



<http://creativecommons.org/licenses/by/4.0/deed.it>

Certificazioni e codici di condotta GDPR: come si sta procedendo?

13 novembre 2021

Chiariamoci!

- Questa presentazione è stata ampliata con il contributo degli Idraulici della privacy in occasione dell'incontro del 13 novembre 2021.



Certificazioni in Italia

- Certificazione ISO/IEC 27701: attivo l'accREDITamento Accredia (e non solo), ma non aderente agli art. 42 e 43 del GDPR perché di sistema di gestione.
- Certificazione di prodotto UNI/PdR 43 «Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR)», accreditata da Accredia, ma non dal Garante.
- Certificazione di prodotto ISDP 10003 «Schema per la protezione dei dati personali», accreditata da Accredia, ma non dal Garante.



Codici di condotta in Italia

- Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali – approvato dal Garante il 29 aprile 2021.
 - > l'11 febbraio 2021, il Garante ha accreditato «l'Odm preposto da ANCIC» (notare la data e l'assenza di denominazione dell'Odm).
- Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti – Approvato il 19 settembre 2019 (ma non sembra sia stato approvato alcun Odm).
- Regione Veneto - Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica (pubblicato sul sito del Garante il 14 gennaio 2021, ma non sembra approvato).
- In fase di presentazione (novembre 2021) al Garante un codice di condotta per i fornitori di cloud SaaS.



Certificazioni all'estero

- Non sembra (tranne la ISO/IEC 27701, con i limiti già citati) siano state approvate almeno in Europa.
- Certificazioni in Germania e in Francia valide in precedenza non sembra siano state approvate dalle DPA o da EDPB.
- Il progetto di «recepimento europeo della ISO/IEC 27701 per usarla con gli art. 42 e 43 del GDPR» è naufragato (le virgolette sono poste perché il titolo riassume un concetto piuttosto ampio).
- Il progetto di «recepimento europeo della Pdr 43» è in fase di conclusione e verrà esteso oltre l'ICT.



Codici di condotta in Europa

- Il CISPE Code of Conduct (<https://www.codeofconduct.cloud/>), per i fornitori cloud di IaaS, è stato approvato da EDPB il 19 aprile 2021.
 - > Il CNIL ha approvato ad oggi 3 Odm (EY, BV e LNE):
<https://www.cnil.fr/fr/recherche/cispe>.
- L' EU Cloud Code of Conduct (<https://eucoc.cloud/>) è stato approvato da EDPB il 19 aprile 2021, ma non sembrano essersi attivati Odm.
- Notare che per ambedue è stato indicato che «this code does not aim to be used as a tool for international transfers” (https://edpb.europa.eu/our-work-tools/our-documents/minutes/49th-plenary-meeting-remote_en).





FINE

