ORDINE
DEGLI AVVOCATI
DI NAPOLI NORD

La Protezione dei dati personali nello svolgimento della professione di avvocato

Vademecum realizzato a supporto degli Avvocati

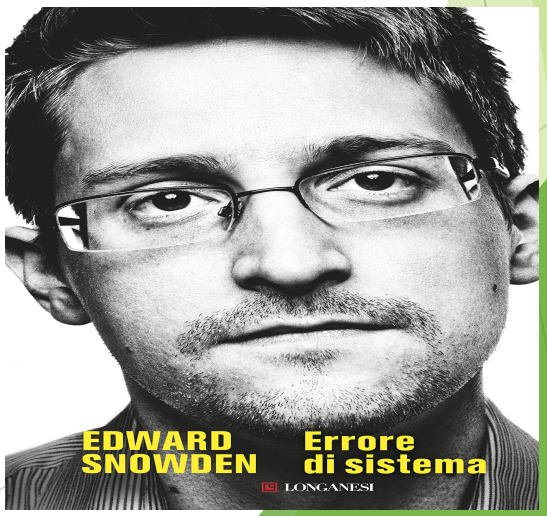
Consiglio dell'Ordine di Napoli Nord

COMMISSIONE PRIVACY
Consiglio dell'ordine degli Avvocati di Napoli Nord

VADEMECUM PRIVACY PER GLI AVVOCATI

"Affermare che non si è interessati al diritto alla privacy perché non si ha nulla da nascondere è come dire che non si è interessati alla libertà di parola perché non si ha nulla da dire."

***Edward Joseph Snowden** (1983 – vivente), attivista e informatico statunitense.*
(in foto, nella copertina del celebre libro «Errore di sistema»)



Il presente Vademecum contiene la descrizione dei ruoli e degli adempimenti relativamente alle procedure e misure di sicurezza tecniche e organizzative da adottare all'interno degli Studi legali, alla luce delle disposizioni del Regolamento Europeo n. 679/2016 (General Data Protection Regulation – GDPR), del D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), dei provvedimenti dell'Autorità Garante per la protezione dei dati personali e del Comitato Europeo per la Protezione dei Dati.

Il Vademecum è a cura dell'Avv. Gianluca Pirozzi, DPO dell'Ordine degli Avvocati di Napoli Nord e dell'Avv. Luca Visconti, CEO di HEU

Hanno collaborato alla stesura del presente Vademecum i componenti della Commissione Privacy del Consiglio dell'Ordine degli Avvocati di Napoli Nord: Avv. Capasso Sabrina, Avv. Cimmino Rosanna, Avv. Pennacchio Roberto, Avv. Iovinella Camilla, Avv. De Prete Antonietta, Avv. Del Prete Francesca.

INDICE

- *Le Fonti*
- *Deontologia forense e regole deontologiche*
- *Ambito di applicazione*
- *Il ruolo dell'Avvocato*
- *Definizione ruoli interni ed esterni*
- *Gestione misure tecniche di sicurezza informatica*
- *Adozione processi organizzativi*
- *Predisposizione formazione delle persone autorizzate*
- *Sistema sanzionatorio – Sanzioni amministrative e penali*

LE FONTI

In riferimento al trattamento dei dati personali, gli avvocati, i praticanti avvocati, avvocati stranieri esercenti legalmente la professione sul territorio dello Stato e gli investigatori privati, devono rispettare

- **Regolamento UE 2016/679** (**«GDPR»**), applicato dal 25 maggio 2018
- **D.lgs. 196/2003** (**«Codice Privacy»**) con recepimento anche di altre Direttive (es. **Direttiva 2002/58/CE** cd. e-Privacy)
- **D.lgs. 101/2018** (**«Decreto»**) Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR
- **Regole deontologiche («Allegato 1»)** relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria (19 dicembre 2018)
- **Codice Deontologico Forense** approvato dal Consiglio Nazionale Forense nell'anno 2014
- **Norme secondarie generali ed astratte** del Garante per la Protezione dei Dati Personali e del Comitato Europeo per la Protezione dei Dati

La Deontologia Forense e regole deontologiche

Art. 13 – **Dovere di segretezza e riservatezza** L'avvocato è tenuto, nell'interesse del cliente e della parte assistita, alla rigorosa osservanza del segreto professionale e al massimo riserbo su fatti e circostanze in qualsiasi modo apprese nell'attività di rappresentanza e assistenza in giudizio, nonché nello svolgimento dell'attività di consulenza legale e di assistenza stragiudiziale e comunque per ragioni professionali.

Art. 28 – **Riserbo e segreto professionale** 1. È dovere, oltre che diritto, primario e fondamentale dell'avvocato mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni che gli siano fornite dal cliente e dalla parte assistita, nonché su quelle delle quali sia venuto a conoscenza in dipendenza del mandato. 2. L'obbligo del segreto va osservato anche quando il mandato sia stato adempiuto, comunque concluso, rinunciato o non accettato. 3. **L'avvocato deve adoperarsi affinché il rispetto del segreto professionale e del massimo riserbo sia osservato anche da dipendenti, praticanti, consulenti e collaboratori, anche occasionali, in relazione a fatti e circostanze apprese nella loro qualità o per effetto dell'attività svolta.** 4. È consentito all'avvocato derogare ai doveri di cui sopra qualora la divulgazione di quanto appreso sia necessaria: a) per lo svolgimento dell'attività di difesa; b) per impedire la commissione di un reato di particolare gravità; c) per allegare circostanze di fatto in una controversia tra avvocato e cliente o parte assistita; d) nell'ambito di una procedura disciplinare. In ogni caso la divulgazione dovrà essere limitata a quanto strettamente necessario per il fine tutelato. 5. La violazione dei doveri di cui ai commi precedenti comporta l'applicazione della sanzione disciplinare della censura e, nei casi in cui la violazione attenga al segreto professionale, l'applicazione della sospensione dall'esercizio dell'attività professionale da uno a tre anni

Art. 18 – **Doveri nei rapporti con gli organi di informazione** 1. Nei rapporti con gli organi di informazione l'avvocato deve ispirarsi a criteri di equilibrio e misura, nel rispetto dei doveri di discrezione e riservatezza; con il consenso della parte assistita, e nell'esclusivo interesse di quest'ultima, può fornire agli organi di informazione notizie purché non coperte dal segreto di indagine.
2. L'avvocato è tenuto in ogni caso ad assicurare l'anonimato dei minori.

Regole deontologiche
Art. 5. Comunicazione e diffusione di dati
1. Nei rapporti con i terzi e con la stampa possono essere rilasciate informazioni non coperte da segreto qualora sia necessario per finalità di tutela dell'assistito, ancorché non concordato con l'assistito medesimo, nel rispetto dei principi di liceità, trasparenza, correttezza, e minimizzazione dei dati di cui al Regolamento (UE) 2016/679 (art. 5), nonché dei diritti e della dignità dell'interessato e di terzi, di eventuali divieti di legge e del codice deontologico forense.

AMBITO DI APPLICAZIONE

ART. 2 GDPR - AMBITO DI APPLICAZIONE MATERIALE

- Il Regolamento UE 679/16 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

ART. 1 REGOLE DEONTOLOGICHE - AMBITO DI APPLICAZIONE

- Le regole deontologiche devono essere rispettate nel trattamento di dati personali per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sia nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla sua definizione

Nelle attività «quotidiane» svolte da ogni avvocato sono riscontrabili

- Operazioni di trattamento di dati personali di persone fisiche
- Trattamento interamente o parzialmente automatizzato di dati personali
- Trattamento non automatizzato di dati personali contenuti in un archivio o destinato a figurarvi
- Trattamento effettuato per far valere un diritto in giudizio
- Per ogni tipo di procedimento giudiziale o stragiudiziale (es. in sede amministrativa, di arbitrato o di conciliazione)

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»

BASE GIURIDICA (LICEITA' DEL TRATTAMENTO)

- Art. 6 lett b) GDPR

Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dell'interessato (es. MANDATO, NOMINA DIFENSORE, PROCURA)

- Art. 9 lett. f) GDPR

Il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziario.

IL RUOLO DELL'AVVOCATO

Chi è il 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

Nell'ambito dell'attività professionale svolta, ricoprono il ruolo di titolare del trattamento le seguenti figure

a) Avvocato;
b) Praticante avvocato
c) Avvocato straniero
d) una pluralità di professionisti, codifensori della medesima parte assistita, consulenti o domiciliatari;
e) un'associazione tra professionisti o una società di professionisti.
f) Investigatori privati
g) Liberi professionisti che svolgono attività di assistenza o consulenza per finalità «giudiziarie»

(Consulenti Domiciliatari Sostituti processuali) si applica il comma 5 lett. c) dell'art. 14 del GDPR (Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato)

Il Titolare del trattamento non è tenuto a dare le informazioni qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale (es. Codice di deontologia professionale)

L'avvocato (o le altre figure menzionate, qualora ricoprano il ruolo di titolare del trattamento) organizza il trattamento anche non automatizzato dei dati personali secondo le modalità che risultino più adeguate, caso per caso, a favorire in concreto l'effettivo rispetto dei diritti, delle libertà e della dignità degli interessati, applicando i principi di finalità, proporzionalità e minimizzazione dei dati sulla base di un'attenta valutazione sostanziale e non formalistica delle garanzie previste, nonchè di un'analisi della quantità e qualità delle informazioni che utilizza e dei possibili rischi.

PRINCIPIO DI ACCOUNTABILITY
Essere in grado di dimostrare il rispetto dei principi previsti dal GDPR

PRINCIPI APPLICABILI AL TRATTAMENTO

- Liceità, correttezza e trasparenza
- Limitazione della finalità (determinate, esplicite e legittime)
- Pertinenza ed adeguatezza (raccogliere solo dati funzionali al perseguimento delle finalita')
- Esattezza, (se necessario, aggiornare i dati)
- Limitazione della conservazione
- Integrità e riservatezza

L’Avvocato deve:

IL TITOLARE DEL TRATTAMENTO

- **Definire ruoli interni ed esterni**
- **Gestire misure tecniche di sicurezza informatica**
- **Adottare processi organizzativi**
- **Predisporre la formazione del personale**

- Nominare persone autorizzate
- Nominare DPO, ove applicabile
- Nominare Responsabile del trattamento (esterno), ove applicabile

- Aggiornamento Software e Reti
- Cifratura dati
- Sistemi Cloud e sistemi di Backup
- Policy utilizzo strumenti informatici
- Policy posta elettronica
- Strong Authentication

- Redazione Informative
- Registro dei trattamenti
- Valutazione dei rischi
- DPIA (ove applicabile)
- Policy Data Breach
- Registro Data Breach
- Policy Diritti degli interessati
- Data retention (Periodo di conservazione)

- Corsi di Formazione
- Test di valutazione

DEFINIZIONE RUOLI INTERNI ED ESTERNI

ISTRUZIONI PERSONE AUTORIZZATE

Secondo l'art. 29 del GDPR e dell'art. 2-quaterdecies del Codice Privacy, chiunque agisce sotto l'autorità del titolare del trattamento ed abbia accesso ai dati personali, non può trattare tali dati se non è istruito. Pertanto l'Avvocato, in qualità di titolare del trattamento, nell'ambito del proprio assetto organizzativo, può prevedere che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche che operano sotto la sua autorità

Nel quadro delle adeguate istruzioni da impartire per iscritto alle persone autorizzate ad al trattamento dei dati, sono formulate concrete indicazioni in ordine alle modalità che tali soggetti devono osservare, a seconda del loro ruolo.

Chi sono?

- Persona addetta a compiti di collaborazione amministrativa
- Sostituto processuale
- Praticante avvocato con o senza abilitazione al patrocinio
- Tirocinante
- Stagista
- Consulente di parte
- Perito
- Investigatore privato
- altro ausiliario che non rivesta la qualità di autonomo titolare del trattamento

Nell’ambito delle istruzioni da fornire alle persone autorizzate deve essere prestata **specifica attenzione** all’adozione di idonee cautele per prevenire l’ingiustificata raccolta, utilizzazione o conoscenza di dati in caso di:

a) acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati;
b) scambio di corrispondenza, specie per via telematica;
c) esercizio contiguo di attività autonome all'interno di uno studio;
d) utilizzo di dati di cui è dubbio l'impiego lecito, anche per effetto del ricorso a tecniche invasive;
e) utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti (tabulati di flussi telefonici e informatici, consulenze tecniche e perizie, relazioni redatte da investigatori privati);
f) custodia di materiale documentato, ma non utilizzato in un procedimento e ricerche su banche dati a uso interno, specie se consultabili anche telematicamente da uffici dello stesso titolare del trattamento situati altrove;
g) acquisizione di dati e documenti da terzi, verificando che si abbia titolo per ottenerli;
h) conservazione di atti relativi ad affari definiti.

Nell’ambito delle attività dello studio legale tutti devono essere a conoscenza che sono utilizzati lecitamente e secondo correttezza secondo i medesimi principi di cui all’art. 5 del Regolamento (UE) 2016/679:

a) i dati personali contenuti in pubblici registri, elenchi, albi, atti o documenti conoscibili da chiunque, nonché in banche di dati, archivi ed elenchi, ivi compresi gli atti dello stato civile, dai quali possono essere estratte lecitamente informazioni personali riportate in certificazioni e attestazioni utilizzabili a fini difensivi;

b) atti, annotazioni, dichiarazioni e informazioni acquisite nell'ambito di indagini difensive, in particolare ai sensi degli articoli 391-bis, 391-ter e 391-quater del codice di procedura penale, evitando l'ingiustificato rilascio di copie eventualmente richieste. Se per effetto di un conferimento accidentale, anche in sede di acquisizione di dichiarazioni e informazioni ai sensi dei medesimi articoli 391-bis, 391-ter e 391-quater, sono raccolti dati eccedenti e non pertinenti rispetto alle finalità difensive, tali dati, qualora non possano essere estrapolati o distrutti, formano un unico contesto, unitariamente agli altri dati raccolti.

Chi è il 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".
Il responsabile, in sostanza, effettua il trattamento in quanto i dati personali gli sono comunicati dal titolare del trattamento.
In pratica, è la persona che tratta dati personali per conto dello studio legale come un contabile, un editore di software, un host web, ecc.
Il responsabile è da considerarsi solo "esterno" allo studio legale. I soggetti a cui lo studio comunica i dati personali trattati in qualità di responsabili del trattamento dovranno essere affidabili e rispettare la normativa relativa alla protezione dei dati personali (es.: commercialista, consulente del lavoro, consulente, fornitori di servizi digitali, conservatori di documenti informatici, ecc.).

Il responsabile non può trattare i dati personali se non è istruito in tal senso dal titolare del trattamento. Le istruzioni potranno essere indicate attraverso l'accordo previsto dall'art. 28 del GDPR

In alcuni casi l'avvocato, nelle vesti di consulente, deve essere nominato responsabile del trattamento. (es. Credit collection, Due diligence)

Chi è il D.P.O.?

Il DPO ai sensi degli artt. 37, 38, 39 del Regolamento UE 679/2016

- **Nella maggior parte dei casi gli avvocati, singoli o associati, non devono nominare un DPO. Per realtà molto grandi l'opportunità di valutare o meno di nominare un DPO deve essere effettuata caso per caso.**

- **L'avvocato può essere nominato DPO. Tale circostanza rappresenta una nuova opportunità lavorativa e professionale, qualora si acquisiscano le competenze necessarie e nel rispetto dei requisiti richiesti dalla normativa.**

GESTIONE MISURE TECNICHE DI SICUREZZA INFORMATICA

SISTEMI SOFTWARE E RETI

E' **molto importante** per la sicurezza informatica dello Studio, **aggiornare i software**.
I programmi, spesso, presentano dei c.d. BUG, cioè errori nel codice di programmazione. Gli hacker o i virus sfruttano queste vulnerabilità per sottrarre informazioni o bloccare i sistemi.

Cosa Fare?

- Installare ed aggiornare periodicamente un antivirus su ogni PC
- Aggiornare periodicamente il sistema operativo dei PC
- Effettuare una scansione antivirus sui pc almeno una volta al mese
- Attivare ed aggiornare il firewall per per impedire l'entrata o l'uscita di connessioni pericolose per il sistema
- Non accedere a reti Wi-Fi poco sicure
- Utilizzare una VPN (virtual private network)

Sicurezza del Trattamento

Il Titolare del trattamento, tenendo conto dello state dell'arte e dei costi di attuazione deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.
Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali tramessi, conservati o comunque trattati.

Cosa fare?

- Pseudonimizzazione e cifratura dei dati personali, in particolare delle categorie particolari di dati o relativi a condanne penali o reati
- Assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienze dei sistemi dei servizi di trattamento
- Ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico e tecnico
- Adottare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Cloud Computing

Erogazione di servizi da parte di un provider attraverso la rete e resi disponibili su server da remoto, per gestione e conservazione dei dati personali

- Sistemi di autenticazione a due fattori
- Service provider affidabile
- Dati crittografati

Backup (Disaster Recovery)

Messa in sicurezza delle informazioni di un sistema informatico attraverso la creazione di più copie di riserva dei dati, da utilizzare come recupero (ripristino) dei dati stessi in caso di eventi malevoli accidentali o intenzionali o semplice manutenzione del sistema

Strong Authentication

Metodo di autenticazione elettronica in cui a un utente di computer viene concesso l'accesso a un sito Web o a un'applicazione solo dopo aver presentato con successo due o più elementi di prova a un meccanismo di autenticazione

- Password complesse – modifica ogni 3 mesi
- Non condividere password
- Token

Policy utilizzo strumenti informatici (posta elettronica)

Viene adottata al fine di prevenire comportamenti, anche inconsapevoli, che possano creare problemi alla sicurezza nel trattamento dei dati personali e a disciplinare le condizioni e le modalità del corretto utilizzo delle risorse informatiche messe a disposizione dal Titolare del trattamento alle persone autorizzate. Si applica a tutte le persone autorizzate, senza distinzione di ruolo e/o livello, a prescindere dal rapporto contrattuale intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.), che per l'espletamento delle proprie mansioni, utilizza strumenti informatici e di telecomunicazioni, o comunque, accede alle banche dati di proprietà del Titolare del trattamento.

- Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

- Ogni Utente è tenuto a adottare comportamenti idonei a prevenire il rischio di accessi non autorizzati che abbiano come mezzo o scopo le risorse informatiche.

Rientrano nel campo di applicazione delle policy, l'utilizzo dei pc, l'utilizzo di internet, l'utilizzo della posta elettronica, l'utilizzo di dispositivi mobili (cellulari e router wifi), etc., che essendo strumenti di lavoro, devono essere utilizzati funzionalmente alle mansioni svolte e/o agli incarichi affidati.

- REGOLE UTILIZZO PC AZIENDALI
- REGOLE UTILIZZO PC PORTATILI
- REGOLE UTILIZZO SUPPORTI RIMOVIBILI
- REGOLE UTILIZZO DISPOSITIVI MOBILI (cd. BYOD)
- REGOLE UTILIZZO DELLE PASSWORD
- REGOLE UTILIZZO DI INTERNET
- **REGOLE UTILIZZO POSTA ELETTRONICA**

La casella di posta elettronica, assegnata dal Titolare del trattamento alla persona autorizzata, è uno strumento di lavoro.
Le persone assegnatarie della casella di posta elettronica sono responsabili del corretto utilizzo delle stesse e in caso di ricezione di messaggi insoliti o che possano palesemente nuocere la sicurezza dei sistemi informativi, per non correre il rischio di essere colpiti da virus, non devono aprire gli stessi.

La policy deve rispettare le Linee guida dell'Autorità Italiana per la protezione dei dati personali per posta elettronica e internet pubblicate sul Registro delle deliberazioni n. 13 del 1° marzo 2007

Adozione processi organizzativi

INFORMAZIONI DA FORNIRE AI CLIENTI

Nell'ambito dell'esercizio della professione di avvocato, il trattamento dei dati personali del cliente riguarda tutti i dati necessari per la formazione del fascicolo del cliente e per la difesa dei suoi interessi: (Dati comuni – Categorie Particolari di dati – Dati relativi a condanne penali e reati)

L'avvocato può fornire in un unico contesto, anche mediante affissione nei locali dello Studio e, se ne dispone, pubblicazione sul proprio sito Internet, anche utilizzando formule sintetiche e colloquiali, l'informativa sul trattamento dei dati personali (art. 13 del Regolamento) e le notizie che deve indicare ai sensi della disciplina sulle indagini difensive.
Le informazioni di cui all'art. 13 del GDPR devono essere rese anche al personale interno (persone autorizzate)

ART. 13 GDPR
-IDENTITA' E DATI DI CONTATTO TITOLARE (ANCHE DPO SE NOMINATO)
-FINALITA' E BASE GIURIDICA DEL TRATTAMENTO
-DESTINATARI
-TRASFERIMENTO DATI A UN PAESE TERZO
-PERIODO DI CONSERVAZIONE
-DIRITTI DELL'INTERESSATO
-DIRITTO DI PROPORRE RECLAMO AL GARANTE
-CONSEGUENZA DELLA MANCATA COMUNICAZIONE DEI DATI
-ESISTENZA DI UN PROCESSO AUTOMATIZZATO COMPRESA LA PROFILAZIONE

PERIODO DI CONSERVAZIONE E CANCELLAZIONE DEI DATI

- Rispetto art. 5 lett e) del GDPR – Limitazione della conservazione
- Restituzione al cliente dell'originale degli atti da questi ricevuti
- Previa comunicazione alla parte assistita, è possibile la distruzione, cancellazione o consegna all'avente diritto o ai suoi eredi o aventi causa, della documentazione integrale dei fascicoli degli affari trattati e le relative copie

Estinto il procedimento o il relativo rapporto di mandato l'avvocato può conservare, in originale o in copia e anche in formato elettronico, gli atti e documenti attinenti all'oggetto della difesa,

- qualora risulti necessario in relazione a ipotizzabili altre esigenze difensive della parte assistita o del titolare del trattamento
- Per utilizzazione in forma anonima per finalità scientifiche
- Adempimento obbligo normativo in materia fiscale, antiriciclaggio, contrasto alla criminalità

- In caso di revoca o di rinuncia al mandato fiduciario o del patrocinio, la documentazione acquisita deve essere rimessa, in originale ove detenuta in tale forma, al difensore che subentra formalmente nella difesa.

- In caso di cessazione anche per sopravvenuta incapacità e qualora manchi un altro difensore anche succeduto nella difesa o nella cura dell'affare, la documentazione dei fascicoli degli affari trattati, decorso un congruo termine dalla comunicazione all'assistito, deve essere consegnata al Consiglio dell'ordine di appartenenza ai fini della conservazione per finalità difensive.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Si tratta di uno strumento fondamentale non soltanto ai fini dell´eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all´interno di un´azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. Il registro consente di mappare più chiaramente i trattamenti e di monitorare gli stessi ai fini del rispetto dei principi del GDPR e dei diritti degli interessati, oltre a contribuire all'esatto adempimento del principio dell'accountability.

Il Registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile. In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

RACCOMANDA

Liberi professionisti con almeno un dipendente e/o che trattano dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale)

MODELLO REGISTRO DEI TRATTAMENTI SEMPLIFICATO PREDISPOSTA DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*							
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*							
TIPOLOGIA DI TRATTAMENTO	**FINALITA' E BASI LEGALI DEL TRATTAMENTO**	**CATEGORIE DI INTERESSATI**	**CATEGORIE DI DATI PERSONALI**	**CATEGORIE DI DESTINATARI** *[Indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[Indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**TERMINI ULTIMI DI CANCELLAZIONE PREVISTI**	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

VALUTAZIONE DEI RISCHI E DPIA

RISK ASSESSMENT

Al fine di implementare le azioni volte al rispetto del principio di Accountability, il Titolare deve effettuare una ricognizione dell'attuale organizzazione e della documentazione vigente in materia di privacy e misure tecniche utilizzate. Si consiglia l'utilizzo di un questionario finalizzato all'identificazione dei principali rischi di non conformità al GDPR, interni ed esterni, alla propria organizzazione

Fattori di rischio e misure da garantire

- Assicurarsi che le procedure siano complete e formalizzate;
- Adeguare i controlli e relativa tracciabilità;
- Assicurassi che siano definite le responsabilità organizzative;
- la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito degli strumenti elettronici;
- dispositivi antincendio previsti dalla normativa vigente;
- gruppo di continuità dell'alimentazione elettrica;
- impianto di condizionamento;
- Valutazione periodica delle misure tecniche adottate e vulnerabilità della rete e dei sistemi;
- Corretta applicazione delle regole sull'utilizzo degli strumenti informatici;
- Tenere conto dell'eventuale impatto legale, economico e reputazionale di un Data Breach;

Utile l'utilizzo delle regole previste dalla norma ISO 27001 La sicurezza delle Informazioni

Nel caso in cui un trattamento possa comportare un rischio elevato, come accade nel caso di introduzione di nuove tecnologie, per i diritti e le libertà delle persone interessate, il GDPR obbliga il Titolare a svolgere una valutazione di impatto prima di darvi inizio.
Qualora residui un rischio elevato per i diritti e le libertà degli interessati, nonostante il Titolare abbia individuato le misure tecniche ed organizzative per attenuarlo, sarà necessario consultare l'autorità Garante Privacy

Casi in cui il trattamento può presentare un rischio

- Trattamenti valutativi o di scoring, compresa la profilazione;
- Decisioni automatizzate che producono significativi effetti giuridici (es. assunzioni, concessioni prestiti, stipula di assunzioni);
- Monitoraggio sistematico (es. videosorveglianza);
- Trattamento di dati appartenenti a categorie particolari o relativi a condanne penali o reati;
- Dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, anziani, richiedenti asilo, ecc.);
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. riconoscimento facciale, device IoT, ecc.).

Linee Guida WP248 DPIA - Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto" dell'11.10.2018 pubblicate dal Garante per la Protezione dei dati personali

POLICY GESTIONE ESERCIZIO DEI DIRITTI

La presente Procedura si applica alle richieste degli Interessati, avanzate ai sensi degli articoli 15 - 22 del GDPR, riguardanti i dati personali trattati, raccolti e/o conservati dal Titolare del trattamento. **Si applica alla gestione di tutte le diverse categorie di Interessati con cui il titolare si interfaccia, vale a dire dipendenti, collaboratori, stagisti, clienti, utenti web, visitatori, fornitori, etc.**

TEMPI

Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.

Scheda di sintesi a mero scopo divulgativo. Per un quadro completo della materia, si rimanda alla legislazione in tema di protezione dei dati personali e ai provvedimenti dell'Autorità.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Conosci i principali diritti previsti dal Regolamento (UE) 2016/679?

Il Regolamento (articoli 15-22) riconosce importanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.).

Accesso ai propri dati personali

Hai il diritto di sapere se è in corso un trattamento di dati personali che ti riguardano e - se confermato - di ottenere una copia di tali dati ed essere informato su: l'origine dei dati; i destinatari dei dati; le finalità del trattamento; l'esistenza di un processo decisionale automatizzato, compresa la profilazione; il periodo di conservazione dei dati; i diritti previsti dal Regolamento.

Rettifica, cancellazione, limitazione del trattamento, portabilità dei dati personali

Puoi chiedere - nei casi previsti dal Regolamento - che i dati personali a te riferiti siano rettificati o cancellati, o che ne venga limitato il trattamento. Puoi inoltre chiedere che i dati che tu hai fornito al titolare siano trasferiti ad un altro titolare («diritto alla portabilità»), nel caso in cui il trattamento si basi sul tuo consenso o su un contratto con te stipulato e venga effettuato con mezzi automatizzati .

Opposizione al trattamento

Puoi opporti al trattamento dei tuoi dati personali per motivi connessi alla tua situazione particolare, da specificare nella richiesta; oppure senza necessità di motivare l'opposizione, quando i tuoi dati sono trattati per finalità di marketing diretto.

Come si esercitano questi diritti?

Puoi presentare, gratuitamente e senza particolari formalità (per esempio, tramite posta elettronica, posta raccomandata, ecc.), una richiesta di esercizio dei diritti al titolare del trattamento (sul sito www.garanteprivacy.it è disponibile un modulo facsimile) . Il titolare del trattamento è tenuto entro 1 mese a rispondere alla richiesta, o a comunicare un eventuale ritardo nella risposta in caso di richieste numerose e/o complesse (la proroga non può comunque superare i 2 mesi). Se la risposta non perviene nei tempi indicati o non la ritieni soddisfacente, puoi rivolgerti al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria.

Scopri di più su: www.garanteprivacy.it/home/diritti

POLICY GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

ART. 4 n. 12 del GDPR

«violazione dei dati personali»: 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

QUINDI?

Attacchi informatici, accessi abusivi, incidenti o eventi avversi (come incendi o altre calamità) che possono causare la **perdita, la distruzione o la diffusione indebita di dati personali trattati** dall'operatore. Il Regolamento 2016/679 (GDPR) introduce nuove prescrizioni che in parte superano quelle preesistenti del Garante italiano. Il Regolamento prevede che nel caso in cui si verifichi un data breach è necessario provvedere ad una **notifica al Garante entro 72 ore** dalla scoperta dell'evento.

I Dati Personali violati possono includere qualsiasi tipologia di informazione, dai dati c.d. ordinari (come ad esempio, dati anagrafici, numeri di telefono, indirizzi e-mail), a Categorie Particolari di Dati Personali (come ad esempio, i dati sanitari)

Redazione piano preventivo Data Breach

«Un attacco informatico, una perdita, una manomissione o un accesso abusivo che compromettano i dati personali trattati»

NOTIFICA

Al Garante entro 72 ore dalla scoperta dell'evento

COMPETENZA

Il Garante dello Stato membro in cui sorge lo stabilimento del titolare o i cui interessati sono riguardati dalla violazione

CONTENUTI

Violazione
Numero degli interessati
Contatti interni (in particolare del DPO, ove presente)
Stima delle conseguenze

COMUNICAZIONE ALL'INTERESSATO

Se sono a rischio i diritti e le libertà degli interessati
Natura della violazione con linguaggio semplice
Conseguenza delle violazioni
Nome e recapiti del DPO, ove presente
Misure adottate per affrontare la violazione

TENERE REGISTRO DEI DATA BREACH PER DOCUMENTARE OGNI TIPO DI VIOLAZIONE ANCHE NEL CASO IN CUI NON E' NECESSARIO EFFETTUARE LA COMUNICAZIONE AL GARANTE.

PREDISPOSZIONE FORMAZIONE DELLE PERSONE AUTORIZZATE

Formazione del personale

COSA FARE?

Occorre considerare che i dipendenti e i collaboratori dello studio legale, in qualità di autorizzati al trattamento ai sensi dell'art. 29 del GDPR, devono obbligatoriamente ricevere le adeguate istruzioni e la formazione necessaria al corretto trattamento di dati personali, nell'esecuzione delle prestazioni lavorative.

Il Titolare del trattamento, ai fini della formazione e del costante aggiornamento dei collaboratori che hanno accesso a Dati Personali, deve provvedere annualmente alla pianificazione di incontri o webinar formativi, a cui le persone autorizzate al trattamento dei dati saranno tenute a partecipare
Inoltre potranno essere adottati strumenti formativi ad hoc (mansionari, istruzioni e circolari operative interne), in particolare, nel caso di:

- emersione di nuove minacce per la sicurezza dei Dati Personali
- adozione di nuove misure di sicurezza
- modifica di processi aziendali
- introduzione di nuove tecnologie

CONSIGLI

•Organizzare corsi di formazione periodici per tutti i dipendenti/collaboratori, avvalendosi di enti di formazione accreditati;

•Effettuare stress test e simulare remediation plan per testare la sicurezza e i tempi di risposta, almeno una volta l'anno.

SISTEMA SANZIONATORIO
SANZIONI AMMINISTRATIVE E PENALI

SANZIONI AMMINISTRATIVE

Il regime sanzionatorio trae le sue origini già dalla Dir. 95/46 che, tuttavia non specificava il tipo e l'entità delle sanzioni previste, affidando agli Stati Membri il compito di disciplinare le conseguenze delle violazioni, senza precisare se le violazioni dovessero essere penali o amministrative. Il Nuovo Regolamento Europeo individua il tipo e l'entità delle sanzioni. In particolare sanzioni amministrative e penali

All'art. 83 il Regolamento prevede, a livello amministrativo le sanzioni equivalenti per le violazioni. Il concetto di equivalenza si traduce nel più ampio principio di coerenza che conduce alla previsione per cui il comitato elabora per le autorità di controllo linee guida riguardanti la previsione delle sanzioni amministrative pecuniarie di cui all'art. 83. Ciò al fine di evitare squilibri tra gli stati membri.

Il regolamento esclude un'applicazione meccanica e assoluta delle sanzioni, preferendo un impianto fondato sulla ponderazione e alla concretizzazione, evitando gli automatismi, e garantendo più flessibilità, decidendo in modo equo secondo una valutazione caso per caso

Gli importi delle sanzioni ex art. 83, seguono dei valori fissi per i quali è individuata la massima somma comminabile, oppure vengono calcolati in percentuale sul fatturato delle imprese. Sussiste però il limite del cumulo sanzionatorio sia per le persone fisiche che per le persone giuridiche, in caso di plurime violazioni.

Il primo livello sanzionatorio va **fino ad un massimo di 10.000.000 di euro o per le imprese, fino al 2% del fatturato mondiale** annuo dell'esercizio precedente, se superiore

Il secondo livello sanzionatorio va fino ad un massimo di 20.000.000 di euro o per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore

Primo livello sanzionatorio → Violazione del consenso dei minori; trattamento che non richiede l'identificazione; principi e misure di data protection-by-design e by-default; tenuta dei registri delle attività del trattamento; adozione di misure di sicurezza adeguate…

Secondo livello sanzionatorio → Violazione dei principi generali applicabili al trattamento; delle condizioni di liceità; delle condizioni per il consenso e diritto di revocato; delle disposizioni relative al trattamento di categorie particolari di dati personali; mancato rispetto dei diritti dell'interessato…

SANZIONI PENALI “speciali”

Tipologie previste dal novellato Codice Privacy D.lgs 196/2003

Art. 167 (Trattamento illecito di dati)

Art. 167- bis (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)

Art. 167- ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)

Art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante)

Art. 170 (Inosservanza di provvedimenti del Garante)

Art. 171 (Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori)