Prot. DC2018SSV397 Milano, 12-12-2018

A tutti gli Organismi di Certificazione accreditati UNI CEI EN ISO/IEC 17065:2012

Responsabile di schema

Alle Associazioni degli organismi di valutazione della conformità

Loro Sedi

Oggetto: **Dipartimento DC - Circolare informativa N° 21/2018**
Prescrizioni per l'accreditamento ISO/IEC 17065 di Organismi operanti le certificazioni per la protezione e valutazione di conformità dei dati personali in ambito ICT, in accordo alla prassi di riferimento UNI/PdR 43.2:2018

Premessa
Si ricorda in premessa a questo documento il comunicato stampa congiunto pubblicato da Accredia e il Garante Privacy in data 18 luglio 2017.
Si riporta di seguito uno stralcio del comunicato Stampa.
In particolare ACCREDIA e il Garante per la protezione dei dati personali ritengono necessario sottolineare - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - che al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione.

Introduzione
Il 19 settembre scorso è entrato in vigore il Decreto Legislativo 101/2018 (GU n. 2015) che adegua il Codice in materia di protezione dei dati personali (D.Lgs. 196/2013) alle disposizioni del Regolamento UE 679/2016, il GDPR (General Data Protection Regulation) applicato nell'Unione Europea dal 25 maggio scorso.
L'obiettivo è assicurare la libera circolazione dei dati personali tra Stati membri e quindi la tutelare i diritti e le libertà fondamentali delle persone fisiche.
Oggetto della nuova normativa, la protezione dei dati delle persone fisiche e le regole per il loro trattamento da parte di soggetti terzi. In particolare, sono definite le responsabilità e le sanzioni per attività come raccolta, conservazione, uso, modifica e diffusione dei dati personali. Inoltre sono disciplinate le garanzie dei sistemi di protezione e le autorità di controllo.
Inoltre, la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La diffusione di carte di credito, carte di debito e sistemi di pagamento elettronico ha reso più facile la raccolta d'informazioni sulla vendita. Inoltre, fatto più significativo, la velocità e il volume degli acquisti e la correlazione tra diverse informazioni è cresciuta in maniera esponenziale

Prassi di Riferimento UNI/PdR 43:2018
La Prassi di Riferimento UNI/PdR 43:2018 "Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR)" è stata elaborata dal Tavolo "Processi di gestione privacy in ambito digitale", sotto il coordinamento di UNINFO, Ente Federato all'UNI, che lavora nell'ambito delle tecnologie informatiche e delle loro applicazioni.
La prassi di riferimento si compone di due sezioni:

- UNI/PdR 43.1 "Gestione e monitoraggio dei dati personali in ambito ICT"
- UNI/PdR 43.2 "Requisiti per la protezione e valutazione di conformità dei dati personali in ambito ICT"

Sede operativa e amministrativa: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Sede legale: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | Partita IVA - Codice Fiscale 10566361001

La sezione 1 fornisce le linee guida per la definizione e attuazione dei processi afferenti al trattamento dei dati personali, mediante strumenti elettronici (ICT), secondo il Regolamento Europeo 679/2016 (GDPR) e la normativa vigente.
La sezione 2 fornisce un adeguato insieme di requisiti che permetta alle organizzazioni, in particolare alle PMI, di essere conformi a quanto previsto dal quadro normativo europeo e nazionale in modo efficace, potendo dimostrare tale conformità ed efficacia anche attraverso un percorso di certificazione.
Solo la UNI/PdR 43.2 può essere usata attività di certificazione.
La prassi di riferimento è scaricabile mediante dal Catalogo online all'interno dell'area UNI Store.

Contesto normativo
A titolo esemplificativo ma non esaustivo si citano alcune leggi e regolamenti vigenti in Italia:

- DIR 95/46/CE;
- D.LGS. 196/03;
- provvedimenti generali Autorità Garante;
- EU Reg. 679/2016;
- decreto legislativo n. 101 del 10 agosto 2018

Processo di Accreditamento
Condizione essenziale per l'accreditamento degli Organismi è il possesso del livello adeguato di competenze riguardo alla protezione dei dati personali.
Si potranno presentare diverse casistiche, in base agli accreditamenti ACCREDIA già posseduti dall'Organismo di Certificazione che presenta la domanda di accreditamento o estensione.
Rimangono invariati i prerequisiti previsti dal RG-01 ed RG-01-03 per la concessione dell'accreditamento ed estensione.
Per organismi già accreditati ISO/IEC 17065, non occorre che questi abbiano già rilasciato dei certificati n questo schema per presentare domanda di estensione dell'accreditamento.
Nel caso in cui l'OdC possegga già accreditamenti rilasciati da altri enti di accreditamento, dovrà essere eseguita una valutazione caso per caso, in base agli accordi EA / IAF MLA applicabili.
Il certificato di accreditamento non riporta settori di accreditamento

OdC già accreditato per lo schema UNI CEI EN ISO/IEC 17065:2012 in uno schema in ambito GDPR	Esame documentale di 0,5 giorni (da svolgersi possibilmente presso l'OdC). 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
OdC già accreditato per lo schema UNI CEI EN ISO/IEC 17065:2012, ma non in uno schema in ambito GDPR	Esame documentale di 1 giorno (da svolgersi possibilmente presso l'OdC). 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
OdC non ancora accreditato UNI CEI EN ISO/IEC 17065:2012, ma accreditato per altri schemi di accreditamento	Esame documentale di 1 giornata. Verifica ispettiva presso la sede dell'OdC di 2 giornate. 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
OdC non ancora accreditato in nessuno schema	Esame documentale di 1 giornata. Verifica ispettiva presso la sede dell'OdC di 4 giornate.

	1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.

Documentazione da presentare ad ACCREDIA per l'esame documentale:
Criteri di qualifica di chi svolge il riesame del contratto, degli auditor e dei Decision Maker;
Curricula degli ispettori e dei Decision Maker e giustificazione per la loro singola qualifica;
Procedura per la costituzione e gestione dei Gruppi di Audit;
Attestato/Certificato rilasciato dall'OdC;
Lista dei certificati già emessi, e delle prossime attività di verifica (dato necessario per poi pianificare la verifica in accompagnamento);
Procedure / regolamenti contrattuali applicabili alla verifica, nonché le procedure interne per la gestione della pratica di certificazione (dall'offerta alla Certificazione);
Per gli OdC NON accreditati UNI CEI EN ISO/IEC 17065:2012, oltre ai documenti sopra riportati, occorre inviare la documentazione richiesta nella domanda di accreditamento.

Mantenimento dell'Accreditamento
Per il mantenimento dell'accreditamento, durante l'intero ciclo di accreditamento, salvo situazioni particolari (Es: gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo…), verranno condotte le seguenti verifiche:

- se l'OdC ha emesso meno di 50 certificati nello schema di certificazione, devono essere effettuate una verifica in accompagnamento e una verifica in sede;
- se l'OdC ha emesso tra 51 e 200 certificati nello schema di certificazione, devono essere effettuate 2 verifiche in accompagnamento e 1 verifica in sede;
- se l'OdC ha emesso più di 201 certificati nello schema, devono essere effettuate 2 verifiche in accompagnamento e 2 verifiche in sede.

Siamo a disposizione per chiarimenti e con l'occasione porgiamo cordiali saluti.

Dott. Emanuele Riva
Direttore Dipartimento
Certificazione e Ispezione