Cybersecurity e Procedure Interne nello Studio Professionale

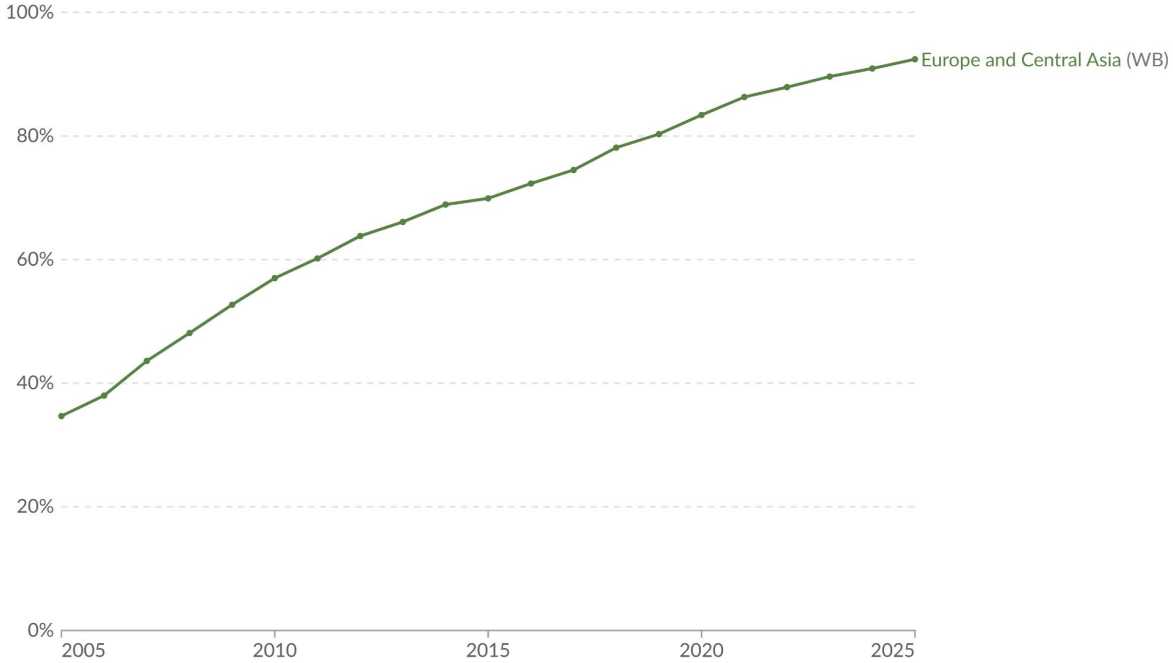
Gestione del rischio, adeguamento normativo (GDPR & AI Act) e best practice per il commercialista moderno



Claudio Sica
Presidente di commissione Tecnologie e Innovazione Studi Professionali

Share of the population using the Internet

Share of the population who used the Internet[1] in the last three months.

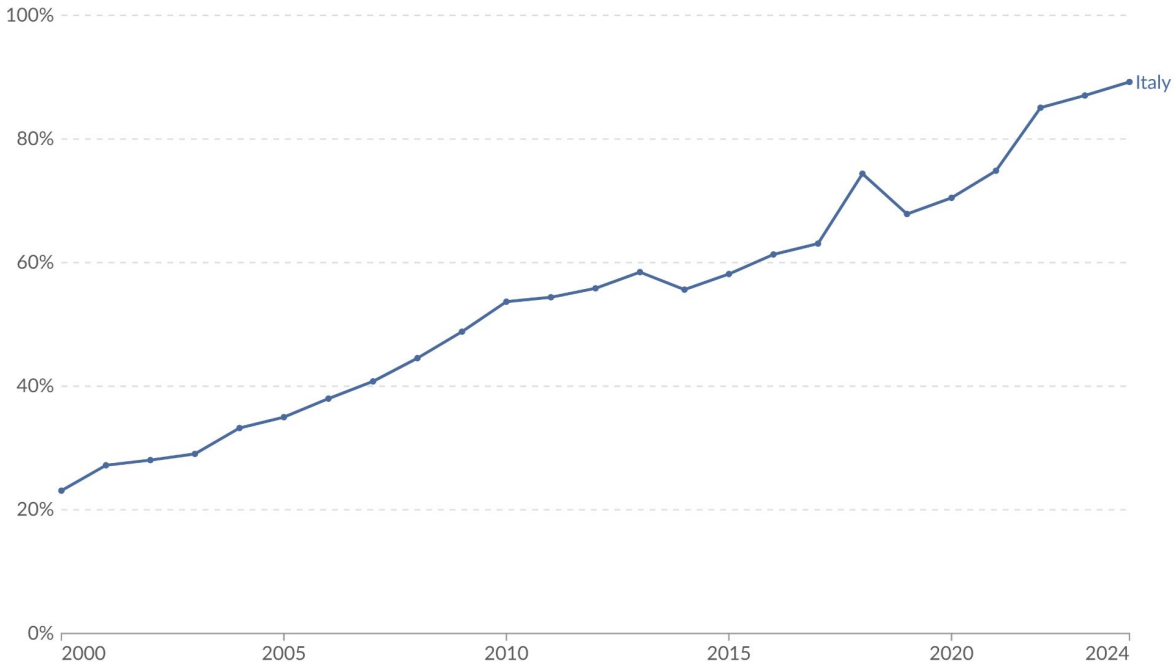


Data source: World Telecommunication/ICT Indicators Database - International Telecommunication Union (ITU), via World Bank (2026)
OurWorldinData.org/internet | CC BY

1. Internet user The International Telecommunication Union defines an Internet user as anyone who has accessed the Internet from any location in the last three months.
This can be from any type of device, including a computer, mobile phone, personal digital assistant, games machine, digital TV, and other technological devices.

Share of the population using the Internet

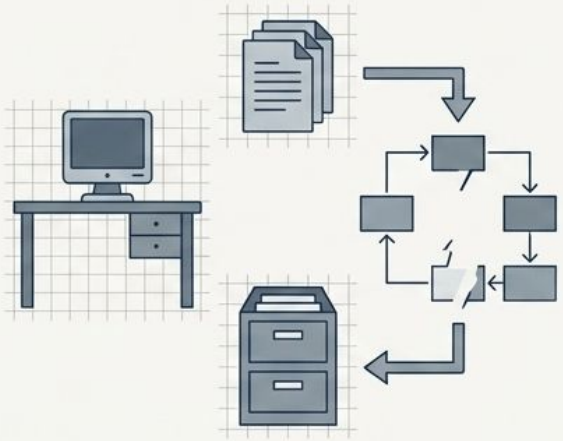
Share of the population who used the Internet[1] in the last three months.



Data source: World Telecommunication/ICT Indicators Database - International Telecommunication Union (ITU), via World Bank (2026)
OurWorldinData.org/internet | CC BY

1. Internet user The International Telecommunication Union defines an Internet user as anyone who has accessed the Internet from any location in the last three months.
This can be from any type of device, including a computer, mobile phone, personal digital assistant, games machine, digital TV, and other technological devices.

IERI



Studio Isolato

OGGI



Ecosistema Digitale Interconnesso

Il perimetro dello studio non è più fisico, ma un ecosistema digitale interconnesso e globale.

Come si lavorava *anni fa*...





Identikit del Professionista

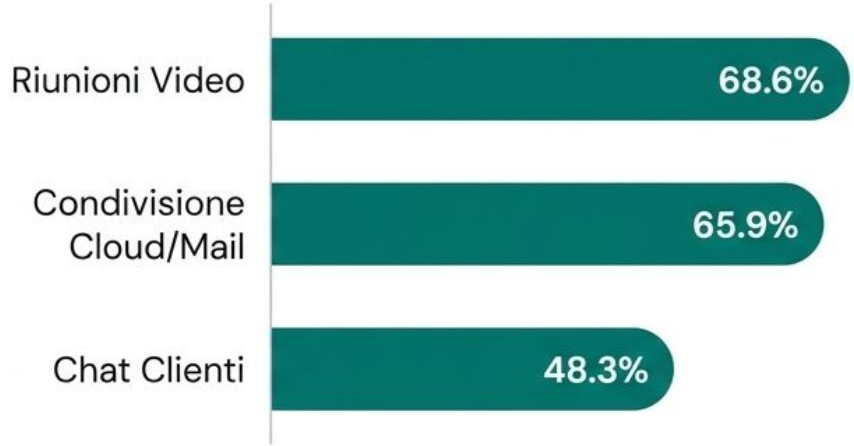
Età: Over 55

Esperienza: 20+ anni

Struttura: Studio Singolo (1-3 figure)

Core Business: Contabilità, Fisco, Revisione, Crisi d'impresa

Strumenti Digitali Utilizzati



Un'elevata dipendenza operativa dagli strumenti digitali all'interno di strutture dimensionalmente contenute.

THE SECURE BLUEPRINT

UTILIZZO PACCHETTO OFFICE / EMAIL



TRATTAMENTO DATI / PRIVACY BASE



CYBERSECURITY & ARCHIVIAZIONE DIGITALE COMPLESSA



INTELLIGENZA ARTIFICIALE



NESSUN DIVARIO GENERAZIONALE: Titolari e collaboratori condividono le stesse lacune sulle architetture digitali complesse.

Mentre il gestionale è padroneggiato, le tecnologie strategiche e la sicurezza rappresentano un territorio inesplorato.

+169% Aumento degli attacchi informatici in Italia nel 2024.

TOP 10 Gli Studi Professionali figurano tra le prime 10 tipologie di vittime.

Doppio rischio per Commercialisti e Consulenti:

- Gestione di dati ipersensibili (finanze, proprietà intellettuale, clienti).
- Assenza di reparti IT strutturati dedicati.


GDPR
Data Protection Officer (DPO)
Compliance
25 May 2018
Data Breaches
Personal Data


AI act
EU Artificial Intelligence Act



Considerando 6 Regolamento Ue 2016/679

"La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali."



*“la protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale”**

*Considerando 1 Regolamento Ue 2016/679

EU Artificial Intelligence Act

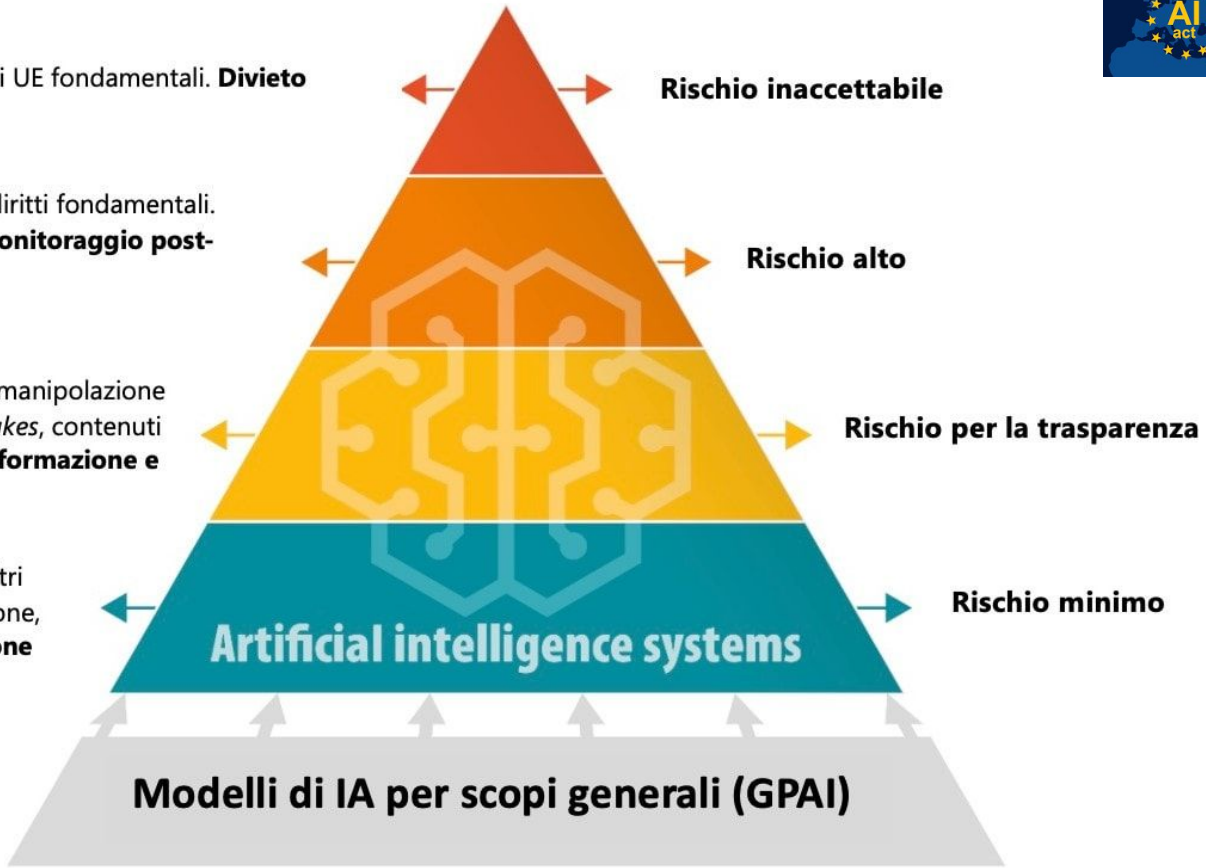
Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»)

Violazione dei diritti e dei valori UE fondamentali. **Divieto assoluto**

Impatto su salute, sicurezza o diritti fondamentali. **Valutazione di conformità, monitoraggio post-marketing, ecc**.

Rischio di impersonificazione, manipolazione o inganno (es. *chatbots*, *deep fakes*, contenuti generati dall'IA). **Obbligo di informazione e trasparenza**

Sistemi comuni di IA, ad es. filtri *spam*, sistemi di raccomandazione, ecc. **Nessuna regolamentazione specifica**



Modelli GPAI - Requisiti di trasparenza
GPAI con rischi sistemici - Requisiti di trasparenza, valutazione e mitigazione dei rischi

La nozione di «deployer» di cui al presente regolamento dovrebbe essere interpretata come qualsiasi persona fisica o giuridica, compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA sotto la sua autorità, salvo nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. A seconda del tipo di sistema di IA, l'uso del sistema può interessare persone diverse dal deployer.

- **DPIA (Data Protection Impact Assessment):** valutazione prevista dal GDPR per stimare i rischi privacy, verificare la proporzionalità del trattamento dei dati e identificare le misure di mitigazione necessarie.
- FRIA **(Fundamental Rights Impact Assessment):** valutazione introdotta dall'AI Act per analizzare l'impatto sui diritti fondamentali, come non discriminazione, libertà di espressione, equo processo, accesso a un rimedio effettivo.

Cosa possiamo fare nei nostri studi?

«dato personale»: *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente….*





Art. 4 comma 1 Regolamento 679/2016

*«**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;*



Art. 4 comma 2 Regolamento 679/2016

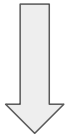


Interessato





«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;*





«responsabile del trattamento»: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali <u>per conto</u> del titolare del trattamento;*

Art. 28 - GDPR

Nomina con atto giuridico a norma

- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

- adotti tutte le misure richieste ai sensi dell'articolo 32;

- assista il titolare del trattamento con misure tecniche e organizzative adeguate,

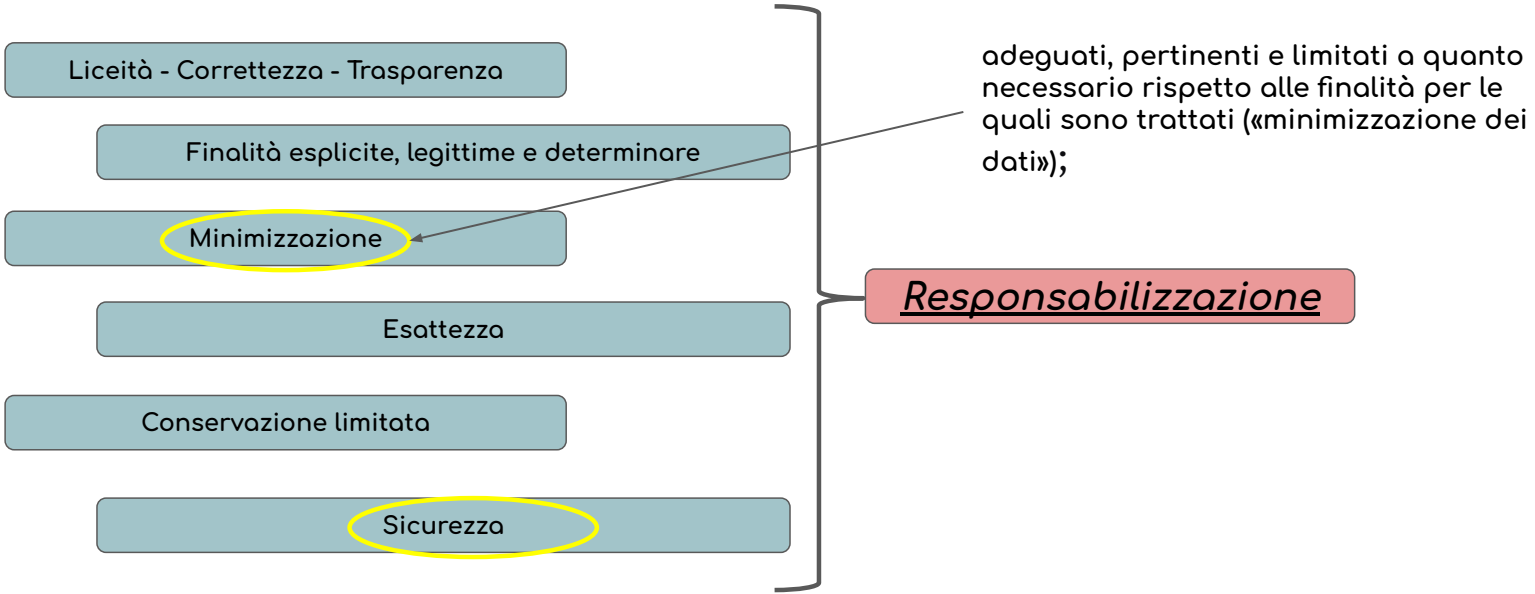
- su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi

- metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi il responsabile deltrattamento

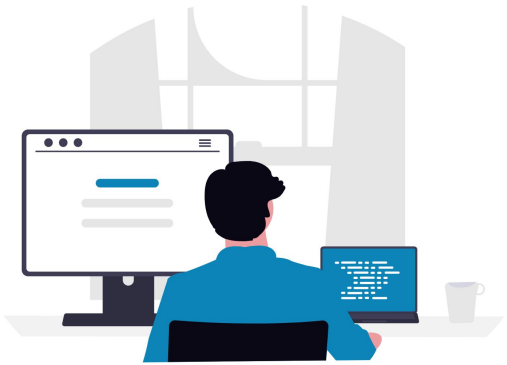
- informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.



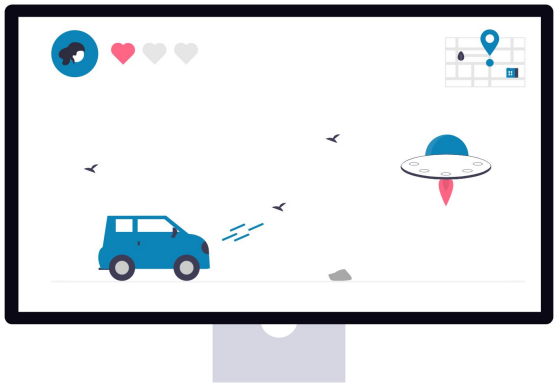
Art. 5 - Principi alla base del Trattamento dei dati personali



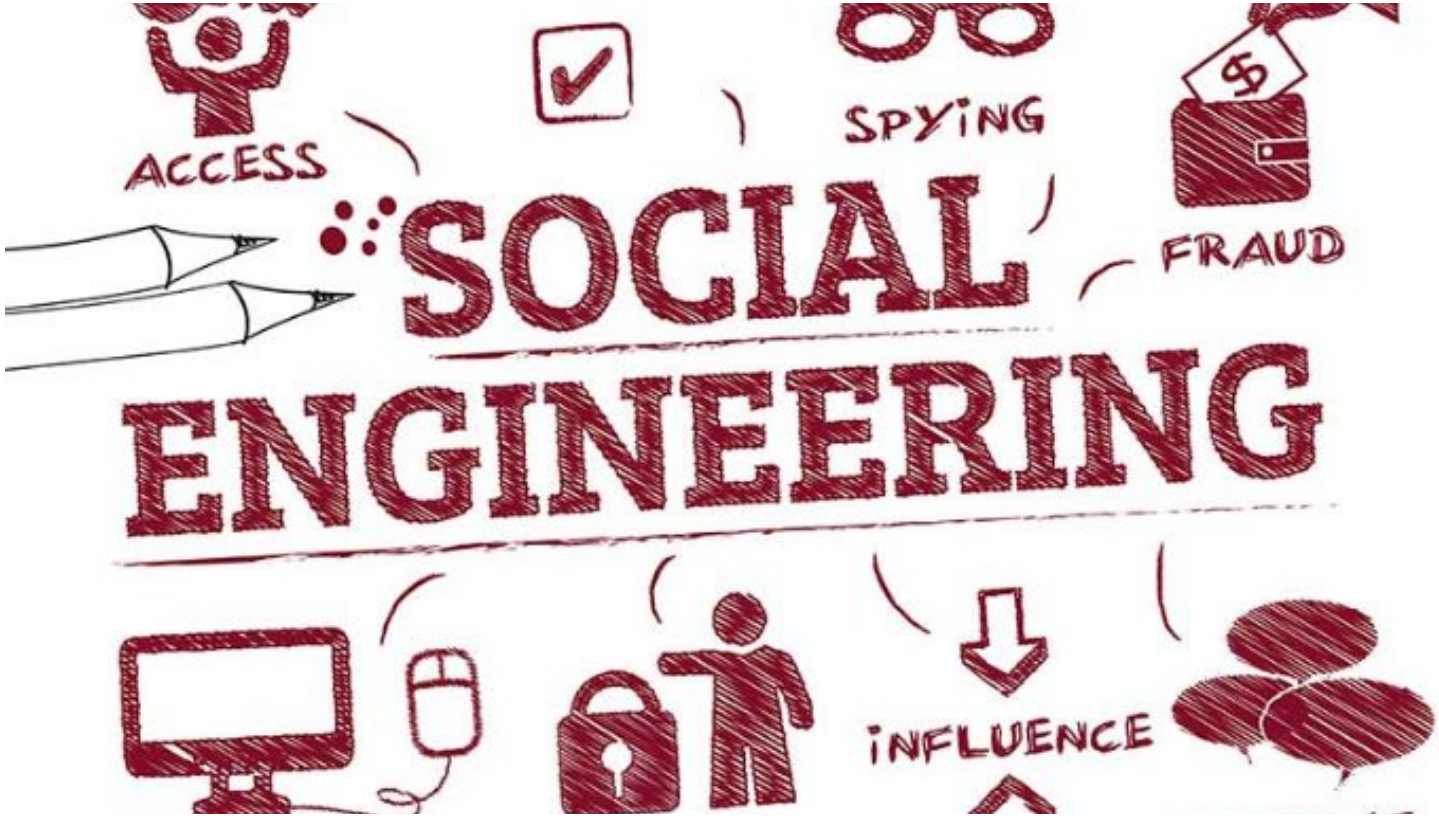
Quali piccole regole adottare?



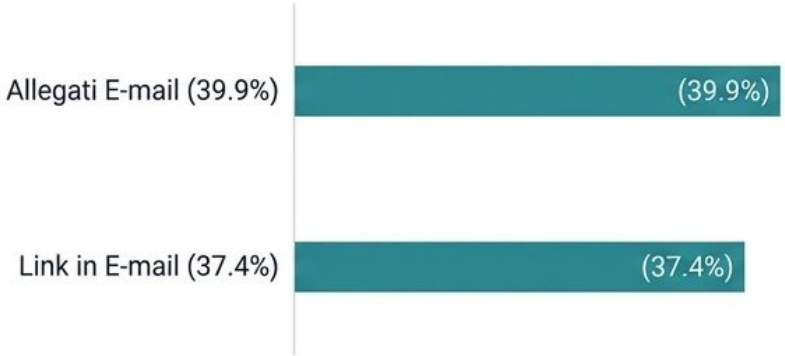
≠




Prestare attenzione


ACCESS
SPYING
FRAUD
SOCIAL
ENGINEERING
INFLUENCE

STATISTICHE DEGLI ATTACCHI



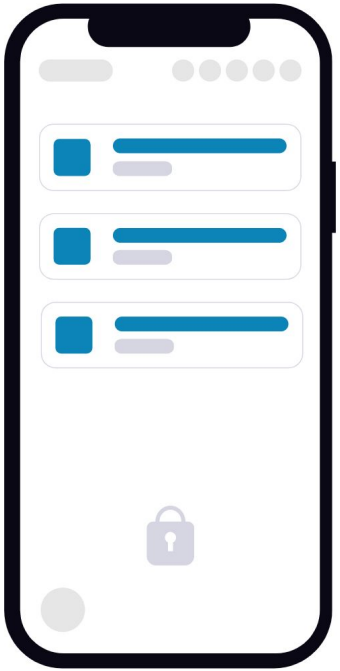
INGEGNERIA SOCIALE: MECCANICA



Il firewall più importante non è un software,
ma l’attenzione critica del professionista e del suo team.

Qualche regola*:

1. Installare app solo da fonti attendibili
2. Non cliccare su link sospetti
3. Effettuare sempre il logout delle applicazioni
4. Non fidarsi di mail o sms che consigliano di installare applicazioni
5. Mantenere il sistema operativo aggiornato
6. Non fornire informazioni personali tramite mail e/o messaggi
7. Limitare l'invio di informazioni personali e dei clienti attraverso le app di messaggistica istantanea
8. Non utilizzare Wi-Fi pubblici per effettuare transazioni o scambio di dati
9. Eseguire il backup delle informazioni sul dispositivo
10. Cifrare i dispositivi



* Cybersecurity kit di sopravvivenza - Ed. goWare

Il Paradigma Zero-Click

A differenza delle truffe tradizionali, il codice malevolo si auto-esegue nel momento in cui il dispositivo elabora il file multimediale.





Schema dell'Incursione

Una sequenza automatizzata che trasforma la ricezione di un file nella completa duplicazione dell'identità.

1.

Infiltrazione: Ricezione silente del file immagine modificato.



2.

Esecuzione: Attivazione della vulnerabilità nella libreria.



3.

Estrazione: Furto della chiave privata crittografica.



4.

Clonazione: Autenticazione temporanea dell'attaccante.



Diagnostica della Compromissione

Il danno non si misura in Terabyte, ma nel furto chirurgico dell'identità crittografica.

Volume Accertato

Decine di account

(Attacchi mirati)

Asset Sottratto

Chiave Privata Crittografica



(Nessun leak di massa)

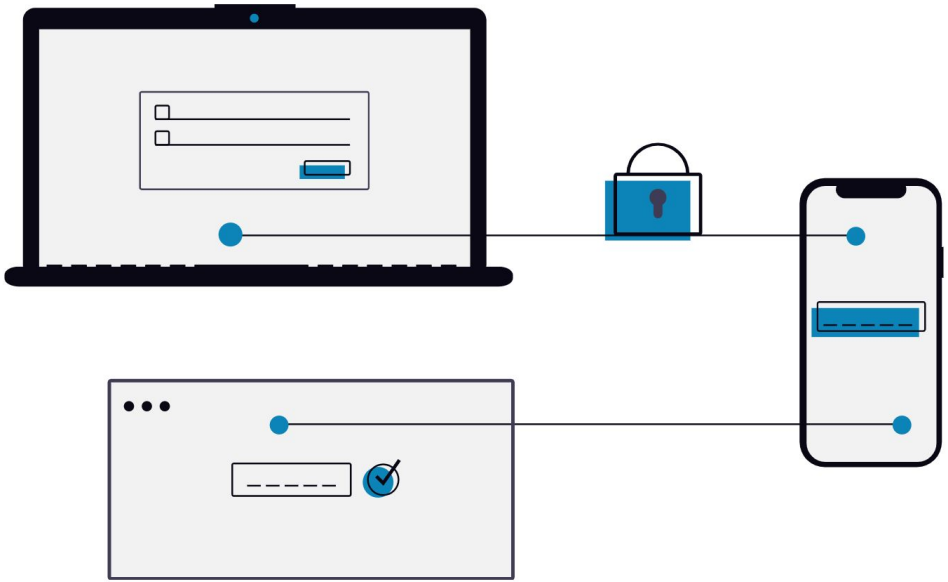
Risultato Finale

Clonazione dell'identità

(Frode ai contatti recenti)

Qualche regola*:

1. Evitare il social login
2. Costruire password forti
3. Sostituirla spesso, sempre diversa, lunga, mista, senza senso
4. Non salvare mai le password nel browser
5. Usare un password manager (es. last pass)
6. Usare l'autenticazione a due fattori



* Cybersecurity kit di sopravvivenza - Ed. goWare

L’importanza dei Backup

Es. Copia in locale -> Copia in un Nas
-> Copia offline o in remoto

Ripristino




AI

Matrice di Rischio: Consumer vs. Enterprise

	Soluzioni Consumer ⊗	Soluzioni Enterprise ✓
Addestramento Modelli	I dati immessi vengono usati per addestrare i modelli pubblici mondiali. ✗	I dati del cliente appartengono al cliente e NON addestrano modelli esterni. ✓
Privacy & GDPR	Nessuna garanzia sui flussi di dati transfrontalieri. ✗	Data Processing Agreement e conformità GDPR garantita. ✓
Certificazioni Sicurezza	Assenti o non verificabili per il singolo utente. ✗	Standard internazionali certificati (es. SOC 2, ISO 27001). ✓
Ritenzione Dati	Memorizzazione sui server a tempo indefinito. ✗	Policy di Zero-Retention disponibili e configurabili. ✓

Caratteristica	OpenAI (Enterprise/API)	Google (Workspace/Cloud AI)	Microsoft (Azure OpenAI)	Anthropic (Claude Enterprise)
Dati Utilizzati per Addestramento?	No, per impostazione predefinita	No, senza esplicito consenso	No, i dati non sono disponibili per OpenAI	No, per impostazione predefinita
Proprietà dei Dati	Il cliente possiede input e output	Il cliente possiede i propri dati	Il cliente mantiene il controllo sui propri dati	Il cliente mantiene il controllo sui propri dati
Controlli sulla Conservazione dei Dati	Sì, configurabili. Opzione ZDR per API	Sì, configurabili tramite console di amministrazione	Sì, integrati con le policy di Azure	Sì, configurabili. Opzione "zero-retention" disponibile
Standard di Crittografia	A riposo (AES-256) e in transito (TLS 1.2+)	A riposo e in transito, standard di settore	A riposo (AES-256) e in transito (TLS 1.2+). Opzione CMK	A riposo (AES-256) e in transito (TLS 1.2+)
Certificazioni Chiave	SOC 2, ISO/IEC 27001/27017/27018	SOC 1/2/3, ISO/IEC 27001/27701/27018	SOC 1/2/3, ISO/IEC 27001/27701/27018	SOC 2 Type II, ISO 27001
DPA per GDPR Disponibile?	Sì	Sì	Sì	Sì
Opzione Residenza Dati UE?	Sì, per clienti idonei	Sì, tramite opzioni di data residency	Sì, con EU DataZones per l'elaborazione esclusiva in UE	Sì, per l'elaborazione. L'archiviazione è negli Stati Uniti per impostazione predefinita

Framework di Analisi (I 6 Pilastri)

Parametri di **valutazione per la conformità** degli strumenti AI nello Studio.



Titolare del Trattamento
(Identity & Jurisdiction)



Dati Raccolti
(Input & Telemetry)



Conservazione
(Retention Policies)



Sicurezza
(Encryption & Architecture)



Sub-responsabili
(Third-party Ecosystems)



Diritti GDPR
(User Control & Compliance)

Parametro di Valutazione/AI	ChatGPT	Claude Sonet	Microsoft Copilot	Gemini
Chi è il titolare del trattamento?	OpenAI Ireland Limited	Anthropic Ireland Limited	Microsoft	Google LLC
Quali dati personali raccoglie?	Dati di contatto, input utente, informazioni social, dati di log e utilizzo, informazioni sul dispositivo, cookie	Dati di identità, informazioni di pagamento, input e output, feedback, informazioni tecniche	Contenuti Microsoft 365, richieste utenti, risposte generate, dati da plug-in di terze parti	Testi, comandi, dati di utilizzo, dati tecnici, dati biometrici
Quali sono le finalità del trattamento	Fornire servizi, migliorare i servizi, prevenire frodi, rispettare obblighi legali	Fornire servizi, comunicare con gli utenti, prevenire frodi, migliorare i servizi	Fornire funzionalità AI, migliorare i servizi, fornire informazioni più pertinenti	Rispondere a richieste, migliorare modelli, personalizzare esperienze
Rispetto dei requisiti dell'articolo 5 del GDPR	Non specificato in dettaglio	Non specificato in dettaglio	Conforme a GDPR, ma non specificato in dettaglio	Misure implementate, ma non descritte in dettaglio
Dove sono conservati i dati	Stati Uniti, condivisi con fornitori di servizi e affiliati in altre giurisdizioni	Stati Uniti o altri paesi al di fuori del SEE e Regno Unito	All'interno del perimetro Microsoft 365, con eccezioni per capacità	Non specificato

Parametro di Valutazione/AI	ChatGPT	Claude Sonet	Microsoft Copilot	Gemini
Tempi di conservazione	Variabile, in base a finalità e impostazioni utente come disattivazione cronologia	Tempo ragionevolmente necessario per le finalità descritte	Non specificato, criteri impostati dagli amministratori con Microsoft Purview	Variabile in base alla finalità, non specificato
Misure di sicurezza adottate	Misure tecniche, amministrative e organizzative	Misure tecniche, amministrative e organizzative	Crittografia, sicurezza fisica, isolamenti logici	Crittografia, controllo accessi, monitoraggio continuo
Nomina di eventuali sub responsabili e/o responsabili esterni	Fornitori di servizi di hosting, sicurezza, marketing	Affiliate, fornitori di servizi, partner commerciali	Non specificato, ma include plug-in di terze parti	Sub-responsabili con accordi di protezione dati
Rispetto dei diritti degli interessati indicati nel GDPR	Accesso, rettifica, cancellazione, limitazione, opposizione, portabilità, reclamo	Accesso, rettifica, cancellazione, limitazione, opposizione, portabilità, revoca consenso	Non specificato in dettaglio, soggetto ai diritti GDPR	Accesso, rettifica, cancellazione, opposizione

Il Cuore Giuridico (GDPR): Le Due Strade



Anonimizzazione (Il Gold Standard)

Meccanismo: Irreversibile. Impossibile re-identificare il soggetto.

Impatto Legale (Considerando 26): Il dato cessa di essere personale. Il GDPR NON si applica più.



Pseudonimizzazione

Meccanismo: Reversibile. I dati sono mascherati, ma esiste una chiave conservata separatamente per re-identificarli.

Impatto Legale (Art. 4(5)): L'identificazione è ancora possibile. Il GDPR si applica integralmente.

Perché l'Anonimizzazione Cambia le Regole del Gioco



Basi Giuridiche

Nessuna necessità di basi giuridiche complesse o DPA aggiuntivi per la condivisione.

Trasferimento Dati

Risolve radicalmente il problema del trasferimento dati fuori dallo Spazio Economico Europeo (Extra-UE).

Gestione del Rischio

Azzera l'esposizione dello studio a data breach derivanti dall'uso di tool AI di terze parti.

Anatomia di un Flusso di Lavoro Sicuro (Testo)



Input

Il documento originale grezzo entra nel sistema.

Motore NLP

Il tool (es. MS Presidio) scansiona e identifica le PII.



Sostituzione

I dati sensibili vengono oscurati con tag contestuali.

AI & Re-identificazione

Il testo sicuro viene inviato all'AI. Il professionista mappa l'output tramite un indice interno.

L'Ultimo Miglio: La Deontologia Digitale

Trasparenza

Comunicare l'uso dell'AI preferibilmente al momento dell'accettazione dell'incarico professionale (integrazione art. 21 Codice Deontologico).

Tracciabilità

Documentare internamente la tipologia di sistemi usati, le misure di riservatezza adottate e le modalità di verifica degli output.

Responsabilità Umana

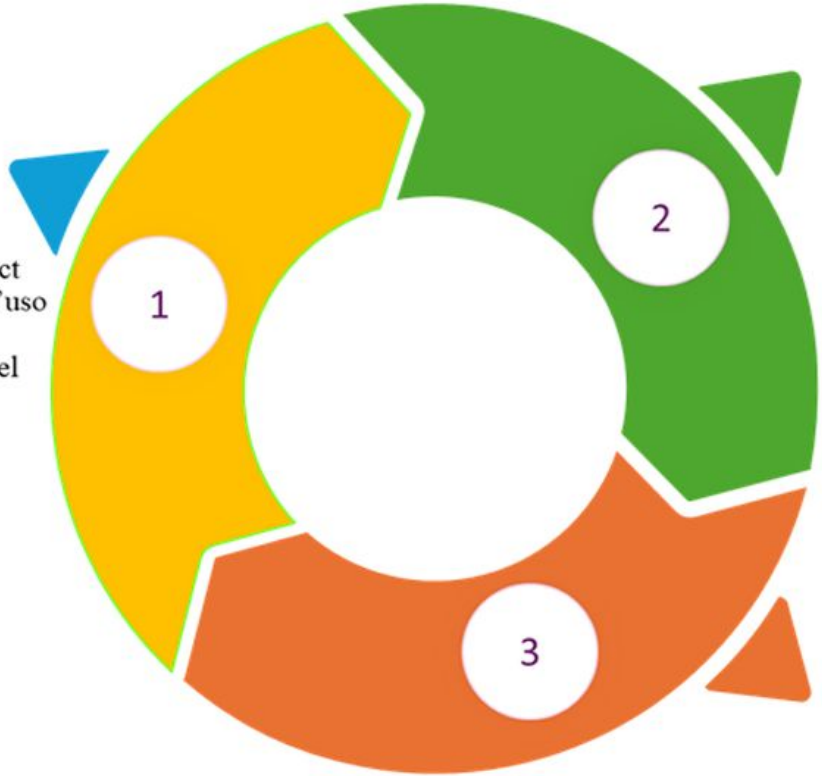
L'AI suggerisce, il commercialista decide. L'intuizione, il giudizio critico e l'empatia non sono delegabili all'algoritmo.

Ciclo di monitoraggio sistemi AI

Mappare l'uso dell'AI

Registro dei sistemi AI

1 - classificare in base al rischio AI Act
2 - documentarne finalità, modalità d'uso e processi coinvolti.
3- associare base giuridica (GDPR) nel caso di trattamento dei dati.



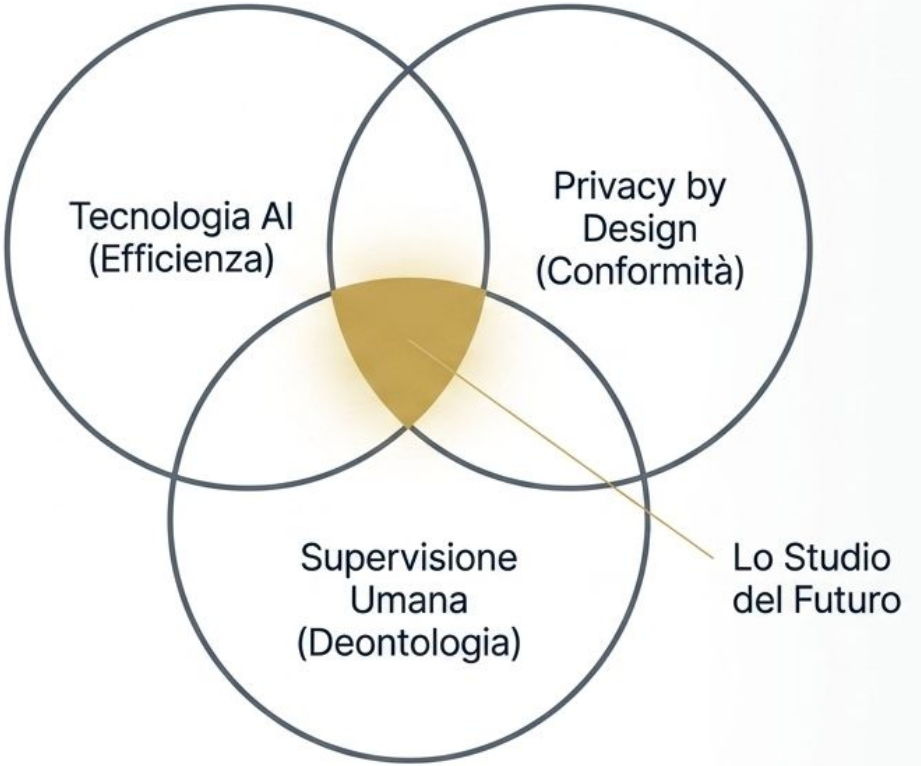
Valutazione operativa

- **DPIA** (Data Protection Impact Assessment): valutazione prevista dal GDPR per stimare i rischi privacy.
- **FRIA** (Fundamental Rights Impact Assessment): valutazione introdotta dall'Ai Act per analizzare l'impatto sui diritti fondamentali.

Monitoraggio continuo

- **Audit** periodici sui sistemi di AI.
- **Aggiornare** registro dei sistemi AI.
- **Formazione** obbligatoria e continua.

Sintesi Strategica: Il Vantaggio della Conformità



Rimanere passivi è un rischio.
L'adozione acritica è un pericolo.

L'implementazione proattiva, basata su infrastrutture sicure (Enterprise/Locali) e governance rigorosa, è il tratto distintivo dello Studio del Futuro.

L'AI amplifica le competenze del Commercialista; la governance dei dati ne protegge l'integrità.

Grazie per l’attenzione

Claudio Sica