**PROCEDURE PER L’ADEGUAMENTO ED IL RISPETTO DELLE NORME PREVISTE DAL REGOLAMENTO**

## *PREMESSA*

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate per il trattamento dei dati personali, identificativi, sensibili e giudiziari effettuato da parte dell’Avv. \_\_\_\_\_\_\_\_\_\_\_\_\_ (nato a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) e dell’Avv.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (nato a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_\_), titolari dello Studio Legale con sede in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, nell’ambito della loro attività professionale di avvocati.

Nel presente documento si forniscono idonee informazioni riguardanti:

* 1. l’elenco dei trattamenti di dati personali (*Art. 30 lett. c),* mediante:
		+ la individuazione dei tipi di dati personali trattati
		+ la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
		+ l’indicazione delle finalità per cui vengono trattati i dati (Art. 30 lett. b)
	2. il nominativo e i dati di contatto dei titolari del trattamento, nonché la distribuzione dei compiti e delle responsabilità, nell’ambito delle strutture preposte al trattamento dei dati (Art. 30 lett. a) e previsione di interventi formativi degli incaricati del trattamento
	3. l’analisi dei rischi che incombono sui dati, nonché le misure, già adottate e da adottare, per garantire l’integrità e la disponibilità dei dati; i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento i criteri da adottare, per garantire l’adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all’esterno (*art. 30 lett. g*)
	4. Considerazioni conclusive e conseguenze applicative
	5. Dichiarazione d’impegno e firma.

**Indice**

|  |  |  |
| --- | --- | --- |
| 1 | Elenco dei trattamenti dei dati personali | Pag. 2 |
|  | 1.1 Tipologie di dati trattati |  |
|  | 1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti |  |
| 2 | Mansionario privacy ed interventi formativi degli incaricati | Pag. 4 |
| 3 | Analisi dei rischi che incombono sui dati | Pag. 5 |
| 4 | Misure atte a garantire l’integrità e la disponibilità dei dati | Pag. 6 |
|  | 4.1 La protezione di aree e locali |  |
|  | 4.2 La custodia e l’archiviazione di atti, documenti e supporti |  |
|  | 4.3 Le misure logiche di sicurezza |  |
| 5 | Criteri e modalità di ripristino dei dati | Pag. 12 |
| 6 | L’affidamento di dati personali all’esterno | Pag. 13 |
| 7 | Controllo generale sullo stato della sicurezza | Pag. 14 |
| 8 | Considerazioni conclusive e conseguenze applicative | Pag. 14 |
| 9 | Dichiarazioni d’impegno e firma | Pag. 14 |

**1. Elenco dei trattamenti dei dati personali**

**1.1 Tipologie di dati trattati**

I dati trattati dai Titolari risultano essere esclusivamente quelli necessari all’assolvimento dell’incarico difensivo ricevuto dal cliente, per quanto concerne l’attività di assistenza giudiziale, ovvero quelli occorrenti al fine di procedere ad assistenza o consulenza nel quadro dell’attività stragiudiziale, ovvero ad attività di investigazioni difensive (Legge 397/00), ovvero quelli trattati nell’ambito del rapporto di lavoro con personale dipendente all’interno dello stesso studio, ovvero con collaboratori, praticanti o consulenti esterni.

L’insieme della tipologia dei dati trattati ricomprende pertanto i seguenti dati comuni, sensibili e giudiziari relativi a clienti / fornitori / consulenti / personale amministrativo / collaboratori / praticanti:

* dati comuni dei clienti, dei fornitori e di terzi ricavati da albi, elenchi pubblici, visure camerali e di fonti analoghe;
* dati comuni del personale dipendente, collaboratori e praticanti necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, dati richiesti ai fini fiscali, previdenziali, e di natura bancaria e postale;
* dati comuni dei clienti, o dei loro familiari, dagli stessi forniti per l’espletamento degli incarichi affidati allo studio e necessari per l’espletamento di ogni tipo di attività di tutela giudiziaria, compresi i dati sul patrimonio e sulla situazione economica, necessari per fini fiscali, redazione istanze ammissione gratuito patrocinio, oltre a quelli afferenti alla reperibilità ed alla corrispondenza con gli stessi, di natura bancaria e postale;
* dati comuni di terzi, forniti dai clienti per l’espletamento degli incarichi affidati allo studio e necessari per l’espletamento di ogni tipo di attività di tutela giudiziaria, compresi i dati sul patrimonio e sulla situazione economica, necessari per fini fiscali, oltre a quelli afferenti alla reperibilità ed alla corrispondenza con gli stessi, di natura bancaria e postale;
* dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali e dati di natura bancaria e postale;
* dati comuni di altri professionisti ai quali lo studio affida incarichi e si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, inerenti a finalità fiscali, di natura bancaria e postale;
* dati sensibili e giudiziari del personale dipendente, conseguenti al rapporto di lavoro, e inerenti i rapporti con gli enti previdenziali ed assistenziali;
* dati giudiziari dei clienti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, e idonei a rivelare la qualità di imputato e indagato;
* dati giudiziari di terzi idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, e idonei a rivelare la qualità di imputato e indagato;
* dati sensibili dei clienti, dagli stessi forniti o comunque acquisiti per l’espletamento degli incarichi affidati allo studio, idonei a rivelare l’origine razziale ed etnica, le convinzioni e l’adesione ad organizzazioni a carattere religioso, politico, sindacale e filosofico, lo stato di salute e la vita sessuale;
* dati sensibili di terzi, forniti dai clienti o comunque acquisiti per l’espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute o la vita sessuale.

**1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti**

### Ufficio

Il trattamento dei dati personali avviene esclusivamente all’interno dello studio sito al \_\_\_\_\_\_\_\_ piano dell’edificio di V. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

L’accesso al condominio è regolato da [un passaggio attraverso un doppio portone di ingresso] in corrispondenza del numero \_\_\_ di Via \_\_\_\_\_\_\_\_\_\_\_\_.

L’apertura del portone esterno è regolata da un meccanismo automatico avviato da una chiave a lettura magnetica tramite posizionamento della medesima all’interno di un alloggiamento posto all’esterno dell’edificio. Attualmente le chiavi magnetiche in dotazione allo studio risultano essere in numero di \_\_\_\_ di cui \_\_\_\_\_ in possesso dei Titolari dello studio ed \_\_\_\_ in possesso di \_\_\_\_\_\_\_\_\_\_\_\_

L’apertura del portone interno dell’edificio è regolata da un ordinario sistema di apertura meccanica a chiave.

L’ingresso è presidiato da un servizio di portineria, attivo secondo gli orari pattuiti con la proprietà.

[L’accesso all’interno dello studio è possibile attraverso un unico ingresso costituito da un portone a due ante blindato e rinforzato da una barra antisfondamento posizionata all’interno, in corrispondenza dell’anta destra della porta, ed attivata negli orari di chiusura dell’ufficio, oltre ad una ulteriore porta interna in legno dotata di chiusura meccanica a scatto.]

Le finestre e le porte di accesso ai balconi sono protette da [imposte in legno a scorrimento laterale a scomparsa, dotate ciascuna di idoneo sistema di blocco meccanico interno atto ad impedire l’apertura dall’esterno una volta chiuse durante gli orari ed i giorni in cui lo studio non risulta presidiato].

Il locale destinato all’archivio (posizionato al piano \_\_\_) risulta chiuso con idonea serratura a chiave, le cui copie sono in possesso dei Titolari e custodite all’interno dello Studio in una cassetta di sicurezza.

Il trattamento dei dati personali avviene con i **seguenti strumenti**:

**A – Schedari ed altri supporti cartacei**

I supporti cartacei, ed altri supporti idonei a conservare dati personali, ivi inclusi quelli contenenti suoni od immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati all’interno di armadi ciascuno dotato di chiusura a chiave.

**B – Elaboratori non in rete**

Per elaboratori non in rete si intendono quelli non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici.

Essi sono costituiti da:

* numero \_\_\_\_\_\_\_\_ postazioni fisse, dislocate come segue:
* Stanza Avv. \_\_\_\_\_\_\_\_\_;
* Stanza Avv. \_\_\_\_\_\_\_\_\_\_;
* Stanza Avv. \_\_\_\_\_\_\_\_\_, Dott.\_\_\_\_\_\_\_\_\_\_, Dott.ssa \_\_\_\_\_\_\_\_\_\_, collaboratori di studio;
* Postazione segreteria all’ingresso dello studio;

**C – Elaboratori in rete pubblica**

I seguenti PC, pur non risultando connessi in rete con altri, dispongono di collegamento ad Internet:

* Numero \_\_\_\_\_\_\_ PC fissi, dislocati come segue:
* Stanza Avv. \_\_\_\_\_\_\_\_\_\_
* Stanza Avv. \_\_\_\_\_\_\_\_\_\_
* Stanza Avv. \_\_\_\_\_\_\_\_\_, Dott.\_\_\_\_\_\_\_\_\_\_, Dott.ssa \_\_\_\_\_\_\_\_\_
* Postazione SEGRETERIA all’ingresso dello studio (tale postazione risulta inibita alla connessione al server da parte della segretaria)

**2. Mansionario privacy ed interventi formativi degli incaricati**

**Titolari del trattamento** sono gli Avvocati \_\_\_\_\_\_\_\_\_\_\_\_\_ (nato a \_\_\_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_) e \_\_\_\_\_\_\_\_\_\_\_\_ (nato a \_\_\_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_\_\_), i quali non hanno proceduto alla nomina di alcun responsabile del trattamento né di un responsabile protezione dati, dal momento che lo Studio non effettua trattamenti su larga scala.

**Incaricati del trattamento** sono: la Sig.ra \_\_\_\_\_\_\_\_\_\_, nata a \_\_\_\_\_\_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_\_\_\_\_ (in qualità di segretaria assunta con contratto \_\_\_\_\_\_\_\_\_), l’Avv. \_\_\_\_\_\_\_\_\_\_\_\_\_, nata a \_\_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (soggetto che svolge la professione di avvocato sia in proprio che in collaborazione con i titolari), il Dr. \_\_\_\_\_\_\_\_\_\_\_\_, nato a \_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_\_\_\_(praticante), soggetti nominati con atto separato, che però costituisce parte integrante del presente documento e per tale motivo allegato, con specificazione scritta ed analitica dei compiti loro affidati che non siano già eventualmente contemplati dal presente documento.

**Consulente esterno incaricato dell’assistenza e manutenzione degli strumenti elettronici** è il signor \_\_\_\_\_\_\_\_\_\_, nato a \_\_\_\_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_\_\_\_\_.

I dati, così come schematizzati nel paragrafo precedente, sono trattati dai titolari e da tutti gli incaricati **che hanno ricevuto un formale incarico**, mediante specifica designazione scritta.

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, ciò al fine di garantire la sicurezza del trattamento medesimo:

* procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune
* modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
* modalità per elaborare e custodire le *password*, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave
* prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
* procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
* procedure per il salvataggio dei dati
* modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali
* dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Al soggetto incaricato della gestione e manutenzione del sistema informativo viene prescritto di non effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

====================

Le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato e periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, ciò al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

====================

Sono previsti **interventi formativi degli incaricati del trattamento**, finalizzati a renderli edotti dei seguenti aspetti:

* profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l’attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
* rischi che incombono sui dati
* misure disponibili per prevenire eventi dannosi
* modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sonoprogrammati in modo tale da avere luogo al verificarsi di una delle seguenti circostanze:

* già al momento dell’ingresso in servizio
* in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali
* in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all’interno, a cura dei Titolari o di altri soggetti esperti nella materia, che all’esterno, presso soggetti specializzati.

Essi tendono a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle connesse sanzioni penali e disciplinari) che riguardano il trattamento dei dati personali.

Gli interventi formativi pongono altresì come obiettivo la compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l’invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere ai Titolari se un dato possa avere o meno natura sensibile o giudiziaria.

In ogni caso, sono previste riunioni periodiche, in numero di 1 l’anno, per fare il punto sull’evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali.

**3. Analisi dei rischi che incombono sui dati**

E’ stata compiuta l’analisi dei rischi che si può così sintetizzare.

Per i dati comuni del personale dipendente, dei clienti, di terzi, dei fornitori, degli altri professionisti cui lo studio affida incarichi, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione può definirsi medio/basso.

Per i dati sensibili e giudiziari del personale dipendente, dei clienti, di terzi, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione è da definirsi medio/basso, poiché il trattamento avviene esclusivamente all’interno dei locali dello studio.

Il rischio di accesso all’interno dello studio da parte di soggetti non autorizzati può essere definito basso, atteso che l’ingresso nell’orario di apertura è controllato da personale dipendente o da incaricati, e che i locali presentano le caratteristiche illustrate nel paragrafo 1.2.

Il rischio di accesso all’interno delle singole stanze dello studio può essere definito basso, atteso che l’ingresso di terzi estranei avviene solo previa accettazione e controllo.

Il rischio di accesso alle singole postazioni di lavoro da parte di persone non autorizzate può essere definito basso, poiché è controllato l’accesso di terzi allo studio e la zona di attesa è distanziata dalle singole postazioni di lavoro e controllabile dalla segreteria.

Avendo adottato le disposizioni di sicurezza stabilite dal D.lgs. 81/2008 ed essendo presente il dispositivo “salvavita”, il rischio elettrico e di incendi conseguenti può comunque definirsi basso.

Non può tuttavia escludersi che le aree ed i locali potrebbero essere interessati da eventi imprevedibili, quali incendi, allagamenti e corto circuiti, o possa verificarsi la possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici).

Per quanto riguarda gli strumenti elettronici, il rischio di accesso ai dati in essi contenuti può essere definito basso, essendo state adottate le misure di sicurezza volte a ridurre il rischio di perdita e di accesso non autorizzato dei dati.

Non sono consentite duplicazioni di dati per finalità differenti da quelle stabilite per il trattamento.

Per quanto riguarda la documentazione cartacea, il rischio può essere definito basso, essendo gli archivi chiusi a chiave e gli armadi dotati di serrature ed essendo state adottate le altre misure indicate, fatta eccezione ovviamente per gli eventi imprevedibili.

Per quanto concerne i documenti ricevuti a mezzo fax il rischio di accesso non autorizzato alle informazioni in essi contenute è medio - basso, ciò in considerazione del posizionamento della macchina telefax posta in zona protetta da intrusioni di personale non autorizzato.

Per quanto riguarda i supporti di memorizzazione, il rischio di deterioramento dei dati in essi contenuti può essere ritenuto basso, attesi i frequenti back up, ed il fatto che essi sono conservati in armadi dotati di serrature, così come i supporti di installazione dei programmi software adottati, quando lasciati dai fornitori in disponibilità.

Gli elaboratori presenti all’interno dello studio non sono tra loro connessi in rete e risultando ciascuno accessibile unicamente mediante digitazione di password personale, il loro impiego è possibile unicamente da parte dell’utilizzatore della singola postazione di lavoro.

Atteso – infine – che gli incaricati al trattamento dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all’organizzazione dello Studio o di persone che con esso hanno stretti contatti, può essere definito basso.

Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori e disfunzioni da virus, in relazione ai quali sono state applicate da parte dell’incaricato della gestione del sistema informativo opportune ed idonee contromisure, più avanti meglio specificate.

Si dà atto che lo studio non utilizza processi automatizzati, essendo sempre previsto l’intervento umano, ai sensi dell’art. 22 GDPR.

**4. Misure atte a garantire l’integrità e la disponibilità dei dati**

**4.1 La protezione di aree e locali**

I locali in cui sono conservati i dati personali trattati sono accessibili ai soggetti che vi svolgono stabilmente l’attività lavorativa, in particolare - alla data del presente atto - la Sig.ra \_\_\_\_\_\_\_\_\_\_\_\_\_ (che ha mansioni di segretaria), l’Avv. \_\_\_\_\_\_\_\_\_\_ (soggetto che svolge la professione di avvocato sia in proprio che in collaborazione con i titolari) il Dr. \_\_\_\_\_\_\_\_\_\_\_\_ (praticante), la Dott.ssa \_\_\_\_\_\_\_\_\_\_\_ (praticante) tutti soggetti nominati incaricati del trattamento dei dati personali nei termini indicati con atto separato che si allega al presente.

Inoltre, accede occasionalmente ai locali dello Studio anche la Sig.ra \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, custode del Condominio, in occasione di consegne di documentazione postale rilasciata a sue mani.

L’eventuale accesso di terzi (clienti, fornitori, personale che svolge interventi di manutenzione di interni e di impianti elettrici, idraulici, informatici ecc.) avviene sempre durante l’orario di apertura dello Studio e sotto il controllo diretto dei Titolari o di uno degli incaricati.

L’ingresso dei terzi in orari di apertura dello Studio avviene normalmente secondo modalità ed orari concordati preventivamente, la porta d’ingresso non si apre con semplice spinta della stessa, ma esclusivamente dall’interno tramite comando elettrico attivato dalla segretaria; i clienti vengono fatti accomodare nella zona d’attesa o subito ricevuti dai professionisti o dalla segretaria, a seconda del motivo della visita.

La postazione ove è collocata la segreteria consente di controllare e percepire i movimenti delle persone che passano dalla porta di ingresso e di quelle che si trovano in attesa di essere ricevute.

Le misure di sicurezza atte ad impedire l’accesso non autorizzato di estranei all’interno dei locali dello Studio sono state già descritte nel paragrafo 1.2.

La porta interna in legno è tenuta sempre chiusa durante l’orario di apertura dello Studio, e viene aperta unicamente previo azionamento di un comando interno una volta identificato il soggetto entrante, ciò a seguito di riconoscimento vocale avvenuto tramite il citofono posto all’ingresso dell’edificio, ovvero riconoscimento visivo attraverso la vetrata di cui risulta in parte costituita la medesima porta.

Le porte di accesso allo Studio (quella blindata adiacente alle scale interne dell’edificio e quella interna al locale) sono dotate di serrature di sicurezza, le cui chiavi sono possedute solo dai Titolari, dall’Avv. \_\_\_\_\_\_\_\_\_\_\_\_, dai Praticanti, dalla Segretaria e dalla Custode (quest’ultima non è autorizzata a fare ingresso nello Studio al di fuori degli orari di apertura dello stesso).

Le porte di accesso delle stanze delle postazioni di lavoro, gli armadi, i cassetti in cui sono conservati i dati personali, sia quelli trattati su supporto cartaceo che quelli trattati su supporto informatico, sono dotati di serrature.

Il locale destinato all’archivio storico – relativo a pratiche non più in corso - (posto al \_\_\_\_\_\_\_\_\_ piano dell’edificio) risulta chiuso tramite lucchetto e serratura a chiave, le cui copie sono in possesso dei Titolari e della Segretaria.

Tutti gli armadi ed i mobili in cui sono custoditi i dati personali trattati dallo Studio sono dotati di porte o ante munite di serratura con chiave.

Nel caso si presenti l’occasionale necessità di non poter riporre faldoni e carte di lavoro negli armadi e nei cassetti dotati di serrature, le stanze di lavoro nelle quali tali documenti risultano temporaneamente giacenti, vengono chiuse a chiave all’atto dell’allontanamento dalle medesime.

Le chiavi di stanze e contenitori chiusi ai predetti fini vengono idoneamente custodite.

Elaboratori, supporti cartacei e supporti informatici sono conservati sollevati dal pavimento al fine di prevenire possibilità di distruzione o deterioramento in caso di allagamento.

Lo Studio è dotato di più estintori regolarmente controllati, al fine di contrastare inizi di incendi.

Gli impianti ed i sistemi di cui è dotato lo Studio appaiono pertanto soddisfacenti al fine di garantire le opportune misure di sicurezza al trattamento di dati personali da esso svolti.

Per l’anno \_\_\_\_\_\_\_ sono quindi previsti semplici interventi di manutenzione.

**4.2 La custodia e l’archiviazione di atti, documenti e supporti**

Per quanto concerne il reperimento, la custodia e l’archiviazione di atti, documenti e supporti diversi (ad esempio, CD, chiavette, fotografie), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

====================

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi direttamente al titolare.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l’intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all’archivio, al termine di tale ciclo.

====================

Gli incaricati devono **custodire** in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli incaricati sono stati dotati di:

* cassetti con serratura
* armadi chiudibili a chiave

nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. All’interno di tali dispositivi i documenti devono essere riposti anche al termine della giornata di lavoro, qualora l’incaricato debba continuare ad utilizzarli, nei giorni successivi. In caso di particolari esigenze lavorative o di ricerca è consentito lasciare temporaneamente atti e documenti sul tavolo di lavoro durante gli orari di chiusura dello Studio, provvedendo tuttavia a garantire l’idonea chiusura della stanza al momento dell’allontanamento da essa da parte dell’incaricato.

Al termine del trattamento, l’incaricato dovrà restituire all’archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

All’interno dello Studio risultano altresì collocate n. \_\_ casseforti opportunamente nascoste e dotate di apertura a chiave, in possesso dei soli Titolari, al cui interno sono custoditi documenti o supporti contenenti dati personali sensibili o giudiziari di particolare rilievo e pertanto necessitanti di una elevata soglia di sicurezza.

====================

Per quanto concerne **l’archiviazione**, i Titolari hanno adibito apposite aree nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali.

Particolari cautele sono previste per l’archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa deve avvenire in luoghi, armadi, casseforti, o dispositivi equipollenti, che possono essere chiusi.

L’archivio delle pratiche non più in corso è collocato all’interno di un locale – posto al \_\_\_\_\_\_\_\_ piano dell’edificio e la sicurezza dei dati in esse contenuti è garantita mediante l’adozione dei seguenti accorgimenti:

* l’accesso all’archivio è consentito unicamente ai soggetti incaricati al trattamento ai quali viene consegnata la chiave di apertura del locale – locale adibito esclusivamente a tale scopo;
* La chiave di accesso all’archivio è in possesso dei due soggetti Titolari e della Segretaria, in qualità di soggetto incaricato;
* la segretaria ha il compito di procedere settimanalmente ad almeno n. 2 controlli da espletarsi all’interno del locale adibito ad archivio, al fine di verificare la regolare conservazione ed integrità del materiale ivi contenuto;

Dopo l’orario di chiusura dello Studio, l’accesso all’archivio è consentito unicamente ai Titolari.

Si dà atto che i dati non più utilizzati verranno eliminati entro il termine di \_\_\_\_\_\_\_\_\_\_\_\_ anni. In qualunque momento, in conformità agli artt. 16 e 17 Reg., l’interessato potrà chiederne la cancellazione o la rettifica.

====================

Gli impianti e le attrezzature di cui sono dotati i Titolari per la custodia e l’archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari, oggetto di trattamento da parte dello Studio Legale appaiono soddisfacenti al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti.

Per l’anno \_\_\_\_\_\_\_\_\_\_\_ sono quindi previsti semplici interventi di manutenzione.

**4.3 Le misure logiche di sicurezza**

Per i trattamenti effettuati con **strumenti elettronici** (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

4.3.1 - Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici presenti all’interno dello Studio Legale.

Per realizzare le credenziali di autenticazione, si associa un codice per l’identificazione dell’incaricato (username), ad una parola chiave riservata (password), conosciuta solamente dall’incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

Ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

* immediatamente, nel caso in cui l’incaricato perda la qualità, che gli consentiva di accedere allo strumento
* in ogni caso, entro sei mesi di mancato utilizzo, con l’unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Le password sono composte da almeno otto caratteri.

Relativamente al sistema di autenticazione informatica sopra descritto, agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

* obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza
* dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall’amministratore di sistema. Agli incaricati è imposto l’obbligo di provvedere a modificare la password, con la seguente tempistica:
	+ immediatamente, non appena viene consegnata loro da chi amministra il sistema
	+ successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti nell’elaborazione delle password:

* esse non devono contenere riferimenti agevolmente riconducibili all’interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, pippobaudo….)
* buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti allo Studio, siano esse colleghi, segretaria o titolare). Nei casi di prolungata assenza o impedimento dell’incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell’incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

* + scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata
	+ consegnino la busta a chi custodisce le copie delle parole chiave (entrambi i Titolari).

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, uno dei Titolari potrà aprire la busta che il medesimo custodisce. Dell’accesso effettuato si dovrà provvedere ad informare, tempestivamente, l’incaricato cui appartiene la parola chiave.

4.3.2. – Credenziali di autorizzazione

Si fa osservare che non appare necessario prevedere profili di autorizzazione distinti, per le diverse persone, in relazione alle limitate dimensioni della struttura del titolare ed al fatto che tutti gli incaricati trattano i medesimi dati, svolgendo attività di segreteria o, per quanto riguarda i collaboratori avvocati e praticanti avvocati, attività di istruzione e redazione delle pratiche legali.

**4.3.3** - Per quanto riguarda la **protezione di strumenti e dati** da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto (applicazione di **antivirus**, *marca, caratteristiche e configurazione di installazione*) riguarda la **protezione dei dati personali dal rischio di intrusione e dall’azione di programmi di cui all’articolo 615-quinquies del codice penale**, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l’interruzione, totale o parziale, o l’alterazione del suo funzionamento (comunemente conosciuti come virus).

A tale fine, si è dotati di idonei strumenti elettronici e programmi, che dovrebbero essere aggiornati, di regola:

* ogni \_\_\_\_\_ giorni / mesi nel caso di strumenti elettronici in rete pubblica
* ogni \_\_\_\_\_ giorni / mesi nel caso di strumenti elettronici che non sono in rete.

Tutti gli incaricati sono stati istruiti, in merito all’utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

Il secondo aspetto (applicazione di **firewall**, *marca, caratteristiche e configurazione di installazione*) riguarda la **protezione degli elaboratori dall’accesso abusivo, di cui all’articolo 615-ter del codice penale**, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l’impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, obbligatori nei casi in cui si trattino dati sensibili o giudiziari.

A tale riguardo la nostra organizzazione si è da tempo dotata di tali strumenti, per la protezione degli elaboratori

**4.3.4. -** Per quanto concerne i **supporti rimovibili** (es. chiavette, CD, DVD….), contenenti dati personali, la norma impone particolari cautele solo nell’ipotesi in cui essi contengano dati sensibili o giudiziari.

La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

* i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
* una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati.

Per l’anno \_\_\_\_\_\_\_\_, sono quindi previsti semplicemente interventi finalizzati all’aggiornamento e alla manutenzione.

**5. Criteri e modalità di ripristino dei dati**

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

Per i dati trattati con strumenti elettronici, sono previste procedure di **backup**, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni (CD, backup online…..).

Il salvataggio dei dati trattati avviene come segue:

* la frequenza dell’operazione è settimanale;
* si utilizzano supporti differenti da quelli in cui sono contenuti i dati dei salvataggi eseguiti la volta precedente;
* per ciascun salvataggio, si esegue 1 copia*.*

Le copie vengono custodite:

* presso l’abitazione di uno dei Titolari all’interno di una cassaforte.

Nell’ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici, l’incaricata Sig.ra \_\_\_\_\_\_ deve:

* avvertire i Titolari del trattamento dei dati e recuperare i supporti di back up nonché quelli contenenti i vari software dello studio installati sugli strumenti elettronici;
* rivolgersi immediatamente e chiedere l’intervento del tecnico manutentore dello Studio, Sig. \_\_\_\_\_\_\_\_\_ (tel. \_\_\_\_\_\_\_\_\_\_\_\_), sollecitandone al più presto l’assistenza;
* con l’ausilio del consulente informatico, reinstallati i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l’intero hardware, provvedere a reinstallare tutti i dati contenuti nei supporti di back up;
* con l’ausilio del consulente informatico, provvedere all’aggiornamento dei sistemi operativi una volta reinstallati;
* verrà dato incarico al tecnico manutentore di suggerire ogni altra misura;
* in ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;

Al fine di evitare la perdita ed il danneggiamento degli strumenti elettronici e dei dati in essi contenuti, è effettuata l’ordinaria manutenzione dei sistemi elettronici dal tecnico incaricato.

In caso di assenza della Sig.ra \_\_\_\_\_\_\_\_, le predette operazioni saranno svolte a cura di altro incaricato al trattamento presente in Studio.

|  |  |
| --- | --- |
| Ai sensi dell’art. 33 GDPR, nel caso in cui vi sia una violazione dei dati personali, il titolare del trattamento, senza indugi – e in ogni caso entro 72 ore - notificherà la violazione all’autorità di controllo competente a norma dell’art. 55.  |  |

**6. L’affidamento di dati personali all’esterno**

Nei casi in cui i trattamenti di dati personali vengano affidati all’esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime.

Per la generalità dei casi in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all’esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali.

Ai sensi dell’art. 45 GDPR il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

Qualora il trasferimento avvenga verso soggetti non considerati sicuri per il trattamento dei dati personali, si stipulano con il destinatario clausole contrattuali conformi ovvero si forniscono, in ogni caso, garanzie adeguate.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

**7. Controllo generale sullo stato della sicurezza**

Ai Titolari è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l’efficacia delle misure di sicurezza adottate, i Titolari, con l’ausilio del consulente informatico, provvedono con frequenza semestrale, anche tramite controlli a campione, ad effettuare una o più delle seguenti attività:

* + verificare l’accesso fisico ai locali dove si svolge il trattamento
	+ verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
	+ monitorare l’efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici
	+ verificare l’integrità dei dati e delle loro copie di backup
	+ verificare la sicurezza delle trasmissioni in rete
	+ verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
	+ verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l’accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati nell’arco del semestre di riferimento.

##### 8. Considerazioni conclusive e conseguenze applicative

Il presente documento scaturisce dall’analisi dei problemi conseguenti all’entrata in vigore del Regolamento UE 679/2016 citato in premessa.

In esecuzione di ciò si è provveduto con atto separato (che costituisce parte integrante del presente documento e per tale motivo anche a questo allegato), redatto a cura dei Titolari Sigg.ri Avvocati \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, all’individuazione e nomina dei soggetti incaricati del trattamento dei dati personali ed alla specificazione scritta ed analitica dei compiti loro affidati ed i termini dell’autorizzazione al trattamento dei dati comuni, sensibili e giudiziari che non siano già contemplati dal presente documento.

Ai destinatari delle comunicazioni precedenti è allegata anche copia datata e firmata in originale del presente documento, perché funga da istruzione circa i compiti e le norme da osservare nell’ambito dell’attività svolta presso lo Studio.

Le nomine, le comunicazioni, l’autorizzazione, unitamente al presente documento che viene allegato, sono consegnate ai destinatari che sottoscrivono per ricevuta.

Il presente documento viene sottoscritto dai Titolari e conservato in originale presso lo Studio, unitamente alle nomine con istruzioni firmate per accettazione dai destinatari.

Ad esso saranno uniti i documenti che in futuro costituiranno integrazione ed aggiornamento del presente atto, necessari per adeguarsi a successive disposizioni di leggi o regolamenti, ovvero a diversa organizzazione dello Studio per la parte che attiene all’organigramma, ai locali ed agli strumenti informatici o comunque automatizzati.

**9. Dichiarazioni d’impegno e firma**

Il presente documento, redatto nel \_\_\_\_\_\_\_\_\_\_\_\_\_, viene firmato in calce da:

* Avv. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ in qualità di Titolare
* Avv. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in qualità di Titolare

L’originale del presente documento viene custodito presso lo Studio, per essere esibito in caso di controlli.

Una sua copia verrà consegnata:

* ai responsabili esterni del trattamento dei dati personali
* a chiunque ne faccia richiesta, in relazione all’instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

*Torino, lì \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*I Titolari.*

*Avv. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Avv. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*