A tutti gli Organismi di Certificazione accreditati ISO/IEC 17021

Vostra mail

Ns. rif.: DC2017SSV206 *Milano,* 21/07/2017

Oggetto: **Dipartimento Certificazione e Ispezione ACCREDIA - Circolare N° 13/2017**
Informativa in merito all'accreditamento per lo schema di certificazione ISO/IEC 27001:2013 con integrazione della linea guida ISO/IEC 27018:2014 - Information Technology, Security techniques, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Introduzione

Con la diffusione del cloud computing crescono le preoccupazioni dei clienti per la trasparenza, la riservatezza e il controllo sul servizio erogato: i clienti spesso non sono a conoscenza di come sono protette le informazioni archiviate nel cloud, dove sono localizzate e cosa succede nel caso in cui si volesse passare a un altro fornitore o il fornitore cessasse la propria attività.

Inoltre, in base alle norme vigenti, la responsabilità per la violazione delle norme sulla protezione dei dati personali spetta al titolare del trattamento: pertanto, si rende necessario uno standard verificabile per i fornitori di servizi cloud per dimostrare la loro capacità di ripresa e di garantire la sicurezza e la protezione dei dati, inclusi quelli personali soggetti alle normative privacy.

Sulla spinta della Commissione Europea, delle Autorità Nazionali e delle Commissioni per la protezione dei dati, ISO e IEC hanno quindi sviluppato il nuovo standard ISO / IEC 27018 (Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors), pubblicato nel 2014.

Contesto Normativo

ISO/IEC 27018 è il primo standard a livello internazionale per contribuire a garantire il rispetto dei principi e delle norme privacy, da parte dei providers di public cloud che se ne dotano: la norma, infatti, è specificamente indirizzata ai service providers di public cloud che elaborano dati personali (PII - Personally Identifiable Information) e che agiscano in qualità di Data (PII) Processor.
Definisce delle linee guida basate su ISO / IEC 27002, prendendo in considerazione i requisiti normativi per la protezione dei dati personali che possono essere applicabili nel contesto del panorama dei rischi di sicurezza informatica di un fornitore di servizi public cloud. Trattandosi di Linee guida, la norma ISO 27018 non è quindi una norma certificabile: ciò nonostante, è possibile ottenere una integrazione di un certificato ISO/IEC 27001 esistente e rilasciato da un Ente Certificatore riconosciuto, a dimostrazione della capacità del Provider di assicurare la protezione dei dati personali, basato sulla integrazione della Norma citata con la Norma ISO/IEC 27001.

La norma si basa e rinforza i precedenti standard ISO/IEC 27001 e ISO/IEC 27002 in materia di Gestione della Sicurezza delle Informazioni, e stabilisce obiettivi di controllo, regole e procedure per implementare misure di protezione dei dati personali (PII) in conformità con i principi di privacy di ISO / IEC 29100, per i fornitori di servizi cloud.

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

1) Norma e regole di Certificazione

Norma di Accreditamento	ISO 17021-1:2015, ISO/IEC 27006:2015
Norma di Certificazione	ISO/IEC 27018:2014, come addendum alla Norma ISO/IEC 27001:2013
Criteri di competenza del Gruppo di Verifica dell'OdC	All'interno del gruppo di verifica devono essere disponibili queste competenze, facenti capo ad una persona singola, o al Team nel suo complesso: • auditor ISO/IEC 27001:2013, con esperienza specifica di audit nella ISO/IEC 27001 di almeno 5 anni, preferibilmente in possesso di certificazione professionale. • ovvero auditor ISO 20000-1:2012, con esperienza specifica di audit nella ISO/IEC 20000 di almeno 5 anni, preferibilmente in possesso di certificazione professionale. Deve inoltre essere data dimostrazione della conoscenza della norma ISO/IEC 27018:2014.
Criteri di competenza del Decision maker	Per almeno un membro dell'Organo di Delibera è richiesta agli Odc la dimostrazione della: • Qualifica come ispettore ISO/IEC 27001, rilasciata in conformità alla ISO/IEC 27006 • Conoscenza della norma ISO/IEC 27018:2014
Tempi di verifica	Possono essere estese alla ISO/IEC 27018 solo organizzazioni già certificate ISO/IEC 27001. Per certificare una organizzazione a fronte della ISO/IEC 27018 occorre incrementare del 30% la durata dell'audit condotto per la ISO 27001. È possibile comunque condurre la verifica ISO/IEC 27001 in momenti distinti dalla verifica ISO/IEC 27018. Prima del rilascio della certificazione devono essere verificati tutti i datacenter presso cui sono dislocati i server che gestiscono il cloud. Nel caso in cui il certificato ISO/IEC 27001 sia stato rilasciato da un organismo differente, la durata dell'audit ISO/IEC 27018 deve essere pari al 50% dell'audit ISO/IEC 27001, e l'OdC deve avere accesso ai rapporti della verifica ISO/IEC 27001.
Certificato	Deve fare sempre riferimento alla Norma ISO/IEC 27001 citando l'utilizzo della linea guida ISO/IEC 27018 nella sua applicazione. Devono essere indicati i prodotti / servizi / applicazioni / processi coperti dalla certificazione.
Documenti IAF e EA	Si applicano tutti i documenti IAF ed EA in vigore per lo schema ISO/IEC 27001.

2) Processo di Accreditamento ACCREDIA

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-01-01 per la concessione dell'accreditamento ed estensione.
Per organismi già accreditati ISO/IEC 27001 con ACCREDIA, non occorre che questi abbiano già rilasciato dei certificati in questo schema per fare domanda di estensione dell'accreditamento.

Il certificato di accreditamento non riporta settori di accreditamento.

Nel caso in cui l'OdC possegga già accreditamenti rilasciati da altri enti di accreditamento, dovrà essere fatta una valutazione caso per caso, in base agli accordi EA / IAF MLA applicabili.

A	OdC già accreditato per lo schema ISO/IEC 27001	Esame documentale di 1 giornata (da svolgersi possibilmente presso la sede dell'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 scelte per l'accompagnamento ai fini del processo di accreditamento e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
B	OdC non accreditato ISO/IEC 27001	Occorre accreditarsi ISO/IEC 27001

Documentazione da presentare ad ACCREDIA per l'esame documentale

- Lista di riscontro o linea guida o istruzioni predisposte dall'OdC per il GVI;
- Curricula degli ispettori e dei Decision Maker
- Modulo del Rapporto di Audit;
- Attestato/Certificato rilasciato dall'OdC;
- Lista dei certificati già emessi, e delle prossime attività di verifica (nel caso sia necessario condurre una verifica in accompagnamento)
- Procedure / regolamenti contrattuali applicabili al processo di valutazione, nonché le procedure interne per la gestione della pratica di certificazione;
- Per gli OdC NON accreditati ISO/IEC 17021, oltre ai documenti sopra riportati, occorre inviare la documentazione richiesta nella domanda di accreditamento.

3) 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:

- Verifica in sede:
  - 0,5 giornate ogni anno per organismi accreditati ISO/IEC 27001 con ACCREDIA
  - 1 giornate ogni anno per organismi non accreditati ISO/IEC 27001 con ACCREDIA

- Verifica in accompagnamento da svolgersi nel ciclo di accreditamento:
  - se l'OdC ha emesso meno di 50 certificati nello schema di certificazione, deve essere effettuata una verifica in accompagnamento ogni 4 anni
  - se l'OdC ha emesso tra 51 e 200 certificati nello schema di certificazione, devono essere effettuate 2 verifiche in accompagnamento
  - se l'OdC ha emesso più di 201 certificati nello schema, devono essere effettuate 3 verifiche in accompagnamento

Siamo a disposizione per chiarimenti.

Con cordialità.

Il Direttore di Dipartimento
Dott. Emanuele Riva