

A tutti gli Organismi di Certificazione e Ispezione accreditati e accreditandi in Italia

Loro sedi

Ns. rif.: DC2016SSV274

Milano, 14/09/2016

Oggetto: Dipartimento Certificazione e Ispezione Accredia - Circolare N° 23/2016 Informativa in merito all'accreditamento prodotto (ISO/IEC 17065) delle certificazioni rilasciate in conformità allo schema ISDP 10003:2015 - Criteri e regole di controllo per la Certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali - Reg. EU 679/2016

Introduzione

La direttiva 95/46/CE del Parlamento Europeo e del Consiglio, aveva ed ha come obiettivo l'armonizzazione dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati. Il diritto alla protezione dei dati va considerato uno dei diritti fondamentali degli individui, nel rispetto del principio di proporzionalità. Per assicurare un livello coerente di protezione dei dati personali, certezza del diritto e trasparenza per gli operatori europei, il Parlamento europeo ed il Consiglio hanno adottato un nuovo regolamento **EU 679/2016** entrato in vigore dal 25 maggio 2016, ma pienamente operativo solo dal 25 maggio 2018.

PsFeA Srl, Organismo di certificazione accreditato da ACCREDIA a fronte della 17065:2012 per lo schema SGCMF 10002:2013 per la certificazione della *data protection* in ambito sanitario e farmaceutico, ha adesso sviluppato uno nuovo schema, l'**ISDP 10003:2015**, applicabile a qualsiasi Titolare del trattamento, qualunque sia il settore di appartenenza ed a prescindere dal tipo di trattamento realizzato e che risponde ai requisiti previsti dal regolamento stesso sia in ambito nazionale che europeo.

PsFeA Srl è quindi il proprietario dello schema ISDP 10003:2015. Questo schema è già stato valutato con esito positivo da ACCREDIA, e può essere oggetto di accreditamento (ambito volontario) da parte di altri Organismi di Certificazione per lo schema ISO/IEC 17065.

Generalità

Lo schema di certificazione ISDP 10003:2015 risponde ai requisiti di cui agli art. 42 e 43 del Reg. 679/2016 ed è applicabile a tutte le tipologie di organizzazioni soggette alle norme vigenti in tema di **tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati**. Lo schema di certificazione specifica ai "Titolari" e "Responsabili" del trattamento, soggetti ai vincoli normativi vigenti nel territorio dell'EU, i requisiti necessari per la corretta valutazione della conformità alle norme stesse.

Va infine sottolineato che il meccanismo di certificazione, pur essendo non obbligatorio, viene richiamato come elemento per la dimostrazione della conformità utilizzabile dai titolari e responsabili ed è previsto fra le attenuanti in caso di sanzione (*ex art. 83 Reg. 679/2016*).

Può inoltre essere applicato ai Titolari o Responsabili di trattamenti di dati non soggetti ai vincoli normativi dell'EU, che necessitano di dimostrare la previsione di garanzie adeguate circa la conformità alle norme sul trattamento dei dati personali.

Lo schema valuta l'assenza di inadeguatezze procedurali che possano creare diseguaglianze o discriminazione negli individui oggetto del trattamento secondo i principi espressi dall'art. 8 paragrafo 1 della Carta dei diritti fondamentali dell'EU e l'art. 16 paragrafo 1 del Trattato di Lisbona.

Tale condizione deve passare attraverso il riordino dell'intero patrimonio informativo dell'organizzazione, supportato da una approfondita valutazione dei rischi e laddove necessario, conseguente valutazione d'impatto che il trattamento dei dati personali può comportare per i soggetti interessati.

Per ulteriori dettagli si rimanda al sito <http://www.pharmasoft-fea.com>

Contesto Normativo

Oltre allo Schema ISDP 10003:2015 che può essere usato ai fini certificativi, sono richiamati altri riferimenti normativi: Leggi, Provvedimenti e Regolamenti Europei

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 AUTORITA' GARANTE;
- EU Reg. 679/2016;
- EN ISO/IEC 17065:2012;
- EN ISO 19011:2012;
- REGOLAMENTO (CE) 765/2008.

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 requisiti 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 in questo schema per presentare domanda di estensione dell'accREDITamento.

Nel caso in cui l'OdC posseda 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.

L'Organismo di Certificazione <u>non</u> è accreditato	<ul style="list-style-type: none"> - Deve presentare domanda di accreditamento alla ISO/IEC 17065 al fine del rilascio di certificazioni ai sensi dello schema di certificazione ISDP 10003:2015 - Esame documentale della durata di 1 giornata - Verifica ispettiva presso la sede dell'Organismo di certificazione della durata di 4 giornate. - 1 Verifica in accompagnamento ISDP 10003:2015
L'Organismo di Certificazione è già accreditato da ACCREDIA, <u>ma non</u> ai sensi della ISO/IEC 17065	<ul style="list-style-type: none"> - Deve presentare domanda di accreditamento alla ISO/IEC 17065 al fine del rilascio di certificazioni ai sensi dello schema di certificazione ISDP 10003:2015 - Esame documentale della durata di 1 giornata - Verifica ispettiva presso la sede dell'Organismo di certificazione della durata di 2 giornate. - 1 Verifica in accompagnamento ISDP 10003:2015
L'Organismo di Certificazione è già accreditato da ACCREDIA ai sensi della ISO/IEC 17065	<ul style="list-style-type: none"> - Deve presentare domanda di estensione dell'accREDITamento alla ISO/IEC 17065 al fine del rilascio di certificazioni ai sensi dello schema di certificazione ISDP 10003:2015 - Verifica ispettiva presso la sede dell'Organismo di certificazione della durata di 1 giornata, comprensiva di esame documentale (svolto on site). - 1 Verifica in accompagnamento ISDP 10003:2015

Documentazione da presentare ad ACCREDIA per l'esame documentale

1. Lista di riscontro o linea guida o istruzioni predisposte dall'Organismo di Certificazione per il Gruppo di audit.
2. Curricula degli Ispettori e/o Esperti Tecnici.
3. Modulo del Rapporto di audit e relative check list.
4. Attestato/Certificato rilasciato dall'Organismo di Certificazione.
5. Lista dei certificati già emessi, e programmazione delle successive attività di audit.
6. Procedure/Regolamenti contrattuali applicabili all'audit, nonché le procedure interne per la gestione della certificazione.

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

Siamo a disposizione per eventuali chiarimenti.

Cordiali saluti.

Il Direttore di Dipartimento
Dr. Emanuele Riva

