# Privacy by design e by default: registro trattamenti, data-breach e meccanismi di certificazione Il ruolo del DPO: considerazioni Torino, 12 ottobre 2017


*Dott. Fabio Giuseppe Ferrara*

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

**Socio AISIS – Capogruppo Area Legal GdL AISIS 2017**

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

**Auditor Qualificato eIDAS - Regolamento Europeo 910/2014 - ACCREDIA**

**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 UNI/CT 526 "UNINFO Attività professionali non regolamentate**

**Membro della Commissione UNINFO UNI/CT 526/GL 01 "Profili professionali relativi alla sicurezza informatica**

**Membro della Commissione UNINFO UNI/CT 526/GL 02 "Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Professionista Web**

**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**

***fabio.ferrara@arnaboldi.eu*** **-** ***info@arnaboldi.eu***

# *Indice*

- **Privacy by design e by default. Cenni**
- **Registro trattamenti**
- **Data-breach**
- **Meccanismi di certificazione**

# Premessa

- Il Regolamento 2016/679 del 27 aprile 2016 è entrato **in vigore il 24 maggio 2016** e sarà applicabile dal **25 maggio 2018** (cfr. art. 99 Reg. EU)
- 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

# 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** (e.g. pseudonimizzazione) 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 (cfr. guida del Garante).

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

# Notifica di Data Breach

# Meccanismi di certificazione

- Obbligo di **notifica della violazione dei dati personali** (c.d. *Data Breach*) entro termini temporali stringenti (i.e. 72 ore)

- Possibile adesione a **Codici di condotta** o **meccanismi di certificazione**

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

STUDIO
ARNABOLDI

# IL REGISTRO DELLE ATTIVITA DI TRATTAMENTO

# 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 (cfr. guida del Garante).

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

# I Registri delle attività di trattamento

- Il 28 aprile u.s. il Garante italiano ha pubblicato sul sito al link: http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali , la prima guida applicativa inerente il regolamento europeo 679/2016 in materia di protezione dei dati personali.

# Dalle Linee Guida del Gdp

**Nella sezione dedicata al registro dei trattamenti il Garante sottolinea i seguenti concetti come fondamentali:**

- ✓**strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico –
- ✓**indispensabile per ogni valutazione e analisi del rischio**.

Inoltre

- ✓La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**.
- ✓Per tale motivo, ***«si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro».***
- ✓Nello specifico, si richiama l'attenzione sulla sostanziale **coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolamento.**

# Il registro tenuto dal Titolare deve contenere le seguenti informazioni:

- Il **nome e i dati di contatto** del **titolare** del trattamento e, ove applicabile, del **contitolare**, del **rappresentante** del titolare e del **responsabile della protezione dei dati**;
- le **finalità** del trattamento;
- una descrizione delle **categorie di interessati** e delle **categorie di dati** personali;
- le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i **trasferimenti di dati** personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle **garanzie adeguate**;
- ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati;
- ove possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative**

# Il registro tenuto dal RESPONSABILE deve contenere le seguenti informazioni:

- il **nome e i dati di contatto** del **responsabile o dei responsabili** del trattamento, **di ogni titolare del trattamento per conto del quale agisce** il responsabile del trattamento, **del rappresentante del titolare del trattamento o del responsabile** del trattamento e, ove applicabile, **del responsabile della protezione dei dati**;
- le **categorie dei trattamenti** effettuati per conto di ogni titolare del trattamento;
- ove applicabile, **i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale**, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
- ove possibile, **una descrizione generale delle misure di sicurezza tecniche e organizzative**.

# Principali aspetti da indirizzare

✓**La determinazione delle finalità e dei tempi e modi di conservazione:** le finalità indicate nel registro NON possono NON essere coerenti con le informative rilasciate. I termini per la cancellazione devono essere indicati per ogni categoria di dati devono essere procedurizzati, così come le modalità di conservazione.

✓**I processi di aggiornamento e modifica del registro:** il registro deve ESSERE aggiornato ogni volta che vi sia una variazione di un processo di trattamento o qualora sia avviata una nuova attività di trattamento

✓**Il valore probatorio del registro e la sua opponibilità a terzi.**

# Principali aspetti da indirizzare

- ✓ **I campi informativi del registro:** il registro, tenuto come titolare, deve contenere almeno gli elementi minimi richiesti dal Regolamento, ma è CONSIGLIATO integrarlo con tutti gli altri elementi necessari ad attestare l'accountability
- ✓ **I razionali per il censimento dei trattamenti:** i dati inerenti l'identificazione dei trattamenti che possono, ad esempio basarsi su fonti informative documentali facilmente reperibili (e.g. DPS, classificazione dei processi di trattamento, asset inventory l'elenco dei DB…) coinvolgendo sempre nel merito le Business Unit/Aree funzionali impattate.

# Principali aspetti da indirizzare

- ✓ **La determinazione delle finalità e dei tempi e modi di conservazione:** le finalità indicate nel registro NON possono NON essere coerenti con le informative rilasciate. I termini per la cancellazione devono essere indicati per ogni categoria di dati devono essere procedurizzati, così come le modalità di conservazione.
- ✓ **I processi di aggiornamento e modifica del registro:** il registro deve ESSERE aggiornato ogni volta che vi sia una variazione di un processo di trattamento o qualora sia avviata una nuova attività di trattamento
- ✓ **Il valore probatorio del registro e la sua opponibilità a terzi.**

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

STUDIO
ARNABOLDI

# L'OBBLIGO DI NOTIFICA DI DATA BREACH

# PREVISTO DAL GDPR

# *L'obbligo di notifica di Data Breach ex GDPR*

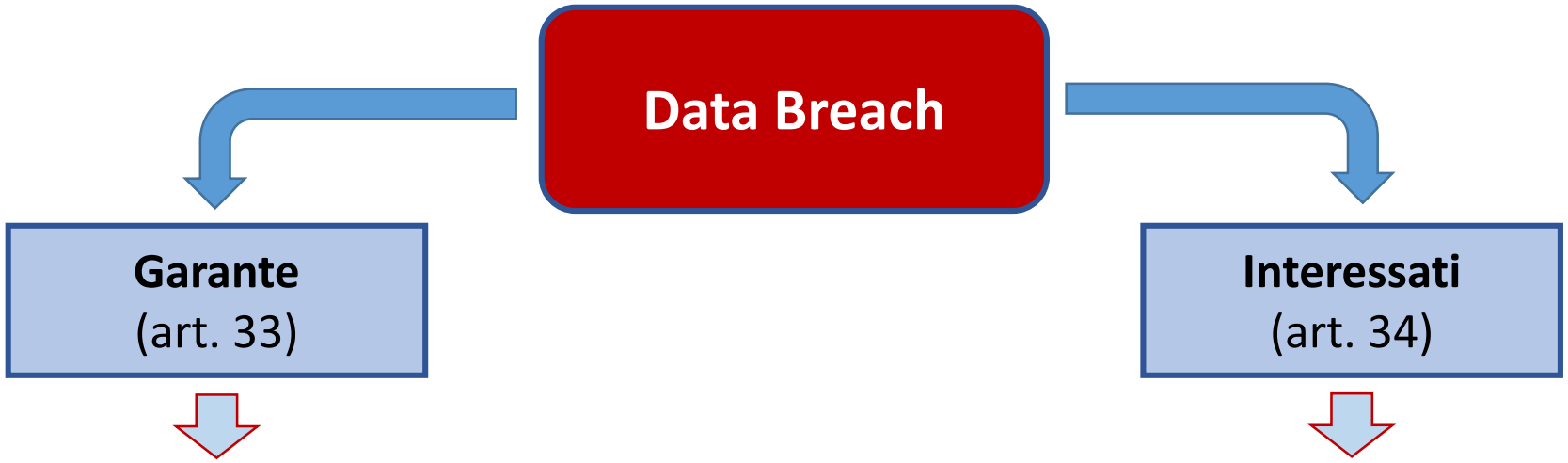
**«DATA BREACH» =**

**VIOLAZIONI DEI DATI**

Definizione – Art. 4 (12) GDPR

- ✓ *"**violazione dei dati personali**": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*

# L'obbligo di notifica di Data Breach ex GDPR




- Senza ingiustificato ritardo e, ove possibile, entro **72h** dall'avvenuta conoscenza, salvo qualora siano improbabili rischi. **Se oltre 72h obbligo di indicare i motivi del ritardo**
- **Obbligo del responsabile di informare il titolare** senza ingiustificato ritardo
- **Contenuto minimo** della notifica di data breach (cfr. art. 33, co. 3)
- Possibilità di fornire **alcune informazioni in fasi successive** (sempre senza ingiustificato ritardo)
- Obbligo di **documentare** qualsiasi violazione

- Quando presenta un **rischio elevato per i diritti e le libertà delle persone fisiche**
- **Contenuto minimo** della notifica di data breach (cfr. art. 34, co. 2)
- **Possibilità di non effettuare la notifica di data breach** all'interessato in caso di:
  - Esistenza di **misure tecniche ed organizzative adeguate** anche successive
  - **Sforzo sproporzionato**. In tal caso **comunicazione pubblica**
- Possibile comunque una **richiesta di notifica di data breach da parte dell'Autorità** (artt. 34, co. 4, e 58, co. 2, lett. e)

# *L'obbligo di notifica di Data Breach ex GDPR*



**EX GDPR**

- **Le associazioni ed altri organismi rappresentanti le categorie dei titolari del trattamento** possono elaborare **codici di condotta** per precisare le modalità di «*notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni di dati personali all'interessato*» (art. 40, comma 2, lett. i)
- L'adesione a **meccanismi di certificazione** può essere di **ausilio** per dimostrare la conformità al regolamento (art. 42)
- Il **Comitato Europeo per la protezione dei dati** di propria iniziativa o su richiesta della Commissione, pubblicherà **Linee Guida**, **raccomandazioni** e **migliori prassi:**
  - per **accertare la violazione e determinare l'ingiustificato ritardo** per la notifica di data breach, così come le circostanze particolari in cui il titolare del trattamento o il responsabile è tenuto a notificare la violazione
  - relative alle **circostanze in cui una violazione è suscettibile di presentare un rischio elevato** per i diritti e le libertà delle persone fisiche

# *Codici di condotta e meccanismi di certificazione:*

# *Analogie e Differenze, quale adottare ed in quali circostanze*

# 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

- 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**

- 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)

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 eventualmente 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 si possono ravvisare delle possibili criticità **per conflitto di interessi nonche per possibile assenza di terzietà**
- 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)?***»

- Nel caso di **certificazione rilasciata dall'Autorità di controllo** competente si si possono ravvisare delle possibili criticità **per conflitto di interessi nonche per possibile assenza di terzietà**
- 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)?***»

# *Il ruolo del Responsabile della protezione dei dati Rpd/DPO: considerazioni…*

# La designazione del responsabile della protezione dei dati

- **Obbligo di nomina del RPD/DPO** da parte del titolare o del responsabile quando:
  - ✓ **Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico**, salvo le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali
  - ✓ **Le attività principali** del titolare del trattamento o del responsabile del trattamento consistono in **trattamenti che** per loro natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**
  - ✓ **Le attività principali** del titolare o del responsabile consistono nel **trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali o reati**

- **L'RPD/DPO può essere contattato dagli interessati** per qualsiasi questione e per l'esercizio dei diritti

- **Il dati di contatto del RPD/DPO** devono essere **pubblicati**, a cura del titolare o responsabile, e devono essere **comunicati all'Autorità di Controllo**

- **Il RPD/DPO non è personalmente responsabile in caso di non conformità al regolamento.** Tale responsabilità è solo in capo al titolare o al responsabile

# Obblighi del titolare e del responsabile

- **Il titolare ed il responsabile devono:**
  - ✓ **coinvolgere il RPD**, tempestivamente ed adeguatamente, in qualsiasi questione che riguardi il trattamento dei dati personali
  - ✓ **sostenere il RPD** nell'esecuzione dei suoi compiti e **dotarlo delle risorse necessarie** per assolvere i propri compiti e mantenere una conoscenza adeguata
  - ✓ **assicurare che non riceva alcuna istruzioni** per l'esecuzione dei suoi compiti, né rimuoverlo o penalizzarlo per l'adempimento dei suoi compiti: l'RPD deve essere indipendente ed agire in assenza di conflitto di interessi
  - ✓ **non penalizzare, né direttamente né indirettamente, il RPD per l'assolvimento dei suoi compiti**

- **Newsletter 15 settembre: Regolamento privacy, come scegliere il responsabile della protezione dei dati**
  - ✓ http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6826945#1
  - ✓ Nella nota inviata a un'azienda ospedaliera l'Ufficio del Garante ricorda che i Responsabili della protezione dei dati personali - spesso indicati con l'acronimo inglese DPO (Data Protection Officer) – dovranno avere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. -> segue

- Nella selezione sarà poi opportuno privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari **documentando** le esperienze fatte, **la partecipazione a master e corsi di studio/professionali (in particolare se risulta documentato il livello raggiunto)**. Gli esperti individuati dalle aziende ospedaliere, ad esempio, in considerazione della delicatezza dei trattamenti di dati effettuati (come quelli sulla salute o quelli genetici) dovranno preferibilmente vantare una specifica esperienza al riguardo e assicurare un impegno pressoché esclusivo nella gestione di tali compiti. ->segue

- L'Autorità ha inoltre chiarito che la normativa attuale non prevede l'obbligo per i candidati di possedere attestati formali delle competenze professionali. Tali attestati, rilasciati anche all'esito di verifiche al termine di un ciclo di formazione, possono rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenza della disciplina ma, tuttavia, non equivalgono a una **"abilitazione"** allo svolgimento del ruolo del RPD. La normativa attuale, tra l'altro, non prevede l'istituzione di un albo dei "Responsabili della protezione dei dati" che possa attestare i requisiti e le caratteristiche di conoscenza, abilità e competenza di chi vi è iscritto. Enti pubblici e società private dovranno quindi comunque procedere alla selezione del RPD, valutando **autonomamente** il possesso dei requisiti necessari per svolgere i compiti da assegnati.

# *Ultima considerazione…*

Ma il ruolo del DPO/RpD è davvero una novità?

NO!!!

Date un occhio: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:it:PDF

SEZIONE 8

RESPONSABILE DELLA PROTEZIONE DEI DATI

Articolo 24:Nomina e mandato del responsabile della protezione dei dati

**Nomina e mandato del responsabile della protezione dei dati**

Ogni istituzione ed organismo della Comunità nomina almeno un responsabile della protezione dei dati personali con il mandato di:

a) garantire che i responsabili del trattamento e gli interessati siano informati dei propri diritti ed obblighi ai sensi del presente regolamento;

b) rispondere alle richieste del garante europeo della protezione dei dati e, nell'ambito delle sue competenze, cooperare con il garante europeo della protezione dei dati su richiesta di quest'ultimo o di propria iniziativa;

c) garantire in maniera indipendente che le disposizioni del presente regolamento vengano applicate all'interno dell'istituzione o organismo di cui fa parte;L 8/14 IT Gazzetta ufficiale delle Comunità europee 12.1.2001

d) **tenere il registro delle operazioni effettuate dal responsabile del trattamento**, riportandovi le informazioni di cui all'articolo 25, paragrafo 2;

e) notificare al garante europeo della protezione dei dati i trattamenti che possono presentare rischi specifici ai sensi dell'articolo 27.

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

STUDIO
ARNABOLDI

# GRAZIE!