



UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII

Dipartimento di Ingegneria
dell'Informazione



unIMC

"LA TRASFORMAZIONE DIGITALE DELLA PROFESSIONE FORENSE: RESPONSABILITÀ, COMPETENZE E PROSPETTIVE FUTURE"

Laura Migliora

Avvocato

Studio legale Meisina e Migliora – Voghera (PV)

E-mail: avv.lauramigliora@gmail.com

Mobile: +39 338 9589299

Venerdì 03 ottobre 2025



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

PARTE I: OBBLIGHI NORMATIVI - GDPR E REGOLE DEONTOLOGICHE



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

NORME E DISPOSIZIONI



IL QUADRO NORMATIVO FONDAMENTALE

Norme professionali tradizionali:

- Art. 3 Legge n. 247/2012: "diligenza e competenza" nell'esercizio professionale
- Art. 6 Legge n. 247/2012: Segreto professionale esteso a "dipendenti e collaboratori"
- Art. 11 Legge n. 247/2012: Obbligo di "formazione continua"

Norme civilistiche:

- Art. 1176, comma 2, c.c.: Diligenza qualificata "con riguardo alla natura dell'attività esercitata"

Norme europee sulla protezione dati:

- Art. 32 GDPR: Misure di sicurezza tecniche e organizzative
- Art. 25 GDPR: Privacy by design e by default

Norme professionali e civilistiche



- **Art. 3 Legge n. 247/2012: «diligenza e competenza»**

2. La professione forense deve essere esercitata con indipendenza, lealtà, probità, dignità, decoro, diligenza e competenza, tenendo conto del rilievo sociale della difesa e rispettando i principi della corretta e leale concorrenza.

- **Art. 6 Legge n. 247/2012: Segreto professionale esteso a «dipendenti e collaboratori»**

1. L'avvocato è tenuto verso terzi, nell'interesse della parte assistita, alla rigorosa osservanza del segreto professionale e del massimo riserbo sui fatti e sulle circostanze apprese nell'attività di rappresentanza e assistenza in giudizio, nonché nello svolgimento dell'attività di consulenza legale e di assistenza stragiudiziale.

2. Le disposizioni di cui al comma 1 si applicano anche nei confronti dei dipendenti e dei collaboratori anche occasionali dell'avvocato, oltre che di coloro che svolgono il tirocinio presso lo stesso, in relazione ai fatti e alle circostanze da loro apprese nella loro qualità o per effetto dell'attività svolta. L'avvocato è tenuto ad adoperarsi affinché anche da tali soggetti siano osservati gli obblighi di segretezza e di riserbo sopra previsti.

- **Art. 11 Legge n. 247/2012: Obbligo di «formazione continua»**

1. L'avvocato ha l'obbligo di curare il continuo e costante aggiornamento della propria competenza professionale al fine di assicurare la qualità delle prestazioni professionali e di contribuire al migliore esercizio della professione nell'interesse dei clienti e dell'amministrazione della giustizia.

- **Art. 1176, comma 2, c.c.:** Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata

Regolamento 2016/679 - GDPR



▪ **Art. 32 GDPR: Misure di sicurezza tecniche e organizzative**

Riguarda la sicurezza del trattamento dei dati personali e obbliga il titolare e il responsabile del trattamento a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio. Tali misure devono assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi, prevedendo la possibilità di pseudonimizzazione e cifratura, e l'adozione di procedure per testare e valutare regolarmente l'efficacia di queste misure

Art. 25 GDPR: Privacy by design e by default

§ 1 "privacy by design" - ha lo scopo di garantire l'esistenza di un corretto livello di privacy e protezione dei dati personali fin dalla fase di progettazione (design) di qualunque sistema, servizio, prodotto o processo così come durante il loro ciclo di vita. Punta a garantire un corretto livello di protezione dei dati in tutte le attività di trattamento ed attuazioni effettuate all'interno di una organizzazione.

§ 2 "privacy by default" - il legislatore europeo ha affermato la necessità che la protezione dei dati personali sia garantita "per impostazione predefinita", esige che il titolare individui, prima di iniziare il trattamento dei dati, quali dati personali sono strettamente necessari, per la finalità specifica per cui sono stati acquisiti, ai fini di proteggere la riservatezza dei dati personali.

LA RESPONSABILITÀ PROFESSIONALE NELL'ERA DIGITALE



Nuovi parametri di valutazione:

- Competenza nell'uso degli strumenti digitali
- Controllo dell'esito dei depositi telematici
- Gestione sicura dei dati del cliente
- Protezione da attacchi informatici
- Formazione del personale sui rischi cyber

Evoluzione giurisprudenziale:

- Cassazione civile, ord. n. 17703/2023: Obbligazione di mezzi e diligenza qualificata
- Tribunale Busto Arsizio, sent. n. 1294/2024: Responsabilità per errori nel deposito telematico

IL GDPR E L'AVVOCATO TITOLARE DEL TRATTAMENTO



Obblighi specifici secondo le linee guida CNF:

- **Art. 25 GDPR:** Privacy by design e by default
- **Art. 32 GDPR:** Misure di sicurezza tecniche e organizzative
- **Principio di accountability:** documentare la conformità
- **Registro dei trattamenti** obbligatorio per dati particolari
- **Data breach notification** entro 72 ore

DOVERI DEONTOLOGICI E SEGRETO PROFESSIONALE DIGITALE



Estensione del segreto professionale nell'era digitale:

- **Protezione end-to-end** delle comunicazioni con i clienti
- **Formazione del personale** sui rischi cyber
- **Controllo degli accessi** ai fascicoli digitali
- **Backup sicuri e disaster recovery**
- **Gestione delle password e autenticazione multi-fattore**
- **Separazione dei dati** per diversi clienti

DATA BREACH



COSA DEVE FARE L'AVVOCATO? (ARTT. 33 E 34 GDPR)

- 1. AVVISARE SENZA INDUGIO LE PERSONE COMPETENTI
- 2. QUALIFICARE LA VIOLAZIONE
- 3. ADOTTARE LE MISURE NECESSARIE PER MINIMIZZARE LE CONSEGUENZE
- 4. EFFETTUARE LE NOTIFICAZIONI ALL'AUTORITÀ GARANTE, A MENO CHE NON SIA IMPROBABILE CHE SUSSISTA UN RISCHIO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE
- 5. SE IL RISCHIO È ELEVATO EFFETTUARE LE COMUNICAZIONI AGLI INTERESSATI
- 6. IN OGNI CASO ANNOTARE TUTTE LE VIOLAZIONI (ANCHE SE NON NOTIFICATE) NEL REGISTRO DELLE VIOLAZIONI

PARTE II: STRUMENTI DELLO STUDIO LEGALE



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

STRUMENTI BASE DELLA DIGITALIZZAZIONE FORENSE



Processo telematico

- **Fascicolo telematico:** Gestione documentale integrata
- **Deposito telematico obbligatorio:** estensione progressiva attraverso normative nel tempo
- **Controllo qualità:** Verifica automatica degli esiti

PEC – posta elettronica certificata

- Valore legale e gestione delle ricevute – archiviazione e conservazione

Firma digitale – Smartcard, token, firma remota

- **CAdES:** Cryptographic Message Syntax (CMS) Advanced Electronic Signature
- **PAdES:** PDF Advanced Electronic Signatures
entrambe le tipologie hanno pieno valore giuridico e sono equiparabili in ogni sede alla firma autografa su carta
- **XAdES:** XML Advanced Electronic Signatures
utilizzato per fatturazione elettronica

Linee guida per la gestione digitale



Consigli in caso di documenti o fascicoli gestiti digitalmente

- **Autenticare gli utenti:** impostare una password minima di 8 caratteri contenenti maiuscole, lettere minuscole, numeri e caratteri speciale; non condividerla; non scriverla chiaramente su un foglio; evitare la pre-registrazione; cambiarla regolarmente;
 - . gestire i diritti e istruire gli utenti: determinare persone che hanno il diritto di accedere ai dati personali;
 - . rimuovere le autorizzazioni di accesso obsolete;
 - . scrivere un regolamento di utilizzo del computer e inserirlo nel regolamento interno nell'ipotesi che sia stato adottato;
- **mobile computing sicuro:** fornire mezzi di crittografia per computer portatili e dispositivi di archiviazione rimovibili (chiavette USB, CD, DVD ...), evitare di memorizzare dati personali sensibili dei clienti.
- **eseguire il backup e pianificare la business continuity:** implementare i backup regolarmente, conservare i supporti di backup in un luogo sicuro, ecc.

CLOUD COMPUTING E SICUREZZA DEI DATI



Gestione sicura dei dati in cloud:

- **Criteri di scelta** del provider cloud
- **Contratti con responsabili** del trattamento
- **Crittografia** dei dati in transito e a riposo
- **Backup** e business continuity
- **Controllo degli accessi** e log di audit
- **Trasferimenti extra-UE** e Transfer Impact Assessment

Esempi di servizi cloud comuni:

Google Drive, Dropbox, iCloud, Gmail, Microsoft 365

Firewall, antivirus e sistemi operativi sempre aggiornati

INTELLIGENZA ARTIFICIALE E AI ACT



Il nuovo Regolamento UE sull'IA (Regolamento UE 2024/1689):

- **Classificazione dei rischi:** Inaccettabile, Alto, Limitato, Minimo
- **Obblighi per i fornitori:** Trasparenza, documentazione, supervisione umana
- **Diritti degli utenti:** Informazione, spiegabilità, ricorso

Applicazioni nell'ambito legale:

- **Legal research:** Ricerca giurisprudenziale automatizzata
- **Document review:** Analisi automatica di contratti
- **Predictive analytics:** Previsioni sull'esito dei giudizi
- **Chatbot legali:** Assistenza clienti automatizzata

CRITTOGRAFIA E PSEUDONIMIZZAZIONE



Tecniche avanzate di protezione dei dati:

- **Pseudonimizzazione** per ridurre i rischi ed **anonimizzazione** quando possibile *«il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile» (Art. 4, par. 5, GDPR)*
- **Chiavi di cifratura** e gestione sicura
- **Crittografia end-to-end** per comunicazioni sensibili
- **Tecniche di hashing** per l'integrità dei dati

SISTEMI DI GESTIONE E AUTOMAZIONE



Strumenti per l'efficienza operativa:

- **Software gestionali** per studi legali
- **Automazione** dei processi ripetitivi
- **Intelligenza artificiale** per la ricerca giuridica
- **Workflow management** per la gestione delle scadenze
- **Document automation** per contratti standard
- **Integration** con sistemi esterni (tribunali, registri)

PARTE III: FORMAZIONE DELL'AVVOCATO E CONFORMITÀ



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

FORMAZIONE CONTINUA E COMPETENZE DIGITALI



Evoluzione della formazione professionale:

- Art. 11 Legge n. 247/2012: Obbligo di aggiornamento continuo
- Competenze trasversali: Legal + Tech + Business
- Formazione del personale su privacy e sicurezza
- Framework di conformità e certificazioni professionali in ambito digitale
 - ISO 27001: Sistema di gestione della sicurezza delle informazioni
 - ISO 27002: Controlli di sicurezza informatica
 - ISO 31000: Gestione del rischio
- Certificazioni GDPR: Meccanismi di conformità
- Audit periodici e valutazioni di conformità
- Documentazione dei processi e delle procedure
- Best practices per miglior utilizzo del potenziale delle tecnologie di cloud e minimizzazione dei rischi in tema di tutela dei dati personali.

IL DPO E LE NUOVE OPPORTUNITÀ PROFESSIONALI



Nuovi ruoli e specializzazioni:

- **Art. 39 GDPR:** Compiti del Data Protection Officer
- **L'avvocato come DPO:** opportunità e conflitti di interesse
- **Consulenza specialistica** in privacy e cybersecurity
- **Legal tech** e innovazione nei servizi legali
- **Compliance officer** per normative emergenti
- **Formazione e consulenza** per altri professionisti

Caratteristiche e contenuti del registro



Obblighi documentali secondo Art. 30 GDPR:

- **Quando è obbligatorio:** Trattamento dati particolari, giudiziari, non occasionale
- **Contenuti minimi:** Finalità, categorie dati, destinatari, tempi conservazione, misure sicurezza
- **Modello CNF:** Template standardizzato per studi legali
- **Aggiornamento:** Revisione periodica e documentazione modifiche

Elementi del registro:

- Identificazione titolare e DPO
- Descrizione trattamenti e categorie interessati
- Trasferimenti extra-UE e garanzie adeguate
- Misure tecniche e organizzative adottate

INFORMATIVA EX ART. 13 PER STUDI LEGALI



Modello di informativa dal sito web del CNF

Informativa ai sensi dell'art. 13 del Regolamento europeo 679/2016 e consenso

Ai sensi dell'art. 13 del Regolamento europeo (UE) 2016/679 (di seguito GDPR), e in relazione ai dati personali di cui lo studio entrerà nella disponibilità con l'affidamento della Sua pratica, Le comunichiamo quanto segue:

Titolare del trattamento e responsabile della protezione dei dati personali

Titolare del trattamento è lo studio I... in persona dell'avv. ... (di seguito indicato anche come "professionista") con domicilio eletto in [LUOGO (solitamente indirizzo dello studio legale)]. Il Titolare può essere contattato mediante ____ [ad esempio PEC o email] all'indirizzo _____. Lo studio legale del Titolare (ha/non ha) nominato un responsabile della protezione dei dati personali (RPD ovvero, data protection officer, DPO) [nel caso in cui lo studio abbia nominato un data protection officer dovrà indicare anche i riferimenti di contatto del DPO].

Finalità del trattamento dei dati

Il trattamento è finalizzato alla corretta e completa esecuzione dell'incarico professionale ricevuto, sia in ambito giudiziale che in ambito stragiudiziale. I suoi dati saranno trattati anche al fine di:

- adempiere agli obblighi previsti in ambito fiscale e contabile;
- rispettare gli obblighi incombenti sul professionista e previsti dalla normativa vigente.

I dati personali potranno essere trattati a mezzo sia di archivi cartacei che informatici (ivi compresi dispositivi portatili) e trattati con modalità strettamente necessarie a far fronte alle finalità sopra indicate.

Base giuridica del trattamento

Lo studio del professionista tratta i Suoi dati personali lecitamente, laddove il trattamento:

- sia necessario all'esecuzione del mandato, di un contratto di cui Lei è parte o all'esecuzione di misure precontrattuali adottate su richiesta;
- sia necessario per adempiere un obbligo legale incombente sul professionista;
- sia basato sul consenso espresso [indicare nello specifico le attività per le quali sia richiesto il consenso: ad esempio invio di una newsletter da parte dello studio legale].

LE SANZIONI



Titolari e responsabili del trattamento possono essere soggetti a sanzioni amministrative significative per il mancato rispetto delle disposizioni del GDPR

L'autorità Garante per la protezione dei Dati personali, può, in particolare:

- rivolgere avvertimenti;
- ammonire l'avvocato, l'associazione o la società professionale;
- limitare temporaneamente o permanentemente un trattamento;
- sospendere i flussi di dati;
- ordinare di soddisfare richieste per l'esercizio dei diritti delle persone;
- ordinare la rettifica, limitazione o cancellazione dei dati
- Può inoltre ritirare la certificazione di conformità concessa all'avvocato, allo studio, all'associazione o alla società professionale, ovvero ordinarne il ritiro all'autorità di certificazione;
- comminare una sanzione amministrativa di importo compreso tra i 10 ed i 20 milioni di euro, ovvero, in caso di grandi studi internazionali di importo compreso tra il 2% ed il 4% del fatturato mondiale.

VALUTAZIONE DEI RISCHI E AUDIT



Gestione sistematica dei rischi digitali:

- **Risk assessment** periodico dei sistemi informatici
- **Vulnerability assessment** e penetration testing
- **Data Protection Impact Assessment (DPIA)**
- **Transfer Impact Assessment (TIA)**
- **AI Impact Assessment** per sistemi ad alto rischio
- **Business continuity planning**
- **Incident response** e gestione delle crisi

TUTELARSI DAL RISCHIO INFORMATICO - POLIZZE CYBER



GARANZIE:

- Responsabilità civile verso terzi per attacco Cyber
- Servizi per la gestione degli Eventi (legali, IT, comunicazione, ripristino dati, costi di notifica, etc)
- Pronto intervento gratuito per assistenza legale e informatica 48H
- Copertura danni accidentali o distruzione dei sistemi informatici
- Tutela per danni relativi all'interruzione della rete
- Tutela per estorsione informatica
- Responsabilità Civile Multimediale (pubblicità online, contenuto dei siti e social media)
- Copertura perdite da interruzione della rete del fornitore esterno di servizi
- Garanzia aggiuntiva estendibile a ogni pacchetto: Trasferimento fraudolento di fondi

CONVENZIONI, AGEVOLAZIONI ED INCENTIVI



- **Convenzioni tra Ordini degli Avvocati ed aziende specializzate :**

Consulenza Privacy, Fornitura Software, documentazione obbligatoria, assunzione di responsabilità in tema di gestione della Privacy/GDPR dello Studio, affiancamento in caso di Controlli della Guardia di Finanza e/o di Data Breach.

- **Bandi di Cassa forense**

Per professionisti individuali e per studi in esercizio associato o in forma societaria, Cassa forense eroga contributi a rimborso parziale delle spese per implementare l'organizzazione dello studio legale e per la formazione del personale in materia di gestioni e sicurezza informazioni ISO 27001; adozione di modelli organizzativi per lo studio legale di cui al D. Lgs. n. 231/2001 con codice etico; gestione privacy dello studio legale e nello specifico: informativa dipendenti – fornitori – clienti – curriculum - policy privacy sito web - lettere di incarico e vademecum con istruzioni operative per dipendenti e/o collaboratori addetti al trattamento dati - atti di nomina per responsabili del trattamento - registro dei trattamenti come titolare del trattamento

CONCLUSIONI E PROSPETTIVE FUTURE



Roadmap per l'avvocato del futuro:

- **Investimento nella formazione** continua e specialistica
- **Implementazione graduale** di sistemi di sicurezza
- **Sviluppo di competenze trasversali** (legal + tech)
- **Adozione di standard internazionali** di conformità
- **Creazione di partnership strategiche** con esperti IT
- **Documentazione sistematica** per l'accountability
- **Monitoraggio continuo** dell'evoluzione normativa su IA

Sfide emergenti:

- Regolamentazione dell'intelligenza artificiale
- Evoluzione delle minacce cyber
- Nuove forme di responsabilità professionale
- Integrazione etica della tecnologia

GRAZIE!



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection