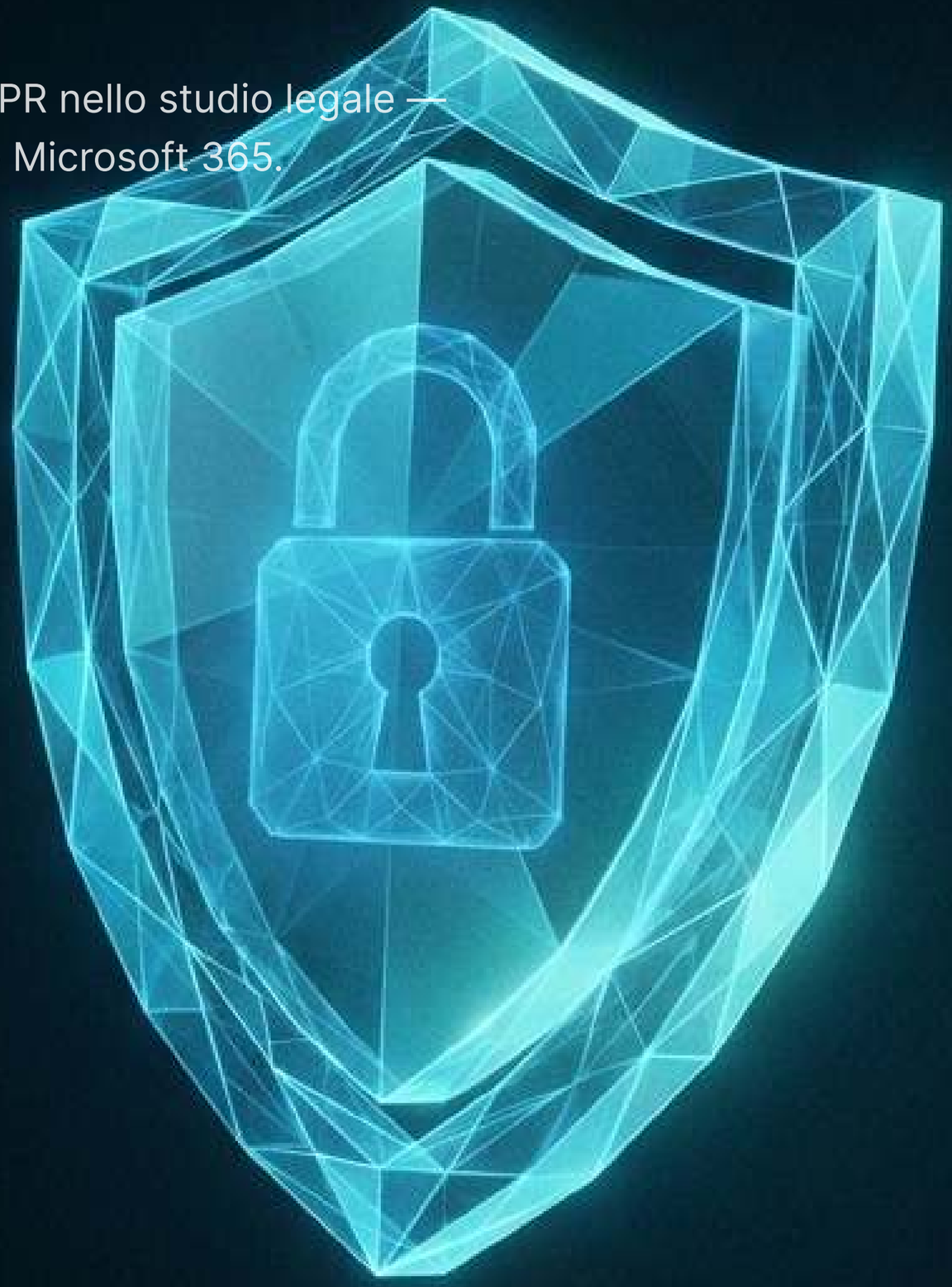
QUANTUM

IL GESTIONALE PER STUDI LEGALI

WHITEPAPER · SICUREZZA DATI & GDPR

Il segreto è anche digitale

Proteggere i dati dei clienti e rispettare il GDPR nello studio legale — tra minacce reali, Secure Score, Zero Trust e Microsoft 365.



A CURA DI
QUANTUM

quantum365.legal

In sintesi

Lo studio legale custodisce i dati più sensibili dei suoi clienti. Proteggerli non è solo un obbligo di legge: è il cuore del segreto professionale e della fiducia.

IL PROBLEMA

Gli studi sono bersagli di alto valore e spesso micro-strutture senza IT dedicato. Un solo data breach significa responsabilità verso i clienti, sanzioni del Garante e danno reputazionale.

COSA IMPARERAI

- ✓ Perché lo studio è titolare del trattamento
- ✓ Gli obblighi GDPR concreti (art. 30, 32, 33)
- ✓ Cosa fare nelle prime 72 ore di un data breach
- ✓ NIS2 e la sicurezza come requisito di filiera
- ✓ Una checklist allineata a Secure Score e Zero Trust

IL PUNTO

La sicurezza non è un prodotto da comprare una volta: è un insieme di misure e abitudini. Microsoft 365 le rende praticabili anche per un piccolo studio.

Il rischio è reale

Gli attacchi crescono e l'Italia è tra i Paesi più colpiti. Per chi custodisce dati riservati, non è una questione di "se", ma di "quando".

357

incidenti gravi in Italia

nel 2024 (+15,2%): l'Italia concentra oltre il 10% degli attacchi gravi mondiali.

4,44 M$

costo medio di un breach

a livello globale nel 2025; in media 241 giorni per identificarlo e contenerlo.

1 su 3

studi legali violati

ha già subìto una violazione (dato USA): molti non se ne accorgono nemmeno.

Fonti: Rapporto Clusit 2025 (incidenti Italia). IBM, Cost of a Data Breach Report 2025 (costo, tempi). ABA, Cybersecurity TechReport 2023 (studi violati, USA).

LO SAPEVI CHE

L'81% degli attacchi malware è ransomware: i dati vengono cifrati e tenuti in ostaggio. Per uno studio significa fascicoli bloccati e clienti esposti.

Come entrano

Le tecniche cambiano, l’obiettivo no: i tuoi dati. Tre porte d’ingresso da conoscere e chiudere.

Ransomware

81% del malware

Cifra i tuoi file e chiede un riscatto: archivi e fascicoli bloccati, attività ferma.

Phishing & credenziali

Il vettore #1

Email che rubano password e accessi. Una sola credenziale basta per entrare nel sistema.

Errore & insider

Il fattore umano

Un allegato inviato per errore, un portatile smarrito, un accesso mai revocato.

LA BUONA NOTIZIA

Una sola misura, l’MFA, blocca oltre il 99,9% degli attacchi automatizzati agli account.

Le prime 72 ore

Quando scatta una violazione, il GDPR impone tempi stretti. Ecco cosa fare, nell'ordine giusto.

1

Rilevi

Accesso anomalo, file cifrati, dati esposti: riconosci la violazione.

2

Documenti

Registri tutto nel registro delle violazioni (art. 33(5)).

3

Notifichi

Al Garante entro 72 ore, se c'è un rischio per le persone (art. 33).

4

Comunichi

Agli interessati, se il rischio è elevato (art. 34).

NON SOLO LA NOTIFICA

Servono comunque il registro dei trattamenti (art. 30) e le misure adeguate (art. 32). La mancata o tardiva notifica costa fino a 10 milioni di euro o il 2% del fatturato.

Nella filiera della sicurezza

La direttiva NIS2 (D.lgs. 138/2024) non include direttamente gli studi legali. Ma cambia comunque le regole del gioco.

NON SEI SOGGETTO DIRETTO

Fuori dagli allegati
Gli studi legali non rientrano nei settori regolati dalla NIS2.

Nessun obbligo diretto
Non devi registrarti sulla piattaforma ACN come soggetto essenziale.

MA SEI NELLA FILIERA

I tuoi clienti sì
Le aziende regolate devono gestire il rischio della loro catena di fornitura.

La sicurezza diventa requisito
Uno studio non sicuro è un rischio: e un fornitore meno affidabile.

La sicurezza informatica diventa un requisito competitivo per lavorare con i clienti più grandi.

La checklist della sicurezza

Otto misure allineate al Microsoft Secure Score e ai principi Zero Trust. Spunta quelle che hai già.

1. MFA su tutti gli account

E blocca l'autenticazione legacy: verifica esplicita.

2. Accessi con privilegio minimo

Ognuno vede solo i fascicoli e i dati che gli servono.

3. Cifratura di dati e supporti

A riposo, in transito e su chiavette esterne (art. 32).

4. Backup isolati e testati

Una copia offline è la difesa contro il ransomware.

5. Formazione anti-phishing

Ricorrente, per tutto lo studio: le persone sono il primo filtro.

6. Procedura data breach pronta

Rilevare, registrare e notificare entro 72 ore.

7. Registro dei trattamenti

Aggiornato, con la mappa dei dati art. 9 e art. 10.

8. Conservazione e cancellazione

Tempi definiti e cancellazione sicura dei dati non più utili.

Sicurezza che si attiva

Microsoft 365 traduce gli obblighi in misure tecniche concrete; Quantum centralizza i dati riservati dentro l'ecosistema.

ENTRA ID + MFA

Verifica esplicita

Identità e accessi protetti: l'MFA neutralizza oltre il 99,9% degli attacchi automatici.

MICROSOFT DEFENDER

Secure Score

Anti-phishing e anti-malware, con un punteggio che misura e fa crescere la postura.

MICROSOFT PURVIEW

Dati protetti

Classificazione, etichette e DLP per non far uscire i dati sensibili (anche on-prem).

QUANTUM + SHAREPOINT

Fascicoli al sicuro

Dati riservati centralizzati con permessi e versioning, anche on-premises.

QUANTUM

PRENOTA UNA DEMO

Metti in sicurezza il tuo studio

Ti mostriamo come proteggere dati e fascicoli sull'ecosistema Microsoft 365: identità, Secure Score, backup e archiviazione sicura, anche on-premises.

PRENOTA UNA DEMO →

CONTATTI

quantum365.legal

info@quantum365.legal

+39 02 29521765

Viale Gran Sasso 10, Milano

Inquadra per il sito

FONTI

GDPR Reg. UE 2016/679 · Rapporto Clusit 2025 · IBM Cost of a Data Breach 2025 · ABA Cybersecurity TechReport 2023 · NIS2 D.lgs. 138/2024 · Microsoft (Secure Score, Zero Trust) · Garante Privacy.