E-Health e nuovo regolamento europeo sulla protezione dei dati

Il principio di responsabilizzazione (ACCOUNTABILITY)
La protezione dei dati fin dalla progettazione (PRIVACY BY DESIGN)
e La protezione dei dati per impostazione predefinita (PRIVACY BY DEFAULT)

Microsoft House, 10 aprile 2017

Dott. Fabio Giuseppe FERRARA

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

Vice-presidente del Comitato scientifico di AssoDPO – www.assodpo.it

info@arnaboldi.eu

Il principio di responsabilizzazione

(ACCOUNTABILITY)

Il Regolamento introduce un'elevata responsabilizzazione dei titolari del trattamento (principio di *accountability*) che dovranno essere in grado di **dimostrare la conformità dei trattamenti** al Regolamento.

ACCOUNTABILITY

- Il Regolamento, recependo le indicazioni già rese dal Gruppo di Lavoro ex art. 29 nel parere 3/2010 adottato il 13 luglio 2010, prevede l'obbligo del Titolare di "*comprovare*" il rispetto dei principi di trattamento dei dati (art. 5) e di 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 (art. 24).

- Anche il Garante francese CNIL si è occupato specificatamente del tema dell'accountability adottando nel gennaio del 2015 un "*accountability standard*" per il cui rilascio è richiesta la soddisfazione di 25 requisiti fra i quali la nomina di un responsabile della protezione dei dati (c.d. data protection officer DPO).

ACCOUNTABILITY

- Il Regolamento introduce, pertanto, un **nuovo approccio** al tema della protezione dei dati personali, obbligando il Titolare ad avere un approccio **proattivo** con una protezione dei dati fin dalla **progettazione** e per impostazione predefinita e ad adottare tutte le misure necessarie ed adeguate in relazione agli obblighi imposti dal Regolamento e connessi alle tipologie di dati trattati, all'ambito del trattamento, alle finalità ed ai rischi del trattamento, alle tipologie di interessati e a tutti gli elementi rilevanti ai fini del regolamento

- Tali misure dovranno essere in grado di consentire al Titolare di dimostrare la conformità del trattamento.

ACCOUNTABILITY

- Il rispetto di tale principio da parte del Titolare implica il conseguente rispetto di **tutte** le disposizioni del Regolamento applicabili, dalla **corretta autorizzazione** delle persone che trattano i dati personali, all'**effettuazione della valutazione di impatto**, alla **tenuta del registro delle attività di trattamento**, alla corretta i**ndividuazione e designazione degli eventuali responsabili del trattamento**, alla designazione ove obbligatoria del **Responsabile della protezione dei dati (data protection officer o DPO)**, alla **notifica delle violazioni (data breach)**, al corretto trasferimento dei dati personali all'estero etc.

- Il Titolare può anche **dimostrare l'*accountability*** mediante l'adesione a **codici di condotta** o **meccanismi di certificazione**

La protezione dei dati fin dalla progettazione (PRIVACY BY DESIGN) e la protezione dei dati per impostazione predefinita (PRIVACY BY DEFAULT)

PRIVACY BY DESIGN E BY DEFAULT

Il Regolamento prescrive nell'art. 25 l'obbligo del Titolare del trattamento:

- di mettere in atto **misure tecniche ed organizzative adeguate**, ad esempio la pseudonimizzazione, per attuare i principi di protezione dei dati ed integrare nel trattamento le garanzie necessarie di conformità al Regolamento e di tutela degli interessati, **tutelando in tal modo il dato personale fin dalla progettazione** (c.d. ***Privacy by Design***);

- di mettere in atto misure tecniche ed organizzative adeguate per garantire che siano **trattati per impostazione predefinita solo i dati personali necessari** per ogni specifica finalità di trattamento (c.d. ***Privacy by Default***).

PRIVACY BY DESIGN E BY DEFAULT

- Il concetto di ***Privacy by Design*** è stato sviluppato negli anni '90 dall'Autorità di protezione dei dati dell'Ontario (Canada) https://www.ipc.on.ca/privacy/protecting-personal-information/privacy-by-design/

- Nel 2010 è stato riconosciuto quale componente fondamentale della protezione dei dati da tutte le Autorità di protezione dei dati e privacy mondiali riunitesi in sede assemblea annuale a Gerusalemme.

- Successivamente tale concetto è stato riconosciuto anche dalla *Federal Trade Commission* quale modalità per proteggere la privacy online e nel 2012 è stato previsto nella bozza di regolamento europeo in materia di protezione dei dati personali predisposta dalla Commissione Europea.

PRIVACY BY DESIGN E BY DEFAULT

- Il Regolamento Europeo 2016/679 pubblicato in GUUE il 4 maggio 2016 conferma le indicazioni della Commissione Europea ed impone al Titolare l'adozione di misure di ***Privacy by Design*** e ***by Default***.
  Si veda al riguardo il documento redatto dall'Autorità Garante dell'Ontario nel 2009 ed aggiornato nel 2013 che individua i 7 principi fondamentali della ***Privacy by Design***.

  - ✓ **Proactive not Reactive**: The *PbD* approach attempts to anticipate and prevent privacy-invasive events before they happen.
  - ✓ **Privacy as the Default Setting**: Ensure that personal data is automatically protected in any given IT system or business practice, so that if an individual does nothing, their privacy still remains intact.
  - ✓ **Privacy Embedded into Design**: Privacy should be embedded into the design and architecture of IT systems and business practices.
  - ✓ **Full Functionality – Positive-Sum, not Zero-Sum:** PbD seeks to accommodate all legitimate interests and objectives in a "win-win" manner, balancing seemly opposing interests, such as security and privacy.
  - ✓ **End-to-End Security – Full Lifecycle Protection:** PbD extends throughout the entire lifecycle of the data involved, from start to finish.
  - ✓ **Visibility and Transparency:** It seeks to assure all stakeholders that component parts and operations remain visible and transparent, to users and providers alike.
  - ✓ **Respect for User Privacy – Keep it User-Centric:** Above all, it puts the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

PRIVACY BY DESIGN E BY DEFAULT

- L'approccio di ***Privacy by Design*** consiste nell'**esame puntuale e preventivo** del trattamento dei dati personali che il Titolare desidera effettuare e degli strumenti che intende utilizzare, nonché **una verifica costante anche durante il trattamento** stesso.
- Tale esame deve tenere conto dello **stato dell'arte** e dei **costi di attuazione**, della **natura**, **dell'ambito di applicazione**, del **contesto** e delle **finalità** del trattamento, così come dei **rischi** aventi **probabilità** e **gravità** diverse per i diritti e le libertà degli interessati.
- L'approccio di ***Privacy by Default*** richiede al Titolare di individuare quelle misure adeguate a garantire in via preventiva il **trattamento dei soli dati necessari per ogni specifica finalità**. Ad esempio la definizione di ogni set minimo di dati che permette comunque di effettuare il trattamento necessario per le specifiche finalità

PRIVACY BY DESIGN E BY DEFAULT

- Come specificato nel Considerando 78, il Titolare del trattamento dovrebbe adottare "*politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default*".

- Gli stessi produttori dei prodotti, dei servizi e delle applicazioni basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni dovrebbero (*a nostro parere* ***DEVONO*** *ovviamente*) tener conto del diritto alla protezione dei dati già durante le fasi di sviluppo e progettazione per supportare i Titolari ed i Responsabili del trattamento nell'adempimento degli obblighi di protezione dei dati previsti dal Regolamento.

NOTA

Secondo il Considerando 78 tali misure potrebbero consistere, tra l'altro, "*nel ridurre al* ***minimo*** *il trattamento dei dati personali,* ***pseudonimizzare*** *i dati personali il più presto possibile, offrire* ***trasparenza*** *per quanto riguarda le funzioni e il trattamento di dati personali,* ***consentire*** *all'interessato di* ***controllare*** *il trattamento dei dati e* ***consentire*** *al titolare del trattamento di creare e migliorare caratteristiche di sicurezza*".

PRIVACY BY DESIGN E BY DEFAULT

- Lo stesso Garante Europeo ha previsto la collaborazione con le comunità di sviluppatori e designer informatici nell'ambito della propria strategia 2015-2019 per incoraggiare l'applicazione della Privacy by Design e della Privacy by Default attraverso l'ingegneria della tutela della privacy.

- **I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione, inoltre, anche nell'ambito degli appalti pubblici.**

- Il Regolamento consente al Titolare ed al Responsabile del trattamento di dimostrare la conformità all'approccio di *Privacy by Design* e *by Default* anche mediante un **meccanismo di certificazione.**

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

STUDIO
ARNABOLDI

GRAZIE!

ASSO DPO