Registro di adeguamento della ditta

LSD s.r.l.

al Regolamento Europeo 679/2016 General Data Protection Regulation per la Protezione dei Dati Personali.

In osservazione del decreto legislativo 196/2003

contenuti:

Introduzione aziendale

La ditta LSD s.r.l.

la società ha come attività tipica la
commercializzazione di sistemi di illuminotecnica ad alto contenuto tecnologico per l'utilizzo in interni ed esterni destinati ai servizi dell'utenza piu' varia, con attività di commercio all'ingrosso ed al minuto, operando collateralmente attività di l'assistenza e consulenza alla clientela
Tipica della gestione è l'assunzione di
mandati di agenzia o di distribuzione da ditte nazionali ed internazionali.

L'organizzazione aziendale avviene mediante l'attività di due soggetti, l'amministratore unico, che svolge attività non solo di amministrazione ma anche operativa, ed attraverso l'attività di almeno un dipendente.

Criteri di dati particolari (sensibili secondo codice privacy), quali genetici, biometrici, relativi alla salute, relativi a condanne penali e reati non sono specificatamente richiesti in quanto estranei alla natura della attività; in caso la LSD ne venisse a contatto il dato verrà immediatamente distrutto, e comunicazione dev'avvenuto recepiamo sarò dato al data controller per la gestione dell'informativa del caso.

Il trattamento dei dati personali avviene in ossequio al GDPR per finalità legittime, esplicite e definite, secondi i principi di minimizzazione, privacy by design, con progetto va pensato e realizzato pensando a come garantire la riservatezza e la protezione dei dati personali che vengono toccati nello specifico progetto, individuando a priori eventuali rischi Privacy, e privacy by default, trattando i dati personali solo nella misura necessaria per gli scopi previsti e per un tempo strettamente necessario

Si notifica che per la propria natura di piccola o media impresa con meno di 250 dipendenti la LSD s.r.l. non realizza trattamenti che possono presentare un rischio per i diritti e le libertà degli interessati, e che il trattamento risulta finalizzato alla gestione amministrativa e finanziaria della attività tipica e che non include dati di cui all'art. 9.1 o all'articolo 10. (dati particolari e dati personali giudiziari), esclusa dal registro trattamenti

Mappatura aziendale ed individuazione dei ruoli e delle responsabilità dei soggetti che effettuano il trattamento

Viene indicata la figura del *data controller* o *titolare del trattamento* nella persona del dott. *Alberto Crosio*. che nella propria attività decide mezzi e finalità di trattamento, che adotterà tutte le misure adeguato in osservanza del GDPR. Identifica il titolare del trattamento.

Viene indicata in solido nelle persone del suddetto *Alberto Crosio* e nella figura di *Enrica Guercio* la figura del *data processor*, quali operatori sui dati per conto del controller. Identificano i responsabili del trattamento

All'interno del complesso di sistemi di relazioni che interessano la LSD vengono rilevati i seguenti soggetti, persona che può essere coinvolta in un processo di trattamento privacy:

Agenti di commercio
Professionisti tecnici (architetti e progettisti)
Consulente fiscale
Consulente le lavoro
Consulenti giuridici

I suddetti soggetti non fanno parte dell'organigramma aziendale ma fanno parte della rete di relazioni professionali esterne; ogni intervento degli stessi sui dati personali sono oggetto di specifica lettera di incarico che attiene alla gestione dei dati, rimandando alla corretta gestione in ossequio al regolamento 679/2016 ed a quanto specificatamente normato dal DL 196/2003

Il titolare del trattamento e il responsabile del trattamento dichiarato di non volere designare sistematicamente un responsabile della protezione dei dati, denominato *Data Protection Manager* (DPO) in quanto, in ossequio a quanto normato nel GDPR le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, non richiedono il monitoraggio regolare, di fatto trattamento dei dati non sia cruciale rispetto all'attività di un'impresa.

Individuazione dei flussi di informazioni e recepimento dati

L'attività tipica della LSD s.r.l. (da qui in poi indicata come "ditta") risiede nel ricevimento di richieste di offerta commerciale e richieste a fornire (da parte di soggetti da qui in poi denominati "cliente")

Flussi in entrata:

I dati anagrafici vengono recepiti su attività del cliente stesso, che comunica con i mezzi più idonei, tipicamente messaggi email, altre volte a mezzo di telefonata diretta, la richiesta ad entrare in contatto con la ditta.

Dati vengono percepiti attraverso l'azione di soggetti collegati alla attività della ditta, quali agenti di commercio e promotori, oppure di tecnici per i quali esiste un rapporto diretto con il cliente.

Flussi in uscita:

I dati recepiti vengono utilizzati nella attività tipica di gestione ordini, pertanto vengono generalmente comunicati ai fornitori della ditta affinché si possa realizzare una gestione dell'ordine generalmente mirata a consegnare direttamente al cliente il prodotto richiesto

I dati vengono inoltre utilizzati per l'attività di contabilizzazione a fini di analisi interna ed a fini fiscali, secondo la normativa vigente

I dati rilevanti vengono utilizzati per comunicazioni ai clienti per aggiornamenti commerciali e tecnici oltreché informativi sulla attività della ditta e dei propri fornitori

Politiche di sicurezza e valutazione dei rischi

Vengono qui a seguito indicate le misure organizzative e tecniche messe in atto per adeguare e garantire che il trattamento dati viene effettuato conformemente al RGPD.

Flusso in entrata comunicazioni email:
Sistema email in assenza di server locale, con server remoto; modalità di accesso IMAP; la permanenza media delle email sugli archivi locali è limitata ad una storicità di un mese, dopo di che i messaggi vengono cancellati e vengono copiati del sistema remoto di backup.
Flusso in entrata comunicazioni audio registrate:
Le comunicazioni telefoniche in entrata ed uscita vengono registrate e tenute ad archivio locale criptato, e vengono cancellate dopo un mese. L'archiviazione remota viene attuata su sistema cloud criptato su fornitore esterno

Sistemi di elaborazione ed archiviazione:
L'elaborazione dei dati avviene su sistemi di informatica individuale (personal computer) su cui sono previsti sistemi a limitazione di accesso (password) e sistema di crittazione XTS-AES-128 con chiave a 256 bit su tutte le unità direttamente collegate

Sistemi alla connessione LAN e WAN
I sistemi di connessione alla rete locale avviene mediante cifratura WPA2. Il router è protetto da password specifica con cambio a nuova password con cadenza mensile. Le porte di accesso sono controllate da firewall ed è attivo un sistema log per la gestione degli accessi, controllato manualmente dal gestore di rete ad intervalli irregolari

Sistemi di backup:
Sistema di backup su hard disk fisici, due copie per unità di elaborazione a backup alternati, gestito da sistema automatico di backup basato su connessione fisica, effettuata ad intervalli settimanali. Le unità di backup sono anche esse criptate XTS-AES-128 con chiave a 256 bit, e tenute in ambito geografico remoto diverso da quello aziendale, affidato al gestore di rete

Archiviazione cloud:
Una copia mirror dei dati viene archiviata con sistema distribuito could, ricevuta da fornitori internazionali, uno di questi (Google) cosa facoltà di redistribuire lo stoccaggio dei dati, in forma criptata e non aggregata, fuori dai confini europei.

Sistema server di stoccaggio email imap: offerto da fornitore esterno Italiano con data center interamente europei
Sistema remoto cloud: offerto da fornitore esterno con data center interamente europei.

Gestione ed archiviazione password:
Le password sono conservate su sistemi remoti ad accesso vincolato da password di accesso, in server remoto, in forma criptato AES-256 bit. L'accesso avviene con l'inserimento di password anche questa cambiata a cadenza mensile

Gestione documentazione cartacea
Nessuna documentazione cartacea, ad eccezione di quella necessaria per l'attività amministrativa e fiscale, viene tenuta in questo formato, ma viene immediatamente digitalizzata e raccolta su sistemi di elaborazione ed archiviazione. Il supporto fisico stampato viene eliminato e reso non intelligibile prima della distruzione

Assenza del Registro dei trattamenti

In osservanza dell'articolo 3 corpo 5 del GDPR viene riconosciuto il diritto all'esonero dell'obbligo di tenuta del Registro dei trattamenti, in quanto la ditta ha una struttura con meno di 250 dipendenti e in quanto il trattamento effettuato viene attuato su dati che non presentano oggettivamente un rischio per i diritti e le libertà dell'interessato, il trattamento non è occasionale e non include il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10

Assenza del Privacy Impact Assessment preventivo

Il PIA preventivo, in osservanza con quando indicato dal Regolamento Europeo 679/2016, viene ritenuto non necessario, oltreché non obbligatorio, in mancanza di un rischio specifico valutato dal data controller, per la mancanza di rischi specifici dovuti alla esiguità dei dati trattati; non si è in presenza infatti di una elevata mole di dati.

L'azione di gestione dati raccolti avviene comunque nella conformità con le normative, e nei requisiti di politica legali applicabili per la privacy.

Azioni di Data Breach

In caso di accertamento di violazione dei dati personali detenuti o affidati alla ditta, è previsto che il titolare del trattamento notifichi la violazione all'autorità di controllo competente (articolo 55) senza ingiustificato ritardo e, comunque entro 72 ore dal momento in cui ne è venuto a conoscenza

La notifica descriverà la natura della violazione dei dati personali e sarà corredata da tutte le informazioni relative (categorie, numero degli interessati e delle registrazioni), descriverà le probabili conseguenze della violazione dei dati personali e le misure che si propone di adottare per porre rimedio alla violazione stessa

Tale notifica sarò firmata dal titolare del trattamento.

Inoltre il titolare del trattamento deve attivarsi per dimostrare contestualmente di avere messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione; deve pertanto documentare la costante azione di cifratura dei dati attuata e provare che questa attività non sia venuta meno nel corso del tempo o che non abbia avuto falle di gestione.

Contestualmente il titolare del trattamento metterà in atto una analisi attenta delle cause del data breach e porrà in atto decisioni per fare si che tale situazione non venga a ripetersi. Si elencano in questa sede come possibili interventi la variazione della forma di cifratura, il cambio necessario di chiave, l'appoggio a servizi terzi diversi per l'azione di cifratura e tenuta dati.

Consenso dell'interessato

Il consenso alla gestione ed al trattamento dei dati viene realizzato con comunicazione specifica della suddetta attività di gestione, realizzata in ossequio dei principi di liberalità, specificità e chiarezza imposti dal GDPR.

Nello specifico la documentazione inviata è svincolata da qualunque informativa non negoziabile, come ad esempio la informativa sulle condizioni generali, avendosi una chiara separazione delle informazioni relative all'ottenimento del consenso per le attività di elaborazione dati dalle informazioni su altri argomenti.

Nelle comunicazioni di consenso dell'interessato viene specificatamente indicata l'identità del titolare della gestione dati, lo scopo di ciascuna delle operazioni di trattamento per le quali è richiesto il consenso, quali tipo di dati saranno raccolti e trattati, l'esistenza del diritto di revocare il consenso, le Informazioni sull'uso dei dati per le decisioni basate esclusivamente sull'elaborazione automatica.

Ogni operazione di comunicazione farà capo ad un preciso consenso formalizzato presentabile nel caso l'interessato ne facesse richiesta.
L'interessato ha il diritto di revocare qualsiasi consenso abbia dato e deve essere informato di questo dal titolare del trattamento.

_____

redatto nel mese di Maggio 2018

Il titolare del trattamento
Dott. Alberto Crosio