Progettato e realizzato da

Commissionato da

UNIVERSITÀ DEGLI STUDI DI TORINO

CORSO GDPR - Regolamento UE 2016/679 - e sicurezza informatica

commissionato da Università degli Studi di Torino

realizzato e progettato da CSI Piemonte

Modulo 1 – Controlli

Sommario

Obiettivi 2

Certificazioni e codici di condotta 2

Audit 2

Sanzioni 3

Conclusioni 4

Obiettivi

In questa quarta ed ultima sezione dedicata alle novità del GDPR – ambito di intervento **Controlli** – analizziamo le seguenti tematiche:

- ✓ **Certificazioni e codici di condotta**
- ✓ **Audit**
- ✓ **Sanzioni**

Torna al sommario

Certificazioni e codici di condotta

Il Regolamento promuove il ricorso a codici deontologici da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione delle DPA ed eventualmente della Commissione (in tal caso, il codice deontologico avrà applicazione nell'intera UE).
Il Regolamento introduce la possibilità per il titolare di far **certificare i propri trattamenti**, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi; **la certificazione può essere rilasciata da un soggetto a ciò abilitato ovvero dall'Autorità garante.**
I Garanti dovranno tenere conto dell'adesione a codici deontologici e/o schemi di certificazione nel valutare eventuali violazioni del Regolamento da parte di un titolare e, più in generale, nell'analizzare i risultati della valutazione di impatto condotta da un titolare.

Torna al sommario

Audit

Il titolare del trattamento deve **verificare regolarmente** l'efficacia delle misure tecniche ed organizzative al fine di **garantire la sicurezza del trattamento** e dimostrare il rispetto delle norme del Regolamento Europeo.

Torna al sommario

Sanzioni

Nel GDPR la **parte sanzionatoria** occupa, per l'interesse dei Titolari, un posto sicuramente di rilievo e stabilisce le **sanzioni amministrative massime**, rinviando alle norme degli stati membri la definizione:

- ✓ delle sanzioni minime per le violazioni amministrative
- ✓ delle pene per gli illeciti penali

Sia *le sanzioni massime che le minime devono essere effettive, proporzionate e dissuasive (art. 84).*

Sono soggette a **sanzioni amministrative fino a 10 milioni di euro, o in caso di un'impresa, fino al 2% del fatturato totale annuo mondiale** dell'esercizio precedente, se superiore, le violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile di cui agli articoli:

- ✓ **8** (consenso dei minori),
- ✓ **11** (trattamenti che non richiedono l'identificazione degli interessati),
- ✓ **25 (privacy by design e privacy by default),**
- ✓ **26** (cotitolarità del trattamento),
- ✓ **27** (nomina rappresentante del Titolare non stabilito nell'Unione Europea),
- ✓ **28 (Responsabili del trattamento),**
- ✓ **29** (istruzioni per chi tratta i dati),
- ✓ **30 (Registro dei trattamenti),**
- ✓ **31** (cooperazione con l'autorità di vigilanza),
- ✓ **32 (sicurezza del trattamento),**
- ✓ **33** (notificazione dei **data breach** all'autorità),
- ✓ **34** (comunicazione dei data breach agli interessati),
- ✓ **35 (DPIA – Data Protection Impact Assessment),**

- ✓ **36** (consultazione preventiva),
- ✓ **37, 38 e 39 (designazione, posizione e compiti del DPO – Data Protection Officer),**
- ✓ **42 e 43 (processi di certificazione).**

Sono soggette a **sanzioni amministrative fino a 20 milioni di euro, o in caso di un'impresa, fino al 4% del fatturato totale annuo mondiale** dell'esercizio precedente, se superiore, le violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile di cui agli articoli:

- ✓ **5, 6 ,7 e 9 (principi base del trattamento),**
- ✓ **da 12 a 22 (diritti degli interessati),**
- ✓ **da 44 a 49** (trasferimento verso paese terzo),

Qualsiasi obbligo del capo IX (specifiche situazioni di trattamento: libertà d'espressione e di informazione, accesso del pubblico a documenti ufficiali, trattamenti di dati nell'ambito del rapporto di lavoro, trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, obblighi di segretezza).
Inosservanza di un ordine dell'Autorità di controllo.

Il "costo" di una mancata compliance normativa è quindi destinato a salire notevolmente.

Torna al sommario

Conclusioni

Molto bene! Hai concluso tutte le sezioni dedicate alla normativa e alle novità introdotte dal GDPR.
Prosegui con il corso, puoi ora affrontare la parte tecnica dedicata alla Sicurezza.

Torna al sommario