E-Health e nuovo regolamento europeo sulla protezione dei dati

Codici di condotta e meccanismi di certificazione: Analogie e Differenze, quale adottare ed in quali circostanze

Microsoft House, 10 aprile 2017

Dott. Fabio Giuseppe Ferrara

Vice presidente del Comitato Scientifico di ASSO DPO – www.assodpo.it

Data Protection Officer - Certificato DPO_042 Bureau Veritas – conforme ISO IEC 17024:2003

Auditor/Lead Auditor - Sistemi di Gestione della Sicurezza delle Informazioni ISO/IEC 27001:2013 Certificato 2015/40/ISMS_15 C.B.International

EUROPEAN PRIVACY Auditor ISDP© 10003/2016 e Auditor Database & Privacy Management SGCMF©10002:2013 PRD UNI ISO/IEC 17065:2012

Membro della Commissione UNINFO UNI/CT 526/GL 3 «Profili Professionali relativi alla privacy»

Membro della Commissione UNI/CT 510/GL 05 "Tecnologie e tecniche per la protezione della Privacy e dei dati personal

Membro dell'organo tecnico UNI/CT 014/GL 07 - Qualificazione delle professioni per il trattamento di dati e documenti

info@arnaboldi.eu

I codici di condotta ed i meccanismi di certificazione

- Il Regolamento Europeo prevede la possibilità di adottare **codici di condotta** e **meccanismi di certificazione** quale ausilio al Titolare e al Responsabile per, rispettivamente, **precisare l'applicazione del Regolamento** e **dimostrare la conformità** alle disposizioni del Regolamento
- Il Regolamento prevede, infatti, degli obblighi generali in capo al Titolare del trattamento contenuti negli articoli 24 e 25 e degli obblighi specifici contenuti in varie altre disposizioni, il cui rispetto può essere dimostrato anche attraverso **l'adesione a codici di condotta o a meccanismi di certificazione**
- I **codici di condotta**, disciplinati dagli artt. 40 e 41 del Regolamento, mentre i **meccanismi di certificazione** sono disciplinati dagli artt. 42 e 43

I codici di condotta

- I **codici di condotta** possono essere **elaborati**, così come **modificati o prorogati**, dalle associazioni e dagli altri organismi rappresentanti le categorie di Titolari o Responsabili del trattamento con il fine di **precisare l'applicazione del Regolamento**

Altri soggetti che possono aderire → **Titolari o Responsabili del trattamento che non sono soggetti al Regolamento quale garanzia adeguata per i trasferimenti di dati personali** verso paesi terzi o organizzazioni internazionali con impegno vincolante e azionabile di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati

Codici di condotta e meccanismi di certificazione

- I **codici di condotta** hanno come scopo quello di precisare l'applicazione del Regolamento, ad esempio relativamente a:
  - ✓ Il trattamento corretto e trasparente dei dati
  - ✓ I legittimi interessi perseguiti dal titolare in specifici contesti
  - ✓ La raccolta dei dati personali e pseudonimizzazione
  - ✓ L'informazione fornita al pubblico e agli interessati e l'esercizio dei diritti degli interessati
  - ✓ L'informazione fornita e la protezione del minore e le modalità con cui è stato ottenuto il consenso dei titolari della responsabilità genitoriale
  - ✓ Le misure adeguate e le procedure anche di PbD e le misure per garantire la sicurezza del trattamento
  - ✓ La notifica di una violazione di dati personali, il trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali
  - ✓ Le procedure stragiudiziali o di altro tipo per comporre le controversie

- La procedura di approvazione dei codici di condotta prevede che il progetto di codice, della modifica o della proroga, venga **sottoposto all'autorità di controllo competente che esprime un parere** sulla conformità al Regolamento ed approva tale progetto, modifica o proroga, se ritiene sussistere garanzie adeguate

- La procedura di approvazione dei codici di condotta **dipende dal luogo di svolgimento delle attività di trattamento** specificate nel codice

Il progetto di codice, la modifica o la proroga riguarda **attività di trattamento che si svolgono solo nello Stato membro**

L'autorità di controllo **registra e pubblica il codice**

Il progetto di codice, la modifica o la proroga riguarda **attività di trattamento che si svolgono in vari Stati membri**

L'autorità di controllo sottopone il progetto di codice, la modifica o la proroga al Comitato che formula un parere sulla conformità al Regolamento o sulla previsione di adeguate garanzie nel caso di adesione al codice da parte di titolari o responsabili del trattamento che non sono soggetti al Regolamento

In caso di parere positivo, **il Comitato provvede a trasmettere il parere alla Commissione che può decidere che il codice di condotta, la modifica o la proroga abbiano validità generale all'interno della UE**

I codici di condotta con validità generale all'interno della UE

Sono adeguatamente **pubblicizzati a cura della Commissione**

Sono raccolti in un registro a cura del Comitato che provvede a **renderli pubblici con mezzi appropriati**

Codici di condotta e meccanismi di certificazione

- I codici di condotta sono **soggetti al controllo di conformità da parte di un organismo** che:
  - ✓ Possiede un **livello adeguato di competenze** riguardo al contenuto del codice
  - ✓ E' stato **accreditato** a tal fine **dall'Autorità di controllo competente** che definisce anche i criteri per tale accreditamento e ne presenta il progetto al Comitato
- Il codice di condotta deve contenere dei **meccanismi che consentono all'organismo preposto al controllo di conformità del codice di effettuare il controllo obbligatorio** del rispetto delle norme del codice da parte dei Titolari del trattamento o dei Responsabili del trattamento che si impegnano ad applicarlo

L'organismo per poter essere accreditato

- Deve dimostrare di essere **indipendente** e **competente** riguardo al contenuto del codice di condotta
- Deve aver istituito **procedure gli consentono di valutare l'ammissibilità dei Titolari e dei Responsabili del trattamento ad applicare il codice**, di controllare che detti Titolari e Responsabili ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento
- Deve aver istituito **procedure e strutture atte a gestire reclami** relativi a violazioni del codice di condotta
- **Deve aver dimostrato** in modo convincente all'autorità di controllo competente **che i compiti e le funzioni** da esso svolti **non danno adito a conflitto di interessi**

IN CASO DI VIOLAZIONE DEL CODICE DI CONDOTTA

L'organismo **deve adottare opportune misure in caso di violazione** del codice di condotta, tra cui **sospensione o esclusione** dal codice del Titolare del trattamento o del Responsabile del trattamento, **informando l'autorità di controllo competente**

Si ricorda che

L'accreditamento dell'organismo può essere revocato dall'autorità di controllo competente se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo violano il Regolamento

I meccanismi di certificazione

- Gli Stati UE, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione Europea incoraggiano l'istituzione di **meccanismi di certificazione per dimostrare la conformità al regolamento** che può anche risultare in una certificazione comune, vale a dire il sigillo europeo per la protezione dei dati
- **La certificazione che è volontaria, non riduce comunque la responsabilità del Titolare o del Responsabile** del trattamento riguardo alla conformità al Regolamento, restando impregiudicati i compiti e i poteri delle autorità di controllo competenti
- **La certificazione è rilasciata** al Titolare del trattamento o Responsabile del trattamento **per un periodo massimo di tre anni e può essere rinnovata** alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti

- La **certificazione può essere revocata** se non risultano più soddisfatti i requisiti richiesti per la stessa

- I **meccanismi di certificazione**, unitamente ai sigilli e ai marchi di protezione dei dati, sono **raccolti dal Comitato in un registro**, il quale provvede anche a renderli pubblici

- L'art. 83 del Reg. UE 2016/679 nel disciplinare le condizioni generali per infliggere le sanzioni amministrative pecuniarie ed il **relativo ammontare,** prevede che si tenga conto di **vari elementi tra i quali** quello mitigante costituito dall'***"adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42»*** (art. 83, comma 2, lettera J)

Codici di condotta e meccanismi di certificazione

La **certificazione è rilasciata:**

- **dagli organismi di certificazione** disciplinati dall'art. 43 del Regolamento

OPPURE

- **dall'Autorità di controllo competente in base ai criteri approvati da tale autorità competente o dal comitato** ed in tale ultimo caso ciò può risultare in una certificazione comune (il sigillo europeo per la protezione dei dati)

Nel caso di certificazione rilasciata dagli organismi di certificazione, tali **organismi sono accreditati per un periodo massimo di 5 anni rinnovabile da:**

L'Autorità di controllo competente

E/O

L'organismo nazionale di accreditamento ex Reg. CE n. 765/2008 (i.e. Accredia) **conformemente alla norma EN-ISO/IEC 17065/2012** e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente

- **La Commissione può adottare atti delegati per precisare i requisiti di cui tener conto per i meccanismi di certificazione e atti di esecuzione per stabilire norme tecniche**
- **Gli organismi di certificazione devono trasmettere all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione**
- **Gli organismi di certificazione sono responsabili della corretta valutazione** in merito al rilascio della certificazione o alla revoca della stessa
- **In caso di violazione dei propri obblighi** l'organismo di certificazione è sanzionato con la **sanzione amministrativa pecuniaria fino a EUR 10 milioni** o il 2% del fatturato mondiale totale annuo dell'esercizio precedente

- Nel caso di **certificazione rilasciata dall'Autorità di controllo** competente si ravvisano delle criticità **per conflitto di interessi e possibile assenza di terziarietà**
- Nel workshop tenutosi a Bruxelles il 26 luglio 2016 è stato evidenziato «***whether a DPA should do both, accredit and certify was subject to controversy. A conflict of interest was identified as impediment***».
- Lo stesso FabLab in tale sede ha posto l'interrogativo al momento irrisolto «***what happens if a DPA acts as a certifier and the project fails (potential conflict resulting from DPAs being competent for certification and supervisory tasks)?***»

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

STUDIO
ARNABOLDI

GRAZIE!