione risolverebbe probabilmente la questione circa le abilità necessarie ai rapporti con il Garante (data l'abitudine dell'avvocato a trattare con le autorità pubbliche), garantendo la conoscenza della normativa di riferimento. Tuttavia, dal punto di vista informatico, sarebbe lecito domandarsi se un avvocato sia in condizione di confrontarsi con le delicate e complesse questioni tecniche connesse al trattamento – e le relative valutazioni di merito – o non debba a tali fini avvalersi di una società informatica con tali competenze. A questo riguardo, dovrebbe affrontarsi il tema della coerenza del rapporto tra il DPO e tale società informatica e l'adempimento delle prerogative di tale ufficio in piena autonomia e in assenza di conflitti d'interesse. (Il tutto volendo tacere le ulteriori criticità, e il relativo conflitto di interesse, legate all'ipotesi in cui il legale nominato DPO fosse anche consulente della società in altri ambiti professionali).

(4) La soluzione ideale, alla luce di quanto precede, sembrerebbe essere la creazione di un ufficio con funzione di DPO, con uno specifico budget di spesa e composto da soggetti in possesso delle

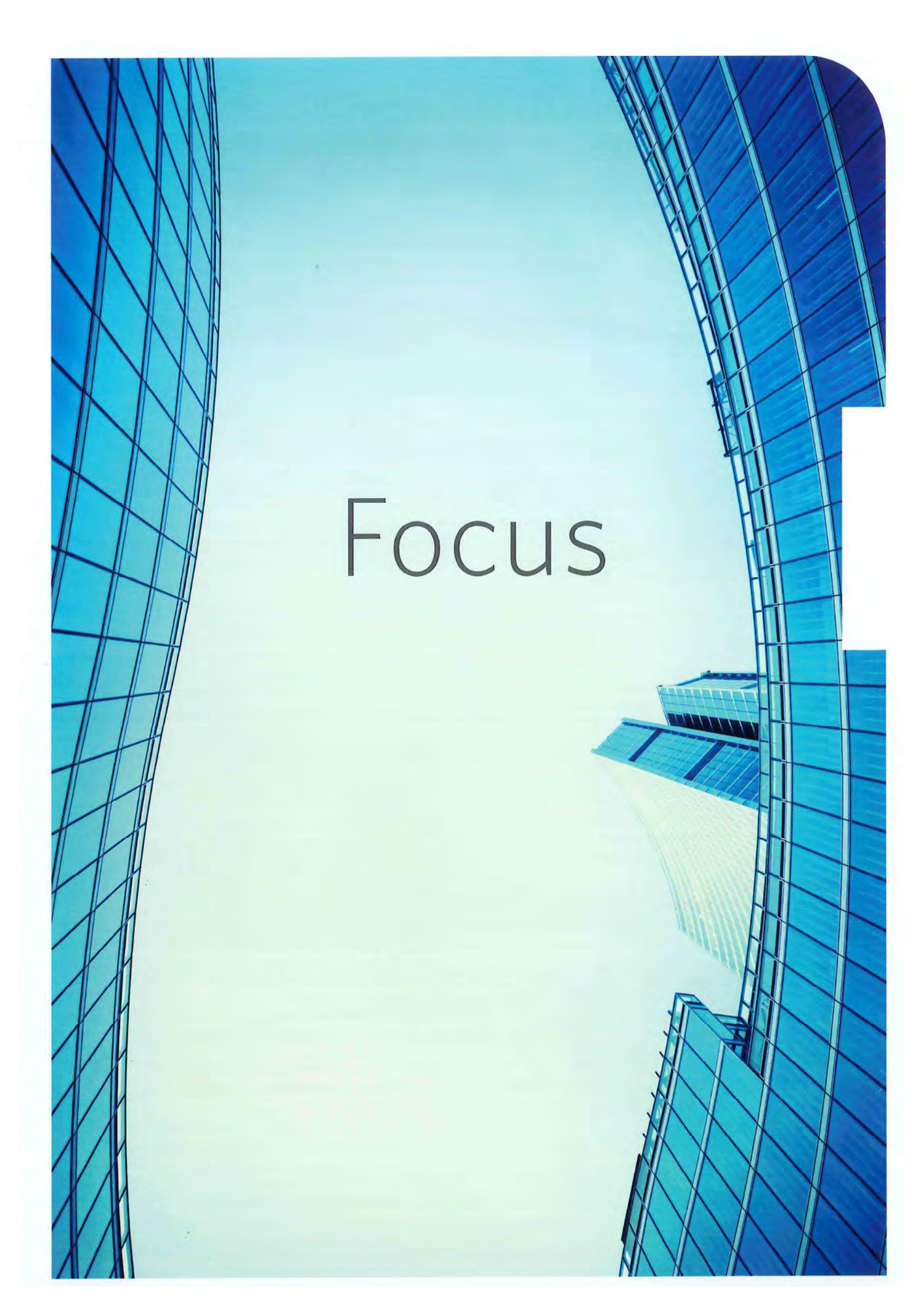
competenze legislative, tecniche, informatiche e caratteriali richieste dal Regolamento. Tali soggetti potrebbero essere, a seconda dei casi, legati all'impresa da un rapporto di lavoro subordinato o da un contratto di consulenza (con le specifiche avvertenze di cui sopra, quanto ad autonomia ed assenza di conflitti di interesse) e sarebbero interamente dedicati alla gestione dei dati personali e del relativo trattamento. In caso di criticità del trattamento dei dati personali e di necessità di un parere esterno, il DPO potrebbe essere assistito, a sua volta, da uno studio legale o di consulenza tecnica, dotato anch'esso dei predetti requisiti d'indipendenza.

Da ultimo rileviamo che con riferimento ai gruppi societari, la normativa non sembrerebbe essere ostativa alla nomina di un DPO centralizzato, invece che un DPO per ciascuna delle entità coinvolte, a condizione che sia soddisfatto il requisito implicito della competenza del candidato tale da ricomprendere tutte le possibili tematiche relative alle realtà societarie del gruppo di riferimento. La soluzione prospettata avrebbe dalla sua il vantaggio di una visione unitaria del trattamento dei dati personali, ma sembrerebbe praticabile solo qualora il trattamento delle entità appartenenti al gruppo non presenti delle specificità tali da impedire una gestione il più possibile omogenea dei dati personali.

III. Conclusioni

La nuova figura professionale del Data Protection Officer da nominare in azienda svolgerà una funzione essenziale per il rispetto della nuova normativa europea sulla privacy: è dunque indispensabile una corretta valutazione di tale ruolo sulla base delle considerazioni che

precedono, e la preparazione di quanto occorrente sia in senso giuridico e societario che di organigramma nell'impresa.

A low-angle, upward-looking photograph of several modern skyscrapers with blue-tinted glass facades. The buildings frame a central area of light blue sky. The word "Focus" is centered in the sky area.

Focus

SILS

Studio Italiano
Legale Societario

SILS, Studio Italiano Legale Societario, ha sede a Milano e **assiste in Italia primarie società e imprese sia nazionali che internazionali**, in aree di specializzazione che comprendono il **diritto della protezione dei dati personali**, il **diritto societario**, in particolare con riferimento ad operazioni di acquisizione, fusione e scorporo di azienda, **rapporti contrattuali** e **contenzioso commerciale**, in particolare nei settori dell'industria automobilistica, dell'energia, farmaceutico, dell'e-commerce, del tessile e dei prodotti di lusso.

L'ampia esperienza maturata dai professionisti di SILS – tutti abitualmente impegnati in incarichi che richiedono anche la perfetta conoscenza della lingua inglese – e la **consolidata reputazione** dello Studio nelle proprie materie specialistiche, si affiancano alla metodologia di risposta in tempi brevi e l'obiettivo costante di fornire **soluzioni pratiche e realmente idonee** alle esigenze della clientela.

Competenza

il nostro team specialistico





Avvocato Luigi Zumbo

Luigi Zumbo si occupa professionalmente da molti anni delle norme regolatrici della protezione dei dati personali e della relativa contrattualistica, avendo maturato ampia esperienza in relazione alle previsioni del cd. “Codice della Privacy” e contribuito anche in sede internazionale alla valutazione preventiva del nuovo Regolamento Europeo (679/2016) applicabile dal maggio 2018 in tutti gli Stati Membri dell’Unione Europea.

Oltre a tale specializzazione, Luigi Zumbo è attivo in generale nei principali settori del diritto d’impresa attinenti al commercio internazionale e alla distribuzione commerciale.

Luigi Zumbo, laureato presso l’Università Statale di Messina (1988) e specializzato presso l’Università Cattolica del Sacro Cuore di Milano (1992, Master in Bilancio d’Impresa), ha conseguito il Graduate Diploma presso la BPP Law School di Londra (2006).

Avvocato Federica Dendena

Federica Dendena si occupa principalmente del diritto della protezione dei dati personali, in particolare con riferimento al trattamento dei dati effettuato dalle imprese, ai conseguenti adempimenti richiesti dall’Autorità Garante ai sensi del cd. “Codice Privacy” e alla gestione delle eventuali sanzioni. Federica Dendena si occupa inoltre di contrattualistica e diritto societario.

Federica Dendena è relatrice in seminari web relativi a tematiche di diritto della protezione dei dati personali ed è co-autrice di diversi contributi in tema di trattamento dei dati personali regolarmente pubblicati in siti e blog specialistici.

Federica Dendena si è laureata presso l’Università Cattolica del Sacro Cuore di Milano (2010) e diplomata al Master di Diritto & Impresa della scuola del “Sole24ORE” (2012).



STUDIO ITALIANO LEGALE SOCIETARIO

Viale Regina Giovanna, 24
20129 Milano

Tel. 02 7628.1370
Fax 02 7628.0622

Federica.Dendena@Silsitalia.it
Luigi.Zumbo@Silsitalia.it

