Informativa sul trattamento dei dati personali

La presente Privacy Policy ha lo scopo di descrivere le modalità di gestione del sito internet http://notaicomolecco.it (di seguito: il "Sito") con riferimento al trattamento dei dati personali degli utenti.

Si tratta di una informativa generale resa nel rispetto dell'art. 13 del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito: il "Regolamento") a tutti gli utenti che consultano e/o si registrano e, più in generale, interagiscono con i servizi resi attraverso il Sito, amministrato e gestito dal Collegio Notarile dei Distretti Riuniti di Como e Lecco - Via Bossi, 8 - Tel. 031 260323 - 22100 Como – email: info@notaricomolecco.it (di seguito: il "Titolare" o il "Collegio").
In questa informativa Le illustreremo le finalità e le modalità con cui il Titolare raccoglie e tratta i suoi dati personali, quali categorie di dati sono oggetto di trattamento, quali sono i diritti degli interessati al trattamento e come possono essere esercitati.

L'informativa è resa esclusivamente per il presente Sito, pertanto il Titolare non si assume nessuna responsabilità in merito agli altri siti web eventualmente consultati tramite collegamenti ipertestuali presenti sul sito stesso. La presente informativa è però relativa anche ad eventuali siti, con top level domain differenti, di titolarità e/o gestiti dal Titolare del trattamento, a cui l'utente può essere reindirizzato dal presente Sito.
Gli utenti, utilizzando il presente Sito, accettano la presente informativa e sono, pertanto, invitati a prenderne visione prima di fornire informazioni personali di qualsiasi genere.

1. Categorie di dati personali

a. Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento di questo sito web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del Sito.

b. Dati forniti volontariamente dall'utente

Fatto salvo quanto sopra specificato in relazione ai dati di navigazione, il Titolare acquisirà i dati personali eventualmente forniti dall'utente attraverso il Sito per accedere a determinati servizi (es. tramite l'Area riservata), ovvero per effettuare richieste via posta elettronica. A titolo

PROCEDURE PER DATA BREACH

Definizioni

La presente procedura è adottata dal Consiglio Nazionale del Notariato con sede legale in Roma, Via Flaminia 160**.**

Il Titolare del trattamento ha nominato un Responsabile del trattamento (DPO), individuato nello Studio Legale E-Lex, con sede legale in via dei Barbieri, 6, Roma.

Ai fini della presente procedura, valgono le seguenti definizioni:

a) Titolare del trattamento: “la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri”.

b) Responsabile del trattamento: “La persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento”.

c) Incaricato del trattamento: “La persona fisica che nell’ambito della struttura aziendale del Titolare è autorizzata a effettuare attività di trattamento di dati personali”.

d) DPO: “Il Responsabile del trattamento come individuato dalla Sezione 4 (artt. 37-39) del Regolamento (UE) n. 2016/679”.

e) Dato personale: “Qualunque informazione relativa a persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, generica, psichica, economica, culturale o sociale”.

f) Trattamento: “qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione”.

Procedura per il data breach

Ai sensi del Regolamento (UE) n. 2016/679, il Titolare del trattamento, in caso sia consapevole di una violazione dei Dati personali trattati, è tenuto: (i) a informare l’Autorità di controllo (il Garante per la protezione dei dati personali, nel caso del territorio italiano) entro e non oltre le 72 ore successive all’avvenuta conoscenza della violazione. Si precisa che il Titolare non è tenuto alla notifica se sia improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà degli Interessati - e, (ii) nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, a informare senza ritardo anche gli stessi Interessati.

A tal fine, il Titolare del trattamento, come sopra identificato, ha previsto un apposito processo per la notifica in caso di Data Breach.

Al fine di rendere effettiva il processo di notifica, è altresì importante che tutti coloro che nell’ambito del rapporto di lavoro e/o di collaborazione trattano Dati personali del Titolare del trattamento siano

previamente sensibilizzati e partecipino attivamente a tale processo, segnalando tempestivamente ogni caso di violazione di cui siano venuti a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione.

Data Breach e potenziali scenari

Il GDPR definisce violazione dei dati personali o Data Breach "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*" (art. 4, n. 12). Le indicazioni di cui alla presente sezione della Procedura valgono per qualsiasi tipologia di Dato personale.

Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, le banche dati gestite dal Titolare del trattamento.

Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione:

- ✓ furto o smarrimento di laptop, smartphone, tablet aziendali contenenti Dati personali;
- ✓ furto o smarrimento di documenti cartacei contenenti Dati personali;
- ✓ furto o smarrimento di dispositivi portatili di archiviazione non criptati, come chiavette USB e hard disk esterni, contenenti Dati personali;
- ✓ perdita o modifica irreparabile di archivi contenenti Dati personali in formato digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali aziendali che non possa essere ripristinata attraverso l'uso di un backup);
- ✓ diffusione impropria di Dati personali, per mezzo di:
  - o invio di e-mail contenente Dati personali al destinatario errato;
  - o invio di e-mail con un file contenente Dati personali allegato erroneamente;
  - o esportazione fraudolenta o errata di Dati personali dai sistemi aziendali;
- ✓ richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;
- ✓ segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

1. Processo di gestione del Data Breach

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Data Breach che prevede:

- ✓ Rilevazione e segnalazione del Data Breach;
- ✓ Analisi del Data Breach;
- ✓ Risposta e notifica del Data Breach;
- ✓ Registrazione del Data Breach.

2. Rilevazione e segnalazione del Data Breach

La rilevazione e segnalazione del Data Breach è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento. Nel caso in cui si verifichi uno degli eventi descritti o in tutti gli altri casi in cui il soggetto che tratta dati personali del Titolare del trattamento sia consapevole di altri eventi potenzialmente rischiosi per i diritti e le libertà dei soggetti interessati è tenuto a informare immediatamente il responsabile dei sistemi informatici e/o il responsabile per la protezione dei dati personali (DPO). Nel caso in cui tali figure non siano disponibili o non diano seguito tempestivamente alla segnalazione, è necessario informare direttamente il Titolare del trattamento.

3. Analisi del Data Breach

A seguito della segnalazione, il responsabile dei sistemi informatici e/o il responsabile per la protezione dei dati personali (DPO) effettuano una valutazione preliminare al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dal Titolare del trattamento.

L'analisi successiva è eseguita dal Titolare del trattamento, sentiti nuovamente il responsabile dei sistemi informatici (qualora il Data Breach investa una vulnerabilità dei sistemi informatici) e/o il responsabile per la protezione dei dati personali (DPO). La suddetta analisi è finalizzata alla raccolta ed identificazione delle seguenti informazioni:

- ✓ categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, clienti, dipendenti, fornitori, etc.);
- ✓ categorie di Dati personali compromessi (ad esempio, Dati personali, Dati sensibili, Dati giudiziari);
- ✓ tipologia di Data Breach: violazione della riservatezza, disponibilità o integrità (ad esempio, accesso non autorizzato, perdita, alterazione, furto, *disclosure*, distruzione, etc.).

Nell'ambito di tale analisi, il Titolare del trattamento competente e il DPO devono identificare le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti della violazione dei Dati personali.

Inoltre, il Titolare del trattamento e il DPO sono tenuti ad effettuare un'analisi di dettaglio finalizzata all'identificazione e alla formalizzazione delle seguenti informazioni:

- ✓ identificabilità degli Interessati;
- ✓ misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o *in toto* mitigato gli impatti relativi al Data Breach;
- ✓ ritardi nella rilevazione del Data Breach;
- ✓ numero di individui interessati.

Sulla base dei suddetti parametri, il Titolare del trattamento competente e il DPO predispongono una valutazione della gravità del Data Breach relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei Dati personali (ad esempio, Dati Sensibili e/o Giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

4. Risposta e notifica del Data Breach

La precedente fase di analisi fornisce al Titolare del trattamento gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dalla violazione di Dati personali rilevata.

Nel caso in cui dovesse risultare improbabile che il Data Breach presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO.

Qualora al contrario dovesse risultare possibile che il Data Breach presenti rischi per i diritti e le libertà degli Interessati, il Titolare del trattamento, con il supporto del DPO, provvedono a predisporre la notifica all'Autorità Garante.

La notifica deve essere comunicata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

La suddetta notifica deve contenere almeno le seguenti informazioni:

- ✓ natura della violazione dei dati personali (*disclosure*, perdita, alterazione, accesso non autorizzato, etc.);
- ✓ tipologie di Dati personali violati;
- ✓ categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;
- ✓ nome e dati di contatto del DPO, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;
- ✓ probabili conseguenze della violazione dei Dati personali;
- ✓ descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;
- ✓ ove la stessa non sia presentata entro 72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, il Titolare del trattamento, ove occorra, con la collaborazione del DPO, raccolgono quanto prima le informazioni supplementari e provvedono a integrare, senza ritardo, la notifica già inoltrata all'Autorità di Controllo.

Oltre a notificare il Data Breach all'Autorità Garante, il Titolare del trattamento è tenuto a valutare l'esigenza di procedere con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, il Titolare del trattamento, di concerto con il DPO, deve valutare i seguenti fattori:

- ✓ il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;
- ✓ gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
- ✓ sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
- ✓ in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la

salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

- ✓ sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;
- ✓ il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La notifica agli Interessati deve, pertanto, avvenire nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

- ✓ sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (e.g., misure di cifratura);
- ✓ a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;
- ✓ la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso occorrerà comunque procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia.

Il Titolare del trattamento, di concerto con il DPO, valutano di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi e lo propongono al Titolare, che procede di conseguenza.

In ogni caso la notifica agli Interessati deve contenere quanto meno:

- ✓ nome e dati di contatto del DPO;
- ✓ descrizione delle probabili conseguenze della violazione;
- ✓ descrizione delle misure adottate o che il Titolare intende adottare per porre rimedio alla violazione e ridurre gli effetti negativi.

5. Registrazione del Data Breach

Il Titolare del trattamento, al fine di documentare le violazioni dei dati personal verificatisi, istituisce un registro interno (di seguito, anche “Data Breach Inventory”) contenente tutte le violazioni di dati personali verificatesi a prescindere dalla relativa notifica all’Autorità Garante.

Nel Data Breach Inventory, tenuto in formato informatico e custodito dal Titolare del trattamento, devono essere puntualmente annotate:

- ✓ L’identificativo (ID) del Data Breach;
- ✓ Data e ora dell’inserimento della rilevazione nel registro;
- ✓ Nome e descrizione del trattamento;
- ✓ Nome del Titolare del trattamento;
- ✓ Nome del Responsabile del trattamento (se presente);
- ✓ Data e ora della violazione;
- ✓ Descrizione della violazione;

- ✓ Tipologia di Data Breach e le relative cause;
- ✓ Conseguenze ed effetti per i diritti e le libertà degli Interessati;
- ✓ Azioni correttive adottate;
- ✓ Data e ora della notifica al Garante (se avvenuta);
- ✓ Copia della notifica al Garante
- ✓ Data e ora della notifica agli Interessati (se avvenuta);
- ✓ Mezzo con il quale è effettuata la notifica agli interessati (se avvenuta).

Il Data Breach inventory è conservato e aggiornato ad opera del Titolare del trattamento, con il supporto del DPO.

Il DPO ha la responsabilità in merito all'esecuzione di attività di monitoraggio e controllo al fine di verificare l'effettivo aggiornamento di tale registro.

6. Data Breach relativo a dati personali trattati in qualità di Responsabile del trattamento

Qualora, a seguito di una segnalazione o nel corso dell'analisi preliminare di cui al precedente paragrafo 4, il Titolare del trattamento rilevassero che la violazione qualificabile come Data Breach riguarda dati personali di titolarità di un soggetto terzo trattati dal Titolare del trattamento in qualità di Responsabile del trattamento, procedono a informare senza ingiustificato ritardo il soggetto terzo titolare del trattamento secondo le istruzioni dallo stesso fornite.

Nel dettaglio, la comunicazione al soggetto titolare del trattamento dovrà contenere quanto meno le seguenti informazioni (oltre a quelle eventualmente richieste dallo stesso soggetto terzo titolare del trattamento):

- ✓ Descrizione della natura della violazione dei dati personali comprensiva, ove possibile, di informazioni in merito alle categorie e al numero di Interessati nonché alle categorie e al volume approssimativo di dati personali oggetto di violazione;
- ✓ Nome e dati di contatto del DPO;
- ✓ Descrizione delle possibili conseguenze della violazione;
- ✓ Descrizione di eventuali misure già adottate o di cui si prevede l'adozione per porre rimedio alla violazione di dati personali e per attenuarne i possibili effetti negativi.

La comunicazione, nel testo convalidato dal DPO, sarà inviata al soggetto titolare del trattamento entro 48 ore dall'avvenuta rilevazione della violazione o nel minore termine eventualmente indicato dal soggetto titolare del trattamento.

7. Prescrizioni per la prevenzione di Data Breach

Il Titolare del trattamento adotta specifiche strategie per prevenire o minimizzare il verificarsi di Data Breach.

In primo luogo, occorre che tutti gli Incaricati del Trattamento siano consapevoli dei Dati personali che trattano attraverso i propri strumenti (anche cartacei) e dispositivi o a cui hanno accesso tramite i sistemi del Titolare del trattamento. A tal fine, la presente procedura viene loro comunicata dal Titolare del trattamento essi dovranno custodire tali Dati personali ed i relativi documenti con cura e in modo responsabile sia all'interno che all'esterno della propria area di lavoro. Si precisa che i soggetti in questione sono già stati istruiti per mezzo di nomina ad Incaricati del trattamento.

Gli Incaricati del trattamento, nello specifico, devono salvare preferibilmente sui dispositivi e sulle cartelle di rete e stampare e conservare presso la propria postazione di lavoro i documenti cartacei contenenti dati personali strettamente necessari al completamento delle proprie attività.

Una volta terminato l'utilizzo, essi devono cancellare i dati personali non più necessari dal proprio dispositivo o da cartelle di rete e server e distruggere i documenti cartacei.

In linea generale, gli Incaricati del Trattamento devono seguire le seguenti buone prassi di sicurezza per la protezione dei supporti (anche cartacei) e dispositivi che potrebbero contenere Dati personali, per prevenire possibili violazioni, già illustrate nella nomina ad Incaricati del trattamento.

Per finalità di prevenzione del furto o dello smarrimento di laptop e dispositivi mobili al di fuori dell'ufficio e in viaggio, gli Incaricati del Trattamento devono:

- ✓ evitare di lasciare il laptop o dispositivo mobile incustodito in luoghi pubblici, anche se temporaneamente;
- ✓ al momento di riporre il laptop per un viaggio o spostamento, considerare l'opzione di spegnimento o di ibernazione per sfruttare tutti i benefici della cifratura del disco nel caso il dispositivo venga perso o rubato;
- ✓ nel caso di trasporto del laptop o dispositivo mobile in automobile in caso di sosta dell'auto in area non custodita è obbligatorio portarlo con sé e non è consentito riporlo nel bagagliaio;
- ✓ non lasciare il laptop o dispositivo mobile incustodito in automobile durante la notte, anche se riposto nel bagagliaio in maniera non visibile;
- ✓ non mantenere le proprie password scritte in modo esplicito insieme al laptop o ai dispositivi mobili;
- ✓ quando si viaggia portando con sé laptop o dispositivi mobili, verificare di averli con sé quando si lascia l'hotel, l'aeroporto o i mezzi di trasporto (p.e. aereo, treno, autobus, taxi);
- ✓ quando si utilizzano mezzi di trasporto pubblico, tenere la borsa contenente il laptop con attenzione vicino a sé.

Per finalità di prevenzione del furto o smarrimento di documenti cartacei, gli Incaricati devono:

- ✓ evitare, laddove possibile, di possedere copie cartacee di documenti contenenti Dati personali all'esterno delle sedi del Titolare del trattamentoa meno di necessità ed evitare di lasciare copie incustodite in luoghi pubblici;
- ✓ rendere non più leggibili i Dati personali contenuti nei documenti cartacei prima di gettare tali documenti.

<u>Per finalità di prevenzione della diffusione impropria, gli Incaricati del Trattamento devono:</u>

- ✓ evitare di fornire Dati personali nel caso in cui si riceva una e-mail di richiesta che presenta elementi anomali (ad esempio, e-mail inviata in orari non lavorativi, scritta in un linguaggio non corretto o inusuali, contenente link o form di inserimento credenziali) e segnalare tale e-mail come potenziale attacco di *phishing*.

esemplificativo, il Sito potrebbe acquisire nome, cognome, data di nascita, indirizzo e-mail, nome utente, password, indirizzo di residenza, sede dello studio, data di iscrizione all'albo.

c. Dati acquisiti in occasione della fruizione dei servizi

Il Titolare potrebbe acquisire inoltre alcuni dati personali riferibili all'utente registrato in occasione della fruizione dei servizi offerti dal Titolare attraverso il Sito. I dati personali sopra indicati saranno trattati dal Titolare esclusivamente per le finalità e nei limiti indicati al paragrafo successivo.

2. Finalità e base giuridica del trattamento

a. per l'erogazione dei servizi richiesti

I dati indicati al paragrafo 1 lett. b) e c) saranno trattati dal Titolare per consentirle la registrazione al Sito e/o la fruizione dei servizi ad esso specificatamente connessi e comunque per finalità istituzionali del Titolare, quali l'effettuazione di ricerche o indagini con finalità scientifiche o statistiche e/o l'inoltro di comunicazioni sull'attività del Collegio e sui servizi dalla stessa offerti ai propri iscritti, per fornire eventuali servizi in abbonamento, per lo svolgimento di qualsiasi attività attinente ai servizi stessi quali, a mero titolo d'esempio, la verifica qualitativa del servizi offerti, la percentuale di soddisfazione degli utilizzatori, la comunicazione di eventuali problemi o l'interruzione dei servizi stessi, nonché per informazioni relative a nuovi servizi e di aggiornamenti su iniziative organizzate, patrocinate e/o supportate dal Collegio. Il conferimento di tali dati è, pertanto, necessario.

b. per l'adempimento degli obblighi di legge

I dati indicati al paragrafo 1 lett. b) e c) saranno trattati dal Titolare ai fini dell'adempimento di obblighi previsti dalla legge, dalla normativa comunitaria nonché dalle disposizioni impartite dalle Autorità a ciò legittimate dalla legge.

3. Categorie di soggetti ai quali i dati personali possono essere comunicati e finalità della comunicazione

Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate a soggetti terzi, che tratteranno i suoi dati personali in qualità di Responsabili del trattamento, quali i consulenti esterni nei limiti necessari allo svolgimento del proprio mandato (es. società di sviluppo e manutenzione sistemi informatici e/o che svolgono attività di elaborazione dati; studi/professionisti di consulenza legale; società di consulenza fiscale, amministrativa/contabile).

L'elenco dei responsabili del trattamento può essere richiesto al Titolare scrivendo a Collegio Notarile dei Distretti Riuniti di Como e Lecco - Via Bossi, 8 - Tel. 031 260323 - 22100 Como – email: info@notaricomolecco.it

4. Periodo di conservazione dei dati e durata dei trattamenti

I dati di navigazione saranno oggetto di conservazione per il periodo strettamente necessario e, comunque, non superiore a 12 mesi.

In caso di accesso all'Area riservata, i suoi dati saranno oggetto di conservazione per tutta la durata del rapporto di iscrizione presso il Collegio; in seguito alla cessazione eventuale del rapporto, per qualsiasi motivo avvenuta, i dati saranno conservati per il periodo strettamente

necessario (fino a 10 anni), per esigenze di tutela dei diritti del Titolare e per l'adempimento di obblighi di legge, salvo che non siano previsti, per legge, periodi di conservazione differenti.

5. Diritti degli interessati

La informiamo che, in conformità alla vigente disciplina, ha i seguenti diritti: chiedere e ottenere informazioni circa l'esistenza di propri dati nella disponibilità del Titolare e accesso a tali dati; per i dati oggetto di trattamento con sistemi automatizzati, chiedere la comunicazione dei propri dati e/o il trasferimento ad altro titolare; chiedere e ottenere la modifica e/o correzione dei suoi dati personali se ritiene che siano inaccurati o incompleti; chiedere e ottenere la cancellazione – e/o la limitazione del trattamento - dei suoi dati personali qualora si tratti di dati o informazioni non necessari – o non più necessari – per le finalità che precedono, quindi decorso il periodo di conservazione indicato al paragrafo che precede.
In particolare, le sono riconosciuti i seguenti diritti: artt. 15 - "Diritto di accesso dell'interessato", 16 - "Diritto di rettifica", 17 - "Diritto alla cancellazione", 18 – "Diritto di limitazione al trattamento", 20 – "Diritto alla portabilità dei dati" del Regolamento UE 2016/679 nei limiti ed alle condizioni previste dall'art. 12 del Regolamento stesso.
Tali richieste potranno essere indirizzate a Collegio Notarile dei Distretti Riuniti di Como e Lecco - Via Bossi, 8 - Tel. 031 260323 - 22100 Como – email: info@notaricomolecco.it
La informiamo che ai sensi della disciplina vigente può proporre eventuali reclami riguardanti i trattamenti di suoi dati personali al Garante per la protezione dei dati personali.
La informiamo che il Titolare ha provveduto a nominare un Responsabile per la protezione dei dati personali contattabile all'indirizzo dpo@e-lex.it

6. Modifica all'informativa

Il Titolare si riserva di modificarne o semplicemente aggiornarne il contenuto della presente informativa, in parte o completamente, anche a causa di eventuali variazioni della normativa applicabile. Tali modifiche e/o aggiornamenti saranno vincolanti non appena pubblicati sul Sito. Il Titolare invita quindi a visitare con regolarità questa sezione per prendere cognizione della più recente ed aggiornata versione dell'informativa ed essere aggiornati sui dati raccolti e sul loro utilizzo.

Cookie Policy

Di seguito si riporta la Cookie policy da utilizzare quale informativa estesa ai sensi dell'art. 13 D.lgs. 196/2003 (di seguito "**Codice Privacy**") e degli artt. 13 e 14 del Regolamento (UE) 2016/679 (di seguito "**GDPR**").

Cosa sono i Cookie?

I Cookie sono pacchetti di informazioni inviate da un web server (es. il sito) al browser Internet dell'utente, da quest'ultimo memorizzati automaticamente sul computer e rinviati automaticamente al server ad ogni successivo accesso al sito.

Per default quasi tutti i browser web sono impostati per accettare automaticamente i cookie.

Tipicamente i cookie possono essere installati:

- Direttamente dal proprietario e/o responsabile del sito web (c.d. *cookie di prima parte*)
- da responsabili estranei al sito web visitato dall'utente (c.d. *cookie di terza parte*). Ove non diversamente specificato, si rammenta che questi cookie ricadono sotto la diretta ed esclusiva responsabilità dello stesso gestore. Ulteriori informazioni sulla privacy e sul loro uso sono reperibili direttamente sui siti dei rispettivi gestori.

Questo sito web può utilizzare, anche in combinazione tra di loro i seguenti tipi di cookie classificati in base alle indicazioni del Garante Privacy e dei Pareri emessi in ambito Europeo dal Gruppo di Lavoro ex art. 29 del GDPR:

- ***Sessione*** che non vengono memorizzati in modo persistente sul computer dell'utente e si cancellano con la chiusura del browser, sono strettamente limitati alla trasmissione di identificativi di sessione necessari per consentire l'esplorazione sicura ed efficiente del sito evitando il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti
- ***Persistenti*** che rimangono memorizzati sul disco rigido del computer fino alla loro scadenza o cancellazione da parte degli utenti/visitatori. Tramite i cookie persistenti i visitatori che accedono al sito (o eventuali altri utenti che impiegano il medesimo computer) vengono automaticamente riconosciuti ad ogni visita. I visitatori possono impostare il browser del computer in modo tale che accetti/rifiuti tutti i cookie o visualizzi un avviso ogni qual volta viene proposto un cookie, per poter valutare se accettarlo o meno. L'utente può, comunque, modificare la configurazione predefinita e disabilitare i cookie (cioè bloccarli in via definitiva), impostando il livello di protezione più elevato.
- ***Tecnici*** sono i cookie utilizzati per autenticarsi, per usufruire di contenuti multimediali tipo flash player o per consentire la scelta della lingua di navigazione. In generale non è quindi necessario acquisire il consenso preventivo e informato dell'utente. Rientrano in questa fattispecie anche i cookie utilizzati per analizzare statisticamente gli accessi/le visite al sito solo se utilizzati esclusivamente per scopi statistici e tramite la raccolta di informazioni in forma aggregata.
- ***Non tecnici*** sono tutti i cookie usati per finalità di profilazione e marketing. Il loro utilizzo sui terminali degli utenti è vietato se questi non siano stati prima adeguatamente informati e non abbiano prestato al riguardo un valido consenso secondo la tecnica dell'opt-in. Questi tipi di cookie sono, a loro volta, raggruppabili in base alle funzioni che assolvono in:
  - ✓ ***Analitycs.*** Sono i cookie utilizzati per raccogliere ed analizzare informazioni statistiche sugli accessi/le visite al sito web. In alcuni casi, associati ad altre informazioni quali le

credenziali inserite per l'accesso ad aree riservate (il proprio indirizzo di posta elettronica e la password), possono essere utilizzate per profilare l'utente (abitudini personali, siti visitati, contenuti scaricati, tipi di interazioni effettuate, ecc.).

- ✓ ***Widgets***. Rientrano in questa categoria tutti quei componenti grafici di una interfaccia utente di un programma, che ha lo scopo di facilitare l'utente nell'interazione con il programma stesso. A titolo esemplificativo sono widget i cookie di facebook, google+, twitter.
- ✓ ***Advertsing***. Rientrano in questa categoria i cookie utilizzati per fare pubblicità all'interno di un sito. Google, Tradedoubler rientrano in questa categoria.
- ✓ ***Web beacons.*** Rientrano in questa categoria i frammenti di codice che consentono a un sito web di trasferire o raccogliere informazioni attraverso la richiesta di un'immagine grafica. I siti web possono utilizzarli per diversi fini, quali l'analisi dell'uso dei siti web, attività di controllo e reportistica sulle pubblicità e la personalizzazione di pubblicità e contenuti.

I cookie presenti sul Sito

Cookie tecnici per i quali non è richiesto il consenso

Il Collegio installerà sul suo dispositivo e, in particolare, nel suo browser o lascerà installare a terzi alcuni cookie che ci sono necessari per acquisire informazioni statistiche in forma anonima e aggregata relative alla sua navigazione sulle pagine del Sito.

Per i trattamenti di dati personali che, previo suo consenso, società terze non note al titolare del trattamento potrebbero porre in essere attraverso i cookie, collegandosi a questo link ed avvalendosi del relativo servizio potrà personalizzare le sue scelte: http://www.youronlinechoices.com/it/le-tue-scelte

Come disabilitare i cookie mediante configurazione del browser

Se lo desidera può gestire direttamente i cookie anche attraverso le impostazioni del suo browser. Tuttavia, cancellando i cookies dal browser potrebbe rimuovere le preferenze che ha impostato per il presente Sito, per questo sarebbe opportuno che visitasse periodicamente questa pagina per ricontrollare le sue preferenze.

Per ulteriori informazioni e supporto è possibile anche visitare la pagina di aiuto specifica del web browser che si sta utilizzando:

- **Internet Explorer**
  Firefox
- **Safari**
- **Chrome**
- **Opera**