Convegno Associazione ICT Dott. Com
in collaborazione con Confprofessioni

Governance digitale sostenibile: dalle policy alle prove

le nostre riflessioni

LE NOSTRE RIFLESSIONI

TAVOLO CONGIUNTO «PROTEZIONE DEI DATI PERSONALI – GDPR» ORDINI PROFESSIONALI

COMMERCIALISTI, AVVOCATI ED INGEGNERI

ORDINI DI TORINO

PAOLA ZAMBON – DOTTORE COMMERCIALISTA - REFERENTE GDPR ORDINE COMMERCIALISTI

CLAUDIO STRATA – AVVOCATO – REFERENTE GDPR ORDINE AVVOCATI

PAOLO TRAVERSA - INGEGNERE - REFERENTE GDPR ORDINE INGEGNERI

Politecnico di Torino – 6 novembre 2026

Tavolo congiunto GDPR ordini professionali di Torino

Gli Ordini dei **Dottori Commercialisti** ed Esperti Contabili, degli **Avvocati** e degli **Ingegneri** di Torino,

hanno lavorato assieme per affrontare al meglio il cammino verso il GDPR



Un supporto per le nostre Categorie

- Evidenziare l'importanza della norma sensibilizzando in particolare sugli effetti della «responsabilizzazione»
- Informare e formare i Professionisti nei propri studi professionali
- Offrire spunti utili per impostare i propri lavori e suggerimenti applicativi
- Invitare i colleghi che hanno maturato esperienza in materia di protezione dei dati personali a proseguire nella loro attività dedicando una particolare attenzione all'auto-formazione
- Essere di riferimento verso le Autorità competenti

Attività svolta dal Tavolo congiunto GDPR

PRIMA DELL'ENTRATA in piena applicazione del GDPR:

autunno 2017: incontri di studio e pianificazione eventi

19/02/2018: inviata circolare agli iscritti relativa alle novità contenute nel GDPR e check list per gli studi professionali

12/03/2018: convegno presso il Tribunale di Torino con la spiegazione dell'utilizzo della checklist ed altri suggerimenti operativi

DOPO L'ENTRATA in piena applicazione del GDPR:

14/06/2018: convegno presso il Tribunale di Torino dal titolo "GDPR e nuova normativa italiana: riflessi su professionisti e PMI".

23/11/2018: convegno Associazione ICT Dott.Com – Politecnico di Torino: nostre interpretazioni operative

24/05/2019: Convegno presso il Tribunale di Torino "Privacy: il GDPR un anno dopo"

22/11/2019: convegno Associazione ICT Dott.Com – Politecnico di Torino: nostre riflessioni

22/06/2020: convegno «ODV e privacy: aggiornamenti al tempo del COVID» (online)

20/11/2020: convegno Associazione ICT Dott.Com – Politecnico di Torino: nostre riflessioni

14/05/2021: Webinar «Data breach: prevenire è meglio che curare»

18/11/2022: convegno «Equità e sostenibilità: una necessaria trasformazione antropocentrica dell'impresa - Dati personali e non - novità normative per le imprese e GDPR"

20/11/2023: convegno «Impresa f.o.r.t.e.»

14/11/2025: convegno «Più forte di ogni dipendenza»



IL CASO ANALIZZATO

Il Garante per la protezione dati personali ha sanzionato una società di consulenza il cui data breach subito ha provocato la perdita di disponibilità e riservatezza dei dati personali di un numero esteso e non determinabile di interessati



Provvedimento n. 529 del 14 luglio 2026

LA VIOLAZIONE NON POTEVA CONSIDERARSI IMPREVEDIBILE O INEVITABILE SECONDO IL GARANTE

Area	Situazione emersa nell'istruttoria
Accesso remoto	La MFA era attiva soltanto per alcune utenze Microsoft 365 e non per la VPN aziendale.
Credenziali	Il blocco dopo dieci tentativi falliti durava cinque minuti; mancavano controlli specifici contro il riuso di credenziali sottratte.
Rete e privilegi	La segmentazione non ha impedito il movimento laterale fino a sistemi critici.
Backup	Uno storage è stato compromesso; dall'altro erano recuperabili copie risalenti a circa due mesi prima.
Vulnerabilità	Il processo di gestione risultava parziale e non formalizzato.

L'attacco aveva sfruttato carenze per le quali erano disponibili misure di contrasto comuni

L'IMPATTO SULL'IMPRESA: DALLA POLICY ALLE PROVE

Il Garante, durante l'istruttoria, aveva chiesto **«elementi certi» sulle specifiche misure di sicurezza presenti al momento della violazione**.

L'impresa deve poter ricostruire **lo stato dei controlli effettuati ad una certa data** oltre a descrivere la propria **policy** o mostrare le misure introdotte dopo l'incidente.

COSA CONSERVARE?

Un sistema documentale dovrebbe conservare, **in modo proporzionato al rischio:**

- **versioni datate delle configurazioni effettuate**,
- cronologia delle modifiche,
- log pertinenti,
- risultati delle scansioni,
- esiti dei backup e
- prove periodiche di ripristino

unitamente a correlate valutazioni del rischio, decisioni sulle eccezioni e responsabilità assegnate, (compreso, se vi è IA, traccia di interventi umani, casi d'uso, dati inviati, output rilevanti), incidenti e cambi di fornitore

IL TITOLARE DEVE DIMOSTRARE L'ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

D.Lgs. 160/2026, entrato in vigore il 30 settembre 2026

- **art. 17:** esibizione giudiziale di prove pertinenti
- **art. 18**: introduce una presunzione *superabile con prova contraria* del nesso tra violazione di uno o più obblighi dell'AI Act ed il danno
- **art. 19**: la conformità del sistema, anche certificata, non esclude di per sé la responsabilità del convenuto

L'onere di dimostrare l'adeguatezza è posto su chi il sistema lo usa con documenti probatori oggettivi

RIFLESSIONI SULLA GOVERNANCE SOSTENIBILE DIGITALE

Un'infrastruttura digitale aziendale è **sostenibile** se l'organizzazione sa **mantenerla, ripristinarla e rendere conto delle sue scelte nel tempo**

- l'impresa deve saper mantenere sicuri i propri sistemi, ripristinare i servizi dopo un incidente e documentare quali controlli erano effettivamente attivi nel tempo.
- la continuità dei servizi e la protezione dei dati dei clienti dipendono da decisioni di architettura, investimenti e verifiche periodiche effettuate.
- l'incidente di un fornitore può coinvolgere molti titolari contemporaneamente dunque occorre valutare con attenzione
- necessario valutare gli investimenti in controlli rispetto al danno che una perdita di dati può produrre anche nell'ottica di garantire una governance sostenibile. Per ciascun controllo critico scrivere: configurazione attesa, sistemi interessati, proprietario, frequenza della verifica e fonte tecnica dell'evidenza



Il «tavolo di lavoro congiunto GDPR»
dei nostri Ordini Professionali
è al fianco dei colleghi.

GRAZIE

PAOLA ZAMBON – DOTTORE COMMERCIALISTA - REFERENTE GDPR ORDINE COMMERCIALISTI

CLAUDIO STRATA – AVVOCATO – REFERENTE GDPR ORDINE AVVOCATI

PAOLO TRAVERSA - INGEGNERE - REFERENTE GDPR ORDINE INGEGNERI