E-Health e nuovo regolamento europeo sulla protezione dei dati

Le principali novità del Regolamento Europeo 679/2016

Microsoft House, 10 aprile 2017

Dott.ssa Nadia Arnaboldi

Dottore Commercialista e Revisore Contabile – Coordinatrice della Commissione «Privacy, 231 e antiriciclaggio» ODCEC Pavia

Fellow of Information Privacy (FIP) - Certified Information Privacy Professional Europe and United States (CIPP/E, CIPP/US)

Certified Information Privacy Manager (CIPM) - Auditor/Lead Auditor ISO/IEC 27001:2013

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

Coordinatrice del Comitato Scientifico di AssoDPO – www.assodpo.it

info@arnaboldi.eu

Chi siamo

- Lo Studio Arnaboldi è nato nel 2004 per fornire una consulenza altamente specialistica a società nazionali e multinazionali in materia di protezione dei dati personali, diritto delle nuove tecnologie e digitalizzazione, implementazione di privacy programs e di tutti gli aspetti di compliance privacy.
- Tutti i professionisti e consulenti dello Studio sono iscritti in albi professionali e/o certificati come **Data Protection Officer**, Certified Information Privacy Professionals Europe e United States (**CIPP/E/US**), Certified Information Privacy Manager (**CIPM**) ISO standard 17024, nonché abilitati come **Auditor Database & Privacy Management** secondo lo schema di certificazione SGCMF 10002:2013 ed **European Privacy Auditor** secondo lo schema ISDP©10003:2015 PRD UNI EN ISO/IEC17065©2012.
- Alcuni professionisti dello Studio sono **contributors** delle riviste mensili Data Protection Leader» (già Data Protection Law & Policy) e «Digital health legal» (già eHealth Law & Policy) edite da Cecile Park Publishing, nonché relatori nell'ambito di convegni e congressi in materia di protezione dei dati personali.

- La dott.ssa **Nadia Arnaboldi**, founder dello Studio, è **autrice di monografie edite da Giuffré Editore e Maggioli Editore** in materia di protezione di dati personali, **Thought Leader in Privacy** di DataGuidance, **componente dei gruppi di lavoro internazionali** «*Global Data Breach Notification at-a-Glance table*» e «*Pharmacovigilance at-a-Glance Advisory*», nonché autrice delle advisory notes per DataGuidance. E' esperta indipendente della Commissione Europea (DG Home Affairs and Justice) in materia di Giustizia, Libertà e Sicurezza nell'ambito del Programma «Diritti fondamentali e giustizia – Protezione dei dati personali» (2007/S140-172522) ed inclusa nella lista di esperti per l'assistenza alla Commissione Europea nell'ambito del programma «Giustizia» e del Programma «Diritti, Uguaglianza e Cittadinanza» (2014-2020 (JUST/2014/AMIJ/001).

- Il dott. Fabio Giuseppe Ferrara, of counsel dello Studio, è membro dell'organo tecnico UNI/CT 014/GL 07 «*Qualificazione delle professioni e del trattamento di dati e documenti*», membro della commissione 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 personali*», membro dell'organo tecnico UNI/CT 014/GL 07 «*Qualificazione delle professioni per il trattamento di dati e documenti*».

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

STUDIO
ARNABOLDI

Il regolamento europeo 2016/679

in materia di protezione dei dati personali

Regolamento Europeo

- **La protezione dei dati personali delle persone fisiche** è un **diritto fondamentale dell'Unione Europea** previsto dall'art. 8, par. 1, della Carta dei diritti fondamentali dell'UE e dall'art. 16, par. 1, del Trattato sul funzionamento dell'UE.
- **Attualmente** la protezione dei dati personali è disciplinata dal **Decreto Legislativo 30 giugno 2003 n. 196** con il quale sono stati riuniti in un unico testo la legge 31 dicembre 1996 n. 675 (abrogata il 1 gennaio 2004) di recepimento nel nostro ordinamento della Direttiva 95/46/EC (Direttiva Privacy) e i vari decreti legislativi e DPR adottati a completamento del quadro normativo
- Il **progresso tecnologico** ed il **mutato scenario** in cui i dati sono trattati, nonché le **divergenze nel recepimento della Direttiva** da parte dei vari stati dell'Unione Europea, hanno reso necessaria una **riforma radicale** del quadro normativo promossa dalla Commissione Europea

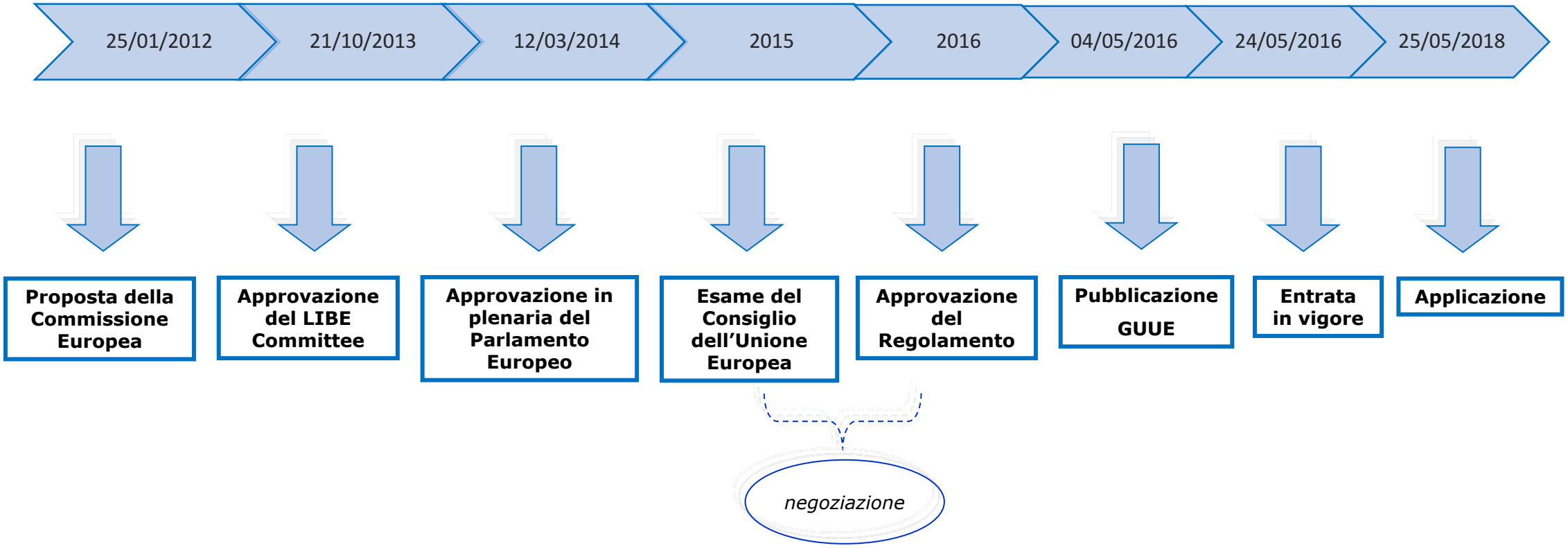
Regolamento Europeo

- Il **25 gennaio 2012** la Commissione Europea proponeva un nuovo "***quadro normativo solido e coerente, trasversale a tutte le politiche dell'Unione***" composto da:
  - ✓ un **Regolamento in sostituzione della Direttiva 95/46/CE** per l'istituzione di un quadro europeo generale in materia di protezione dei dati;
  - ✓ una **Direttiva in sostituzione della decisione quadro 2008/977/GAI16** che stabilisce le norme applicabili alla protezione dei dati personali trattati ai fini di prevenzione, indagine, accertamento o perseguimento dei reati e relative attività giudiziarie.
- Dopo oltre 4 anni di negoziati a livello di trilogo tra Commissione Europea, Parlamento e Consiglio, **in data 4 maggio 2016** la riforma si è quindi concretizzata con la **pubblicazione nella GUUE del Regolamento 2016/679** del 27 aprile 2016 che abroga la direttiva 95/46/CE e della Direttiva (UE) 2016/680

Regolamento Europeo

- Il Regolamento 2016/679 del 27 aprile 2016 è entrato **in vigore il 24 maggio 2016** e sarà applicabile dal **25 maggio 2018**
- Introduce **modifiche sostanziali** nell'**approccio** alla normativa in materia di protezione dei dati personali che dovrà essere **proattivo** e non reattivo
- **Introduce un'elevata responsabilizzazione** dei titolari del trattamento (principio di *accountability*) che dovranno essere in grado di **dimostrare la conformità dei trattamenti** al Regolamento
- Obbliga i titolari del trattamento a rivedere ed **aggiornare le proprie procedure** e ad adottare un approccio orientato ad una concreta tutela degli interessati
- La **Protezione dei dati personali assume un ruolo centrale** in tutte le decisioni dei titolari e dei responsabili del trattamento

SCENARIO: REGOLAMENTO 2016/679



Le principali novità

Ambito di applicazione territoriale

- **Estensione dell'ambito applicativo** anche alle attività svolte da **titolari stabiliti fuori dall'UE per i trattamenti dei dati di interessati che si trovano in paesi UE** quando le attività di trattamento riguardano:

  a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;

  b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Principi per il trattamento dei dati personali

- In aggiunta ai principi già noti nell'ordinamento nazionale quali liceità, correttezza, finalità, adeguatezza, pertinenza, esattezza, i nuovi principi di:
  - ✓ **Trasparenza**: obbligo del titolare di **informare gli interessati** in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate ai minori, per consentire l'espressione di consensi validi e l'esercizio dei diritti
  - ✓ **Responsabilizzazione** (c.d. *accountability*): obbligo del titolare mettere in atto **misure tecniche e organizzative adeguate** che devono essere costantemente monitorate ed aggiornate, se necessario, per **garantire, ed essere in grado di dimostrare** che il trattamento è effettuato conformemente al Regolamento

Approccio basato sulla valutazione del rischio e la valutazione di impatto sulla protezione dei dati

- Obbligo di effettuare una preventiva **valutazione dell'impatto del trattamento sulla protezione dei dati personali (DPIA)**, quando un tipo di trattamento presenta rischi elevati per i diritti e le libertà degli interessati, in **particolare se sono utilizzate nuove tecnologie e tenuto conto della natura, dell'oggetto, del contesto e delle finalità di trattamento**
- La valutazione di impatto viene effettuata dal titolare **consultandosi con il responsabile della protezione dei dati**
- L'analisi deve essere **rivista** se insorgono variazioni del rischio
- **Obbligo di consultare l'Autorità di Controllo se la DPIA evidenzia un rischio elevato in assenza di misure per attenuare il rischio**

Privacy by Design e by Default

- **Tutelare i dati personali fin dalla progettazione** (**Privacy by design**), **mediante l'adozione di misure tecniche ed organizzative adeguate** per attuare i principi di protezione dei dati ed integrare nel trattamento le garanzie necessarie di conformità al Regolamento

- Garantire che siano **trattati per impostazione predefinita solo i dati personali necessari** per ogni specifica finalità di trattamento (**Privacy by default**) mediante misure tecniche ed organizzative adeguate

I Registri delle attività di trattamento

- Obbligo di tenuta di un **registro delle attività di trattamento** sia per il **titolare** che per il **responsabile**, in caso di imprese o organizzazioni con 250 o più dipendenti, a meno che il trattamento possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa categorie particolari di dati personali o dati personali relativi a condanne penali e reati.

- Il registro deve essere tenuto **in forma scritta**, anche in formato elettronico

Contitolari - Nomina dei responsabili del trattamento – Nomina del Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

- Obbligo dei **contitolari** di regolamentare con un **accordo interno**, il cui contenuto essenziale è messo a disposizione dell'interessato, le rispettive responsabilità.
- La nomina del responsabile deve essere formalizzata mediante un **apposito contratto o altro atto giuridico** che disciplini i trattamenti di dati effettuati dal responsabile per conto del titolare (cfr. art. 28 Reg. EU 2016/679).
- Obbligo di nomina del **Responsabile della Protezione dei dati (RPD) o Data Protection Officer (DPO)** al ricorrere di determinati presupposti. La nomina dovrà essere conforme alle prescrizioni del Reg. EU 2016/679 ed alle indicazioni contenute nelle Linee Guida del Gruppo di Lavoro ex art. 29

Codici di condotta e meccanismi di certificazione – Notifica di Data Breach – Sanzioni

- Possibile adesione a **Codici di condotta** o **meccanismi di certificazione**
- Obbligo di **notifica della violazione dei dati personali** (Data Breach) entro termini temporali stringenti
- Severo **regime sanzionatorio**

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

STUDIO
ARNABOLDI

GRAZIE!

ASSO DPO