Il registro dei trattamenti e la DPIA (*Data Protection Impact Assessment*)

PADOVA, 3 MAGGIO 2018 — CAMERA DI COMMERCIO

Il Registro del trattamento

UN ADEMPIMENTO NECESSARIO

Considerando:

(82) Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.

Art. 30 - Il registro del Titolare (1° comma)

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) 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, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Art. 30 - Il registro del Responsabile (2° comma)

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) 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;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) 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, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Forma

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Esenzioni

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti,

a meno che il trattamento che esse effettuano;

- possa presentare un rischio per i diritti e le libertà dell'interessato,
- il trattamento non sia occasionale
- o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1,
- o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Garante italiano:

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a **rischio** *(si veda art. 30, paragrafo 5)*, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno **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**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

RACCOMANDAZIONI

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 e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva **valutazione di impatto** dei trattamenti svolti.

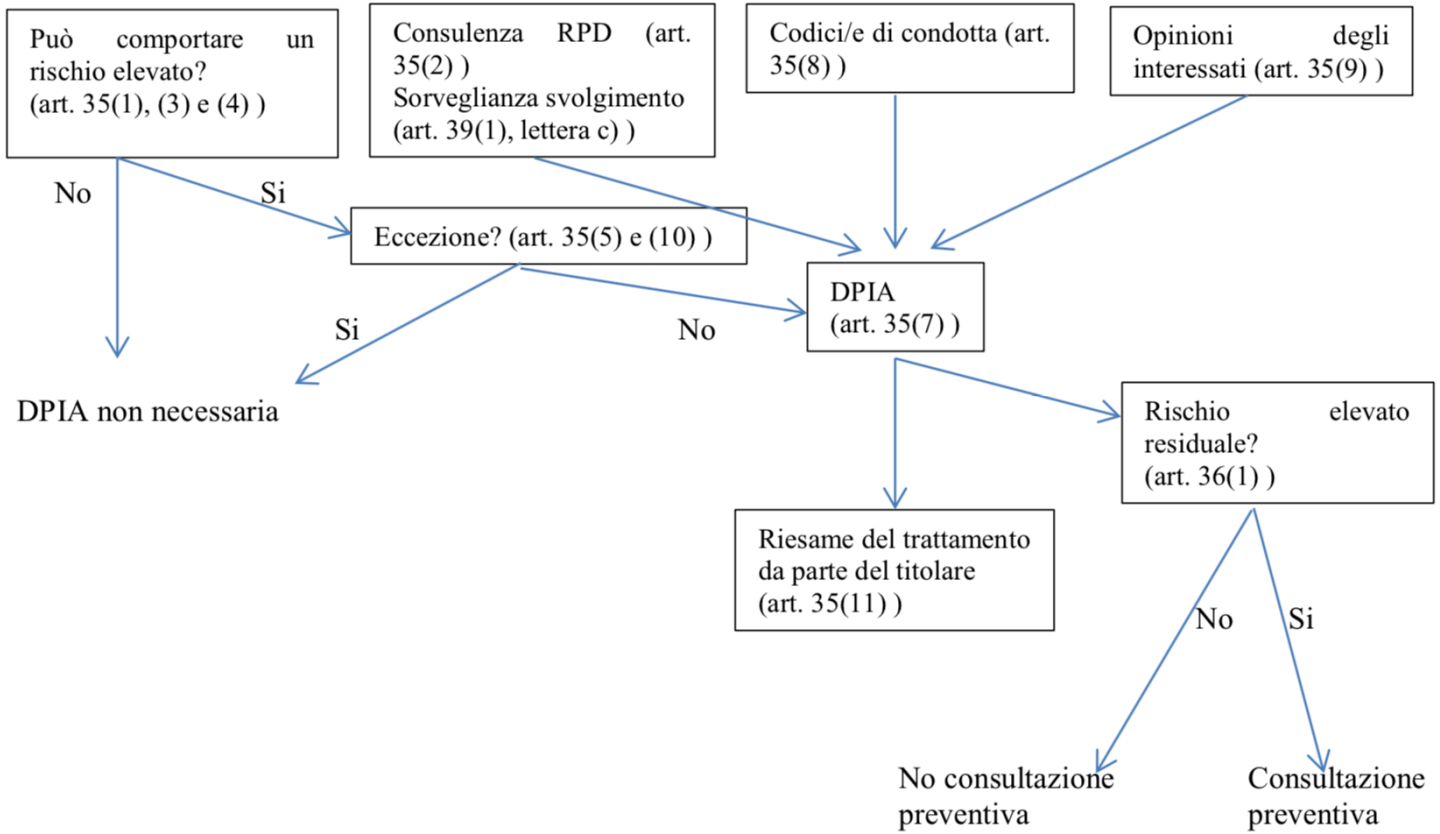
Valutazione di impatto (DPIA)

Quando un tipo di trattamento, allorché prevede in particolare l'uso di **nuove tecnologie**, considerati la **natura**, **l'oggetto**, il **contesto** e le **finalità** del trattamento, può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche… (art. 35)

Quali diritti e libertà?

privacy ed altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione diritto alla vita, diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, processo equo, diritto al matrimonio, etc.

Quando



Quando

La valutazione d'impatto sulla protezione dei dati è richiesta **in particolare** nei casi seguenti:

1. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automa-tizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

2. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati

3. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

I criteri del WP29

1. *Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive*
2. Decisioni automatizzate
3. Monitoraggio sistematico
4. *Dati sensibili o dati di natura estremamente personale*
5. Trattamenti di dati su larga scala
6. Combinazione o raffronto di insiemi di dati
7. Dati relativi a interessati vulnerabili
8. *Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative*
9. *Tutti quei trattamenti che, di per sé, "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto"*

Esempi

Ospedale che tratta dati genetici e sanitari relativi ai pazienti (sistema informativo ospedaliero)	•Dati sensibili •Dati relativi a interessati vulnerabili •Dati trattati su larga scala
Utilizzo di un sistema di videosorveglianza per il controllo del traffico autostradale. Il titolare prevede di utilizzare un sistema intelligente di analisi delle immagini per l'individuazione dei veicoli e il riconoscimento automatico delle targhe	•Monitoraggio sistematico •Utilizzo innovativo di tecnologia
Azienda che controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su Internet, ecc.	• Monitoraggio sistematico • Dati relativi a interessati vulnerabili

Esempi

Raccolta di dati pubblici tratti dai *social media* per la creazione di profili	• Valutazione o scorni • Larga scala • Raffronto • Dati sensibili o strettamente personali
Un'istituzione che crei un database nazionale di valutazioni creditizie o per finalità antifrode	• Valutazione e scorni • decisioni automatizzate • Impedimenti all'esercizio di diritto o contratto • dati sensibili o dati strettamente personali
Conservazione per scopi di archiviazione di dati sensibili pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o studi clinici sperimentali	• Dati sensibili • Dati di interessati vulnerabili • Impedimento esercizio di un diritto

CHI

Spetta al titolare garantire l'effettuazione della DPIA (art. 35, paragrafo 2).

La conduzione materiale della DPIA può essere affidata a un altro soggetto, interno o esterno all'organismo; tuttavia, la responsabilità ultima dell'adempimento ricade sul titolare del trattamento.

Il titolare deve consultarsi con il responsabile della protezione dei dati (RPD/DPO), ove designato (art. 35, paragrafo 2); tale consultazione e le conseguenti decisioni assunte dal titolare devono essere documentate nell'ambito della DPIA. Il RPD è chiamato anche a monitorare lo svolgimento della DPIA

Se il trattamento è svolto, in tutto o in parte, da un responsabile, **quest'ultimo deve assistere il titolare nella conduzione della DPIA** fornendo ogni informazione necessaria conformemente con l'art. 28, paragrafo 3, lettera f).

COSA

COME

Sono pubblicati alcuni schemi generali:

- **DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[30]. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf**

- **ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/G uia_EIPD.pdf**

- **FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798**

- **UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf**

COME

Sono pubblicati alcuni schemi particolari:

- **Privacy and Data Protection Impact Assessment Framework for RFID Applications. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf**

- **Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[32] http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf**

COME

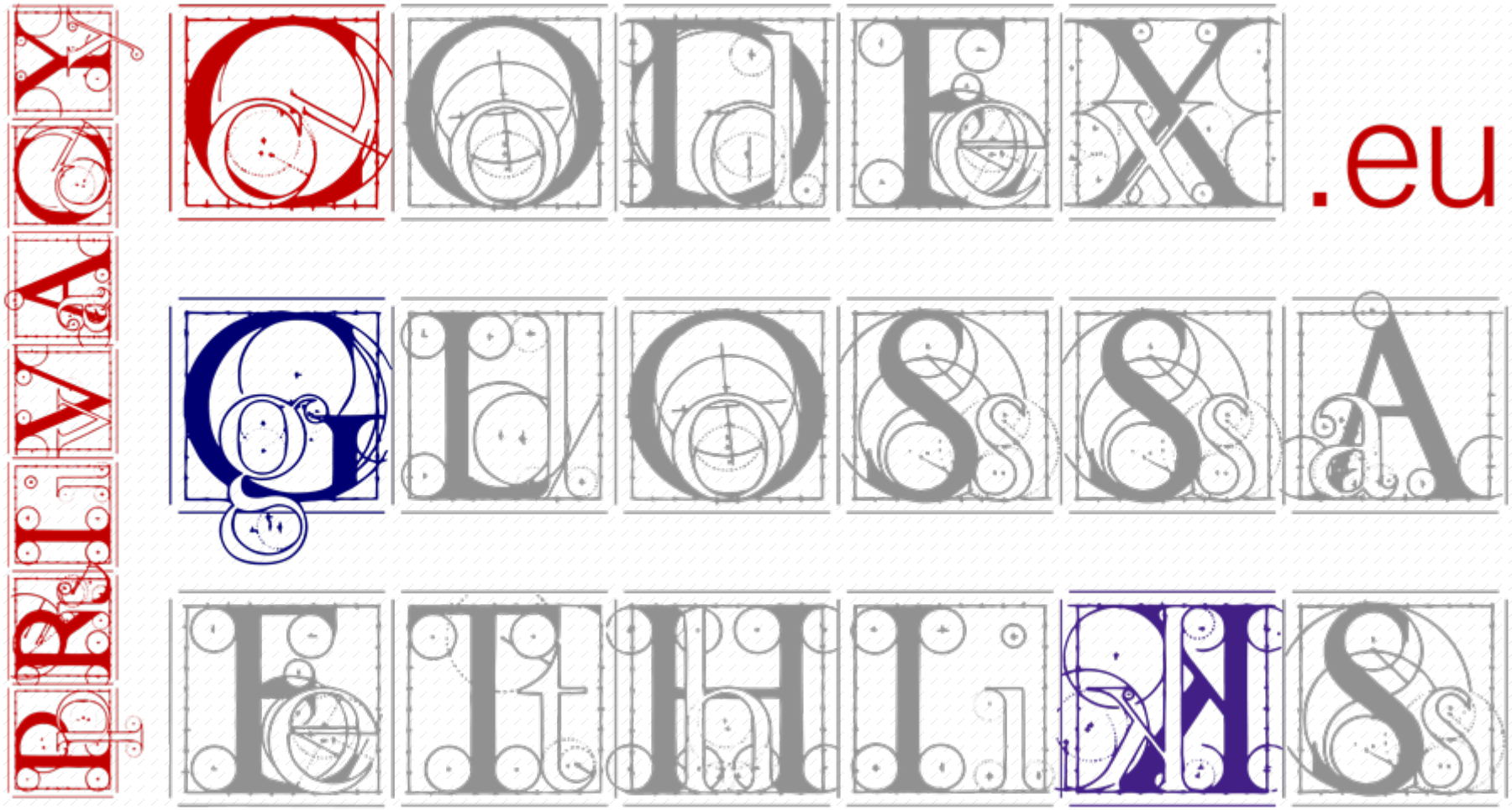
A **Giugno 2017** è stato pubblicato lo schema **ISO/IEC 29134:2017**

Information technology -- Security techniques -- Guidelines for privacy impact assessment

https://www.iso.org/standard/62289.html

Lo schema riprende sostanzialmente le linee guide dell'autorità francese che aveva individuato una metodologia ed un template

https://www.cnil.fr/fr/node/24129



Fine della presentazione

Avv. Massimiliano Nicotra (www.studionicotra.com — www.avvmax.com — www.privacycodex.eu)

Spazio per le domande e la discussione

Grazie per la vostra pazienza… e attenzione