L'HACKER NEL FALDONE: PRIVACY E CRIPTAZIONE DEI DATI NELLO STUDIO LEGALE

27 Gennaio 2021

LA SICUREZZA

Estratto dalle FAQ «Privacy e Studi Legali»

A cura della Commissione Privacy dell'Ordine degli Avvocati di Roma

Responsabile: Cons. Avv. Cristina Tamburro

Vice Responsabile: Cons. Avv. Andrea Pontecorvo

ORDINE AVVOCATI DI ROMA

ORDINE AVVOCATI DI ROMA

Quali misure di sicurezza devono essere adottate (principio di accountability)?

Il GDPR stabilisce l'obbligo per il titolare del trattamento di adottare "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*" (art. 32 GDPR). Nello specifico il GDPR orienta la scelta verso le misure che assicurino, se del caso:

"*a) la pseudonimizzazione e la cifratura dei dati personali;*

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

Oltre alle suddette indicazioni di massima, il GDPR non prevede un elenco prestabilito delle misure di sicurezza da adottare, in quanto rimette la scelta al titolare del trattamento sulla base di una sua valutazione.

Questo perché il GDPR si fonda sul principio di responsabilizzazione (*accountability*), che implica la libertà del titolare del trattamento di approntare, nei limiti del rispetto dei principi imposti dalla normativa, le misure che ritiene più adeguate alla protezione dei dati personali.

Il principio di responsabilizzazione comporta, però, anche la necessità di dover dare prova della valutazione svolta e delle scelte operate, rendendo di fatto non possibile basarsi solamente su modelli precompilati ovvero su documentazione standard.

Il GDPR indica fra gli elementi che l'avvocato dovrà considerare per la scelta delle misure di sicurezza da adottare lo "*stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*" (art. 32).

ORDINE AVVOCATI DI ROMA

Cosa si intende per pseudonimizzazione e cifratura dei dati personali?

La pseudonimizzazione e la cifratura dei dati sono strumenti che perseguono il medesimo fine di oscurare il dato per renderlo incomprensibile a coloro che non hanno la “chiave” per accedervi, sebbene con alcune differenze.
La pseudonimizzazione è definita nel GDPR come la tecnica che permette il trattamento dei dati personali in modo tale che tali dati “non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive” (art. 4, punto 5).
Più semplicemente tale tecnica consiste nel sostituire i dati personali con dei codici o pseudonimi, così che un terzo non possa individuare la persona a cui si riferiscono i dati.
Per l’avvocato tale misura può, e deve, essere adottata per esempio nell’intestazione dei fascicoli di studio, sulla cui copertina è consigliabile non indicare i nomi delle parti, ma un codice o un numero di classificazione. In questo modo, solo chi è a conoscenza del codice di classificazione del fascicolo può risalire all’identità della persona a cui i dati si riferiscono.
La crittografia o cifratura, invece, si basa di solito su un algoritmo e su una password.
Con la crittografia un qualunque file di dati (testo, immagini, ecc.), con l’utilizzo di un algoritmo, viene trasformato in un insieme di segni e simboli assolutamente privi di significato che potranno essere decifrati e resi leggibili solo con l’utilizzo della "chiave" giusta. In questo modo, anche se un estraneo accede ai file o al dispositivo protetto da cifratura, non potrà visualizzare i dati se non in possesso della password.

ORDINE AVVOCATI DI ROMA

Cosa si intende per “capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento” di cui all’art. 32,par. 1, lettera b), GDPR?

L’art. 32 par. 1 lettera b) fa riferimento ai concetti di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi informatici che trattano i dati personali.
Per riservatezza si intende la protezione dei dati trasmessi o conservati per evitarne l’intercettazione e la lettura da parte di persone non autorizzate.
Per integrità, si intende la conferma che i dati trasmessi, ricevuti o conservati siano completi e inalterati.
La disponibilità, invece, è da intendersi come conferma che i dati siano accessibili e i servizi funzionino anche in caso di interruzioni dovute a eventi eccezionali o ad attacchi di pirateria informatica.
Con il concetto di resilienza, infine, ci si riferisce alla capacità di un sistema di adattarsi alle condizioni d’uso e di resistere all’usura al fine di assicurare la disponibilità dei servizi che vengono forniti e l’adeguata protezione dei dati che vengono trattati con tali sistemi.

ORDINE AVVOCATI DI ROMA

Cosa si intende per “capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico” di cui all’art. 32,par. 1, lettera c), GDPR?

La norma di cui all’art. 32 par. 1 lettera c) GDPR attribuisce rilievo al concetto di disaster recovery, che consiste nella capacità di reagire in modo efficace e tempestivo ad eventuali criticità dovute ad incidenti fisici o tecnici, allo scopo di ripristinare la disponibilità e l’accesso dei dati personali oggetto di trattamento.
A tale riguardo, sarà quindi importante per i titolari predisporre un programma specifico attraverso cui analizzare innanzitutto i rischi che potrebbero andare a colpire il sistema informatico; prevedere poi le adeguate misure da adottare per minimizzarli; ed infine predisporre un piano di emergenza che permetta di attuare un sistema alternativo di elaborazione dei dati da utilizzare in attesa della completa riattivazione.

ORDINE AVVOCATI DI ROMA

Quali sono le misure da adottare per i documenti e fascicoli gestiti digitalmente?

Per la gestione dei documenti e fascicoli digitali, si consiglia di:

- impostare un sistema di autenticazione: prevedere l'accesso tramite una password diversa per ogni avocato e collaboratore;
- gestire e profilare gli accessi: prevedere che le persone accedano ai soli dati di cui hanno necessità per il proprio lavoro ed evitare che tutti accedano a tutto indiscriminatamente e rimuovere le autorizzazioni obsolete;
- impostare un sistema di backup: evitare che i documenti e i fascicoli digitali siano conservati su un unico computer, ma prevedere un sistema di copia o sincronizzazione dei dati su un altro supporto custodito;
- proteggere gli strumenti informatici: dotarsi di software di protezione contro le minacce informatiche (antivirus, antimalware, firewall, ecc.);
- mantenere in efficienza gli strumenti informatici: installare e utilizzare solo software sicuri e prevedere il periodico aggiornamento e manutenzione dei dispositivi hardware e dei software utilizzati;
- gestire i dispositivi mobili: prevedere un sistema di protezione adeguato (password, crittografia, ecc.) per computer portatili, smartphone, chiavette USB, CD, DVD, tablet, hard disk portatili, ecc., ed evitare, per quanto è possibile, di memorizzare su tali dispositivi dati personali sensibili dei clienti e comunque prevedere un sistema di copia e sincronizzazione (backup) dei dati presenti anche su altri supporti custoditi a studio;
- gestire la dismissione e manutenzione degli strumenti informatici: se si dismette definitivamente un dispositivo (p.es. smartphone, tablet, pennetta usb, ecc.) si dovrà procedere alla cancellazione definitiva dei dati presenti o, se non è possibile, bisognerà rendere inutilizzabile il dispositivo. In caso di malfunzionamento dei dispositivi si consiglia di rimuovere i dati presenti prima di consegnarlo ad un tecnico per la riparazione e comunque di affidarsi all'assistenza di personale e società qualificate che assicurino non solo un intervento a regola d'arte, ma anche le dovute rassicurazioni sulla sicurezza dei dati presenti.

ORDINE AVVOCATI DI ROMA

Quali password scegliere e come gestirle?

Per accedere agli strumenti informatici (dispositivi, e-mail, programmi, gestionali, ecc.), si dovrà adottare una password “sicura” diversa per ogni persona e per ogni tipologia di accesso. Si consiglia di utilizzare una password composta da almeno 8 caratteri alternando lettere minuscole e maiuscole, numeri e caratteri speciali che non possa essere scoperta da un programma o da una persona in un breve lasso, ma che nello stesso tempo sia facile da ricordare.
La password non dovrà essere condivisa e non dovrà essere scritta chiaramente su un foglio e andrà cambiarla regolarmente.
Fra i metodi per creare una password sicura e facile da ricordare vi è quello di partire da una frase piuttosto che da una singola parola complessa, provvedendo a modificare alcune lettere in modo che non rimanga di senso compiuto.
Per una password sicura si consiglia di:

- non utilizzare le stesse password per più account o utilizzate negli account personali (p.es. social network, e-mail privata, sito per hobby privati, ecc.);
- non scegliere una password contenente riferimenti agevolmente riconducibili alla persona o ai suoi famigliari oppure in generale a parole a lei riconducibili (p.es. codice fiscale, nome della moglie o dei figli, luogo e data di nascita, ecc.);
- non utilizzare parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.) o acronimi che si possono trovare nel dizionario, anche in lingue straniere;
- non prevedere citazioni, slogan, motti o detti conosciuti;
- non utilizzare sequenze di tasti sulla tastiera (asdf) o sequenze di numeri (1234);
- non impostare password di soli numeri, di sole lettere maiuscole o di sole lettere minuscole;
- non prevedere ripetizioni di caratteri (aa11);
- non utilizzare password adottate in precedenza;
- non adottare una password utilizzata in un esempio trovato di come si sceglie una buona password.

ORDINE AVVOCATI DI ROMA

Quali misure di sicurezza adottare nell'utilizzo della posta elettronica e di Internet?

Nell'utilizzo delle e-mail e di internet, al fine di garantire la massima protezione dei dati trattati e degli strumenti utilizzati è consigliabile adottare le seguenti misure di sicurezza e buone prassi:

- scegliere un provider di posta elettronica che fornisca le dovute rassicurazioni in merito a sicurezza e competenza;
- utilizzare un account di mail specificatamente ed esclusivamente dedicato all'attività professionale;
- evitare di fornire la propria mail per iscriversi a portali, newsletter o servizi non attinenti all'attività di lavoro o che non assicurino un livello adeguato di sicurezza;
- evitare di aprile le e-mail non richieste, quelle provenienti da persone sconosciute, quelle con contenuto anomalo, quelle classificate come "spam" e quelle provenienti da enti, uffici o società (p.es. banche, Agenzia delle entrate, Inps, Inail) che normalmente utilizzano pec e non e-mail; nel dubbio è consigliabile accedere attraverso il portale ufficiale del mittente piuttosto che utilizzare il link indicato nella mail sospetta;
- evitare di scaricare file, link o programmi allegati alla posta elettronica di cui non è sicuro della provenienza o presenti su siti internet non attendibili o inaffidabili (spesso gratuiti) come siti freeware o shareware. Non installare automaticamente le opzioni predefinite (barre degli strumenti, componenti aggiuntivi, plugin, motori di ricerca, ecc.);
- evitare di fornire o comunicare con e-mail o su internet informazioni o dati relativi a password o credenziali di accesso ai propri dispositivi;
- se si deve inviare uno stesso allegato a più persone, è consigliabile non lasciare in chiaro gli indirizzi e-mail di tutti i destinatari, a meno che i destinatari si conoscano fra loro e si tratti di una discussione comune a tutti (si ricorda che anche gli indirizzi e-mail sono da ritenersi dati personali);
- se si devono inviare allegati diversi a più soggetti, si consiglia di inviare e-mail separate per ogni destinatario con il rispettivo allegato. Inoltre, se non espressamente previsto e autorizzato, non si dovranno inviare dati personali attinenti a soggetti terzi rispetto al destinatario della e-mail e se tali dati sono contenuti in uno stesso file (p.es. elenco di nomi, indirizzi ecc.), si dovranno mantenere separati i rispettivi dati personali o rimuovere i dati personali non attinenti al singolo destinatario;
- utilizzare sempre le connessioni sicure per inviare le mail e navigare su internet ed evitare di connettere i dispositivi a reti wi-fi pubbliche, hotspot o reti non protette.

ORDINE AVVOCATI DI ROMA

Quali sono le misure di sicurezza da adottare per i documenti, archivi e fascicoli cartacei?

Per la gestione dei documenti, archivi e fascicoli cartacei, si consiglia di:

- evitare di indicare sulle copertine dei fascicoli i dati personali delle parti (p.es. nome, cognome, indirizzo, cod. fiscale ecc.), ma utilizzare una sigla o codice sostitutivo in base alla classificazione adottata dallo studio (c.d. pseudonimizzazione);
- evitare di lasciare incustoditi i documenti e fascicoli sulla propria scrivania o in altri luoghi dello studio, ma riporli negli appositi archivi o cassetti da mantenere chiusi, soprattutto se nello studio accedono persone estranee (p.es. addetti alle pulizie, collaboratori occasionali, fornitori di servizi, ecc.);
- evitare di lasciare incustoditi i documenti nella stampante o nello scanner quando a tali dispositivi accedono anche terze persone;
- se è necessario inviare documenti contenenti dati personali di più persone, se non espressamente necessario, è consigliabile mantenere separati i rispettivi dati personali o rimuovere i dati personali non attinenti al destinatario formando tante copie differenti (p.es. formando tanti estratti o copie del documento in modo che ogni destinatario riceva solo i dati che gli riguardano);
- è consigliabile non stampare, estrarre o fotocopiare documenti con dati personali se non strettamente necessario alla finalità dell'incarico;
- è consigliabile custodire i fascicoli e i documenti in archivi e/o armadi dotati di serrature e chiavi;
- è consigliabile portare fuori dai locali dello studio fascicoli e documenti contenenti dati personali se non strettamente necessario e comunque con la massima attenzione e custodia;
- è consigliabile non portare i fascicoli e i documenti fuori dai locali dello studio, se non necessario allo svolgimento dell'incarico e in tal caso, se non è strettamente necessario, evitare di portare fuori gli originali. In ogni caso è consigliabile custodire con attenzione i fascicoli e i documenti, evitando di lasciarli in luoghi non sicuri (p.es. in macchina, in luoghi pubblici, presso un cliente, ecc.);
- riporre in modo ordinato i documenti negli appositi fascicoli e poi negli appositi archivi o cassetti, in maniera che possano essere reperiti facilmente;
- evitare di passare i documenti originali nelle macchine fotocopiatrici, scanner, fax, fascicolatori o altri macchinari se vi è il rischio di inceppamento e danneggiamento del documento (p.es. evitare di far passare i documenti originali attraverso il vassoio automatico della fotocopiatrice, ma utilizzare l'opzione manuale a vetro fotocopiando un documento alla volta);
- formare e informare i colleghi, collaboratori e le persone che accedono allo studio su tali regole e misure.

ORDINE AVVOCATI DI ROMA

Si può utilizzare un servizio cloud? E con quali accortezze?

Il GDPR non vieta l'utilizzo di servizi cloud, ma l'avvocato dovrà comunque tutelare e proteggere i dati personali, verificando la presenza di adeguate garanzie di sicurezza, soprattutto perché spesso l'offerta di servizi cloud si fondano su condizioni di contratto predisposte dagli stessi fornitori la cui negoziabilità è quantomeno limitata, specialmente per quanto attiene agli standard di sicurezza.

Pertanto, prima di utilizzare un servizio cloud su cui trasferire i dati personali dei propri clienti, è consigliabile analizzare alcuni aspetti relativi:

- alla gestione e "destino" dei dati personali alla cessazione del rapporto contrattuale;
- all'ubicazione dei server dove sono conservati i dati e ai possibili trasferimenti extra-UE (p.es. per la presenza di subappaltatori del fornitore);
- alla possibilità, da parte del fornitore dei servizi cloud di monitorare l'utilizzo dei servizi da parte dell'utente e la possibilità di un accesso e trattamento di dati personali;
- alla possibilità per l'avvocato-utente di poter effettuare audit precontrattuali, test, o verifiche sul fornitore ed eventuali subfornitori dei servizi cloud;
- alla verifica che le politiche (policy) di sicurezza applicate dal fornitore dei servizi cloud siano in linea con le prescrizioni del GDPR e con gli standard di sicurezza riconosciuti (p.es. ISO 27001) o siano avvalorati con certificazioni rilasciate da organismi tersi indipendenti;
- all'obbligo da parte del fornitore dei servizi cloud di segnalare tempestivamente e in modo circostanziato eventuali violazione dei dati (data breach);
- alla possibilità per l'avvocato-utente di richiedere la copia dei dati trasferiti in un formato facilmente fruibile (portabilità dei dati), ad esempio, per l'esigenza di poter migrare i dati in un altro servizio cloud senza rischiare di perdere i dati.
- Pertanto, l'avvocato che intende utilizzare un servizio cloud è tenuto ad effettuare una verifica accurata sul fornitore (due diligence) per valutare se il fornitore è in grado di soddisfare non solo le esigenze operative, ma anche quelle di sicurezza dei dati personali trattati.
- È consigliabile comunque conservare una copia dei dati anche su supporti da custodire all'interno dello studio.
- Non deve, comunque, trascurarsi che il ricorso ai servizi cloud presenta diversi vantaggi, anche perché le infrastrutture e i livelli di sicurezza offerti dai fornitori di servizi cloud spesso risultano difficilmente replicabili all'interno dello studio, se non con importanti investimenti di risorse non sempre alla portata dei piccoli e medi studi legali.

ORDINE AVVOCATI DI ROMA

Quali sono le attività che deve compiere l'avvocato in caso di raccolta di dati personali attraverso il sito internet?

Il sito web può essere utilizzato dall'avvocato per promuovere la propria attività professionale, per presentare i componenti dello studio, pubblicare articoli, ma anche consentire la raccolta di dati personali mediante un questionario online, una consultazione online, un modulo di contatto, la creazione di un account online, nonché attraverso i cookies.

Se il sito web dello studio permette l'inserimento di dati personali, ad esempio il modulo di contatto e richiesta informazioni, è opportuno che sia utilizzata la connessione con protocollo sicuro HTTPS (tecnologia "SSL") per garantire il rispetto delle misure di sicurezza in funzione della confidenzialità delle informazioni scambiate con il professionista.

L'avvocato dovrà inserire, all'interno del registro delle attività di trattamento, un apposito modulo dedicato al trattamento dei dati personali sul sito web.

Siffatto modulo dovrà contenere l'indicazione di:

- identità e dettagli di contatto del titolare;
- scopi;
- categorie di persone;
- categorie di dati personali;
- categorie di destinatari;
- trasferimenti verso un paese terzo o un'organizzazione internazionale;
- scadenze per la cancellazione;
- descrizione generale delle misure di sicurezza tecniche e organizzative.

Ai sensi dell'art. 23 del Codice Deontologico, inoltre, nel caso in cui l'avvocato riceva una proposta di incarico tramite il sito web ha l'obbligo di formalizzare il mandato accertando l'identità del cliente.

ORDINE AVVOCATI DI ROMA

Quali sono i dati obbligatori che l'avvocato deve necessariamente includere nel sito web?

Il sito web del professionista deve contenere alcuni dati obbligatori.
Tali elementi obbligatori sono previsti:

- dal Codice deontologico, quali l'indicazione del titolo professionale, la denominazione dello studio e l'ordine di appartenenza ex art. 35, comma 3 del Codice Deontologico.
- Ai sensi dell'art. 35, comma 5 del Codice Deontologico il praticante può utilizzare soltanto il titolo per esteso "praticante avvocato" con l'eventuale indicazione di "abilitato al patrocinio" qualora abbia conseguito l'abilitazione;
- dall'art. 7 del D. Lgs. n. 70/2003 sul commercio elettronico (che prevede l'irrogazione di una sanzione amministrativa da Euro 103 ad Euro 10.000), quali il riferimento alle norme professionali e al codice deontologico e le modalità di consultazione dei medesimi, nonché il numero della partita IVA. In base a quanto disposto dalla Legge n. 247/2012 il compenso non è tra le informazioni che possono essere diffuse;

dal GDPR, quali l'obbligo incombente per i titolari di siti web di informare gli utenti che visitano il sito sulle modalità di utilizzo dei cookie, l'Informativa sul trattamento dei dati e le informazioni di cui agli artt.13 e 14 GDPR.

ORDINE AVVOCATI DI ROMA

In caso di utilizzazione dei cookies l'avvocato come deve rendere la relativa informativa?

In primis, l'avvocato dovrà verificare l'effettiva presenza di cookie sul sito web attraverso il dipartimento IT del provider, attraverso i fornitori di servizi o controllando gli strumenti utilizzati per la messa a disposizione del sito web.
Successivamente, è necessario determinare i tipi di cookie utilizzati sul sito web dell'avvocato.
Alcuni cookie richiedono il consenso dell'utente, come i cookie pubblicitari, i cookie "social network" generati dai pulsanti di condivisione, quando raccolgono dati personali senza il consenso delle persone interessate, ed alcuni cookie di misurazione degli accessi.
In questo caso, il consenso deve essere precedente all'inserimento o alla lettura del contenuto del sito. Finché il cliente non ha dato il suo consenso, questi cookie non possono essere depositati o letti dal sito stesso.