

VALUTAZIONE RISCHI SULLA PROTEZIONE DEI DATI PERSONALI (ART.35 REGOL.UE 2016/679)

Ai fini del regolamento europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, si intende assolvere alla valutazione dei rischi, all'adozione di adeguate misure di sicurezza per la tutela preventiva e i criteri organizzativi seguiti per una corretta attuazione. Il documento fa riferimento all'azienda:

Denominazione: [LIBERA][MENTE CONSULENZA E PRATICHE FILOSOFICHE DI ALBERTO LATORRE

indirizzo: VIA SAN CARLO, 16 – 25080 – MUSCOLINE (BS)

Partita IVA: 02470170982

Codice Fiscale: LTRLRT74M22B157I

Definizione soggetti - titolare al trattamento e responsabili

Tenuto conto degli obblighi derivanti dal regolamento in oggetto, e delle responsabilità a seguito del trattamento si definisce:

- **Titolare al trattamento dei dati personali:** persona fisica che determina le finalità, i mezzi e criteri da seguire per l'insieme delle operazioni che coinvolgono qualsiasi informazione riguardante una persona fisica identificabile. Tale soggetto è individuato nella persona:

ALBERTO LATORRE cod.fisc. LTRLRT74M22B157I in quanto titolare legale rappresentante dell'azienda

- **Responsabile al trattamento:** qualsiasi persona o autorità che tratta i dati personali per conto del titolare del trattamento nominato attraverso formale incarico o mediante designazione per iscritto, qui individuato nella persona:
- ALBERTO LATORRE cod.fisc. LTRLRT74M22B157I in quanto titolare legale rappresentante dell'azienda

I dati verranno utilizzati unicamente dagli addetti incaricati e dagli enti a cui l'interessato richiede la prestazione.

Finalità del trattamento

Il presente documento, unito al consenso debitamente compilato e firmato dal soggetto destinatario servono per tutelare, stabilire criteri e procedure per la protezione dei dati personali e garantire misure di sicurezza adatte a prevenire eventuali rischi, interni ed esterni, derivanti da:

- Calamità naturali o eventi distruttivi artificiali: perdita di dati da allagamento, incendio, movimenti tellurici;
- Minacce intenzionali: accessi non consentiti, furto, manomissione di dati su supporti cartacei e informatici, accessi non autorizzati, perdita di dati dovuta a virus o intrusione informatica;
- Minacce involontarie: blackout elettrico, malfunzionamenti software, malfunzionamenti hardware;

a seguito di attuazione di:

- Obblighi da contratto, o per adempiere, prima e dopo l'esecuzione, a specifiche richieste;
- Adempimenti di obblighi di legge di natura amministrativa, contabile, civilistica, fiscale, regolamenti, normative comunitarie ed extracomunitarie;
- Gestione dei clienti (amministrazione, ordini, contratti, fatture)
- Gestione dei fornitori (amministrazione, ordini, contratti, fatture)

Principi del trattamento

I dati richiesti saranno:

- Trattati in modo lecito, corretto e trasparente
- Raccolti unicamente per le finalità richieste
- Adeguati, pertinenti e limitati

- Esatti ed aggiornati
- Conservati e trattati per garantire un'adeguata sicurezza

Categorie Dati Personali

Il genere di dati che possono entrare in possesso del titolare del trattamento sarà:

- anagrafici (generalità, indirizzo, data e luogo di nascita, codice fiscale)
- bancari (IBAN, metodi di pagamento)
- dati comuni relativi a clienti e fornitori per finalità contabili e di fornitura beni/servizi
- dati relativi allo svolgimento dell'attività ed alle informazioni commerciali

Strumenti utilizzati

I dati verranno trattati attraverso:

- Schedari e supporti cartacei: i documenti saranno conservati per la durata massima di 10 anni raccolti in archivi e sistemati nei locali dello Studio
- Sistema informatico aziendale: l'azienda dispone di una rete informatica privata realizzata con collegamenti wi-fi e provvisti di collegamento ad internet, costituita da:
nr. 1 modem
- Banca Dati e supporti di memorizzazione: i dati verranno memorizzati periodicamente attraverso copie backup su computer e dispositivi esterni di archiviazione (hard disk e chiavette usb), conservati in luogo chiuso e protetti.

Analisi del rischio e misure di sicurezza

L'analisi di un potenziale e grave rischio per i diritti e le libertà dell'interessato sono determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento sulla base di una valutazione oggettiva. La valutazione riguarda la possibilità del verificarsi di danni fisici, materiali, immateriali.

- *Calamità naturali o avvenimenti distruttivi artificiali*
 - *Allagamento:* considerata la posizione dell'azienda, si esclude la probabilità del verificarsi dell'evento, tuttavia tutti i documenti e i sistemi informatici sono rialzati o disposti su ripiani.
 - *Incendio:* sono state adottate misure di prevenzione previste dalla legislazione in materia di sicurezza come la verifica periodica di caldaie, l'impianto elettrico, di condizionamento, la manutenzione ordinaria degli estintori.
 - *Movimenti tellurici:* considerata la posizione dell'azienda sono state adottate le misure previste dagli eventi di questo genere, uscite di emergenza, dispositivi di sicurezza e planimetrie.
- *Minacce intenzionali*
 - **Accessi non consentiti:** solo il titolare e il responsabile al trattamento hanno la possibilità di aprire e chiudere i locali dell'azienda
 - **Accessi non autorizzati, furti e manomissioni:** i dati su supporto cartaceo sono custoditi, archiviati in faldoni o scatole e nascosti al pubblico all'interno di armadi in locali chiusi. Eventuali documenti gettati via verranno distrutti manualmente o utilizzando un apposito distruggidocumenti per evitare che qualsiasi soggetto esterno possa identificarne il significato.
Tutto ciò che verrà trattato per le finalità richieste, sarà nascosto al pubblico ed inserito in cartelline non trasparenti ed in armadi chiusi.
 - **Virus o intrusione informatica:** i dispositivi informatici, chiusi e riparati, sono protetti attraverso sistemi di autenticazione conosciuti solo all'incaricato del trattamento, variati periodicamente e custoditi in buste sigillate all'interno di armadi chiusi a chiave.
In caso di momentaneo abbandono della postazione di lavoro, i computer sono protetti da screensaver con blocco della sessione, attivabile unicamente con password conosciuta solo dall'incaricato.

Come forma di tutela in tempo reale, ogni dispositivo è fornito di antivirus, attivo, aggiornato e rinnovato periodicamente, firewall e altri software antintrusione.

- *Minacce involontarie*

- **Blackout elettrico:** in caso di malfunzionamenti alla rete elettrica, i dispositivi sono provvisti di gruppi di continuità per garantire il salvataggio, la conservazione e la prevenzione dalla perdita improvvisa di dati
- **Malfunzionamenti software/hardware:** l'azienda viene seguita dal servizio di assistenza delle case software utilizzati e dal fornitore dei dispositivi informatici, in caso di difetti, problemi o qualsiasi evento che non porti a buon fine l'esecuzione del proprio operato.

Al fine di conservare correttamente tutti i dati informatici utilizzati, oltre ai dispositivi elettronici, vengono effettuate copie periodiche di backup e punti di ripristino su disco fisso esterno e chiavette usb esterne, sigillate in buste non trasparenti, archiviate in armadi chiusi a chiave e in luoghi conosciuti solo agli addetti al trattamento.

Aggiornamento

L'azienda si impegna, tenendo conto dello stato dell'arte e dei costi di attuazione, a muoversi per tenere aggiornati i sistemi di sicurezza, utilizzando le misure più appropriate al raggiungimento delle finalità richieste, al riesame periodico, o immediato, della valutazione dei rischi e delle procedure di protezione, mantenimento e tutela.

Firma del titolare del trattamento

Muscoline (BS), li 28 maggio 2018

Alberto Latorre