La tutela dei dati personali, la certificazione art. 42, la sicurezza dei dati, la formazione

Luigi PAVANI
Business Development Manager

RINA Services S.p.A.

luigi.pavani@rina.org

Agenda

- INTRODUZIONE
- Misure di Sicurezza: adeguamento dei sistemi informativi e rapporti contrattuali con i fornitori
- Accountability e coadiuvanti in caso di controllo (Certificazioni e codici di condotta)
- Confronto tra ISO 27001 e GDPR

Il Regolamento UE

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE)

(2) Il presente regolamento è inteso a

- contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica,
- al progresso economico e sociale,
- al rafforzamento e alla convergenza delle economie nel mercato interno e
- al benessere delle persone fisiche.

Il Regolamento UE - obiettivi

166) Al fine di conseguire gli obiettivi del regolamento, segnatamente tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire la libera circolazione di tali dati nell'Unione

OBIETTIVI:

- tutelare i diritti e le libertà fondamentali delle persone fisiche
- in particolare il diritto alla protezione dei dati personali
- garantire la libera circolazione di tali dati nell'Unione

Information Security nel Regolamento UE

Violazione dei dati personali: *[personal data breach]*	La violazione di sicurezza *[breach of security]* che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati;
Disponibilità	la distruzione, la perdita,
Integrità	la modifica,
Riservatezza	la divulgazione o l'accesso non autorizzati

Risk management nel regolamento UE

Situazioni di rischio:

(75) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale.
in particolare:

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;

Rischio:
incertezza sugli obiettivi del trattamento dei dati personali

Il Regolamento UE - rischi

Situazioni di rischio:

(75) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale. in particolare:

(2) Il presente regolamento è inteso a

- contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica,
- al progresso economico e sociale,
- al rafforzamento e alla convergenza delle economie nel mercato interno e
- al benessere delle persone fisiche.

se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;

Rischio:
incertezza sugli obiettivi del trattamento dei dati personali

Esempi di attributi che possono identificare le persone [ISO 29100]

- Age or special needs of vulnerable natural persons
- Allegations of criminal conduct
- Any information collected during health services
- Bank account or credit card number
- Biometric identifier
- Credit card statements
- Criminal convictions or committed offences
- Criminal investigation reports
- Customer number
- Date of birth
- Diagnostic health information
- Disabilities
- Doctor bills
- Employees' salaries and human resources files
- Financial profile Gender
- GPS position
- GPS trajectories
- Home address
- IP address
- Location derived from telecommunications systems
- Medical history
- Name
- National identifiers (e.g., passport number)
- Personal e-mail address
- Personal identification numbers (PIN) or passwords
- Personal interests derived from tracking use of internet web sites
- Personal or behavioural profile
- Personal telephone number
- Photograph or video identifiable to a natural person
- Product and service preferences
- Racial or ethnic origin
- Religious or philosophical beliefs
- Sexual orientation
- Trade-union membership
- Utility bills

ISO/IEC29100
Information technology — Security techniques — Privacy framework
2011-12-15

Principi di Data Protecion [ISO 29100]

Table 3 – The privacy principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

Agenda

- Introduzione
- **Accountability e coadiuvanti in caso di controllo (Certificazioni e codici di condotta)**
- Misure di Sicurezza: adeguamento dei sistemi informativi e rapporti contrattuali con i fornitori
- Confronto tra ISO 27001 e GDPR

Il Regolamento UE – Sanzioni

Articolo 83

Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

Il Regolamento UE – Certificazione - Vantaggi

CAPO IV

Titolare del trattamento e responsabile del trattamento

Sezione 1

Obblighi generali

Articolo 24

Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Il Regolamento UE – Certificazione - Vantaggi

Articolo 28

Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

Il Regolamento UE – Certificazione - Vantaggi

Sezione 2

Sicurezza dei dati personali

Articolo 32

Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

Il Regolamento UE - Certificazione - Vantaggi

Articolo 46

Trasferimento soggetto a garanzie adeguate

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Il Regolamento UE- codici di condotta

Sezione 5

Codici di condotta e certificazione

Articolo 40

Codici di condotta

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

2. Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:

a) il trattamento corretto e trasparente dei dati;

Il Regolamento UE- codici di condotta

4. Il codice di condotta di cui al paragrafo 2 del presente articolo contiene i meccanismi che consentono all'organismo di cui all'articolo 41, paragrafo 1, 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, fatti salvi i compiti e i poteri delle autorità di controllo competenti ai sensi degli articoli 55 o 56.

Il Regolamento UE- codici di condotta

5. Le associazioni e gli altri organismi di cui al paragrafo 2 del presente articolo che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice, la modifica o la proroga all'autorità di controllo competente ai sensi dell'articolo 55. L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate.

6. Qualora il progetto di codice, la modifica o la proroga siano approvati ai sensi dell'articolo 55, e se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice.

10. La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 9.

11. Il comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

Il Regolamento UE- Monitoraggio codici di condotta

Articolo 41

Monitoraggio dei codici di condotta approvati

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente.

Il Regolamento UE- Certificazione

Articolo 42

Certificazione

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

Il Regolamento UE - Certificazione

2. Oltre all'adesione dei titolari del trattamento o dei responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo, possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

3. La certificazione è volontaria e accessibile tramite una procedura trasparente.

4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56.

Il Regolamento UE – Organismi di Certificazione

Articolo 43

Organismi di certificazione

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:

a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56;

b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio ([1]) conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56.

Il Regolamento UE – Organismi di Certificazione

4. Gli organismi di certificazione di cui al paragrafo 1 sono responsabili della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione soddisfi i requisiti.

5. L'organismo di certificazione di cui al paragrafo 1 trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta.

6. I requisiti di cui al paragrafo 3 del presente articolo e i criteri di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in forma facilmente accessibile. Le autorità di controllo provvedono a trasmetterli anche al comitato. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

7. Fatto salvo il capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento di un organismo di certificazione di cui al paragrafo 1 del presente articolo, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il presente regolamento.

Il Regolamento UE – Compiti dell'autorità di controllo

Articolo 57

Compiti

1. Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo:

m) incoraggia l'elaborazione di codici di condotta ai sensi dell'articolo 40, paragrafo 1, e fornisce un parere su tali codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma dell'articolo 40, paragrafo 5;

n) incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5;

o) ove applicabile, effettua un riesame periodico delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;

p) definisce e pubblica i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;

q) effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;

h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;

Il Regolamento UE – Compiti dell'autorità di controllo

Garante per la protezione dei dati personali

Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali

Attraverso l'adesione a codici deontologici ovvero l'adesione a schemi di certificazione il responsabile può dimostrare le "garanzie sufficienti" di cui all'art. 28, paragrafi 1 e 4. Il Garante sta valutando i codici deontologici attualmente vigenti per alcune tipologie di trattamento nell'ottica dei requisiti fissati nel regolamento *(art. 40)*, mentre per quanto concerne gli schemi di certificazione occorrerà attendere anche l'intervento del legislatore nazionale che dovrà stabilire alcune modalità di accreditamento dei soggetti certificatori *(se diversi dal Garante: si veda art. 43)*. In ogni caso, il Gruppo "Articolo 29" sta lavorando sui temi e sarà opportuno tenere conto degli sviluppi che interverranno in materia nei prossimi mesi.

http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento

La Certificazione

Certificazione di Processo	Articolo 42, Articolo 43 La certificazione individuata sul Regolamento è una Certificazione di Processo, che rientra nell'ambito della «Certificazione di Prodotto» ISO 17065 Comprende requisiti organizzativi, procedurali, tecnologici e legali, relativi al processo generale di gestione dati personali
Certificazione ISO 27001	Non esplicitamente richiamata nel Regolamento E' una Certificazione di Sistema di Gestione, che rientra nell'ambito della «Certificazione di Sistema» ISO 17021 Comprende requisiti organizzativi, procedurali, tecnologici sulla gestione delle informazioni

La ISO 27001 INTEGRA la certificazione di processo

La ISO 27001 può essere un ottimo strumento per la strutturazione di un sistema di gestione orientato alla sicurezza dei dati a supporto della conformità di processo

Agenda

- Introduzione
- Accountability e coadiuvanti in caso di controllo (Certificazioni e codici di condotta)
- **Misure di Sicurezza: adeguamento dei sistemi informativi e rapporti contrattuali con i fornitori**
- Il DPO

Misure di Sicurezza: adeguamento dei sistemi informativi e rapporti contrattuali con i fornitori

Protezione dati fin dalla progettazione e per impostazione predefinita:

(Art. 25) al momento di determinare i mezzi del trattamento e all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati

Misure di Sicurezza: adeguamento dei sistemi informativi e rapporti contrattuali con i fornitori

Responsabilità del titolare del trattamento: *[controller]*

(Art. 24) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
Se ciò è proporzionato rispetto alle attività di trattamento, le misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

Misure di Sicurezza: adeguamento dei sistemi informativi e rapporti contrattuali con i fornitori

Sicurezza del trattamento :

(Art. 32) il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Corrispondenza tra Regolamento UE e ISO/IEC 27001

Regolamento UE	ISO/IEC 27001
Interessati	Stakeholder
Dato Personale	Information asset
Violazione dei dati personali	Information security incident
Misure	Control
I rischi per i diritti e le libertà delle persone fisiche	Risk
Misure previste per affrontare i rischi	Risk management
Requisiti del regolamento	Control objectives

luigi.pavani@rina.org

Corrispondenza tra Regolamento UE e ISO/IEC 27001

Regolamento UE	ISO/IEC 27001
Affidamento di attività di trattamento	A.15 Supplier relationship
Protezione dati fin dalla progettazione e per impostazione predefinita	A.14.2 Security in development and support process A.11.1 Secure Areas
Responsabilità del titolare del trattamento	5 Leadership
Sicurezza del trattamento	La norma ISO 27001 per intero
Notifica di una violazione dei dati personali all'autorità di controllo	A.16 Information Security incident Management
Valutazione di impatto sulla protezione dei dati	6.1.2 Information security risk assessment
Responsabile della protezione dei dati	5.3 Organizational roles, responsibilities and authorities A.6.1.1 Information security Roles and Responsibilities

luigi.pavani@rina.org

Corrispondenza tra Regolamento UE e ISO/IEC 27001

Regolamento UE	ISO/IEC 27001
Sicurezza del trattamento	
a) la pseudonimizzazione e la cifratura dei dati personali;	A.10 Cryptography
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;	Il SGSI A.11.2 Equipment A.17.2 Redundancies
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;	A.16 Incident management A.17 Information Security Aspects of Business continuity management
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.	9 Monitor and measure A.18 Information security reviews

La Privacy e il Cloud

Il fornitore di cloud ***E'*** un responsabile del trattamento
Infatti i trattamenti sono:

la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

La Privacy e il Cloud

ISO/IEC 27018 - techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

A public cloud service provider is a ‘PII processor’ when it processes PII for and according to the instructions of a cloud service customer. The cloud service customer, who has the contractual relationship with the public cloud PII processor, can range from

- a natural person, a ‘PII principal’, processing his or her own PII in the cloud,
- to an organization, a ‘PII controller’, processing PII relating to many PII principals.

La Privacy e il Cloud

ISO/IEC 27018 - techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
Requisiti aumentati (rispetto alla ISO 27002)

5.1.1 Policies for information security
Control 5.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Public cloud PII protection implementation guidance
The information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers).

Privacy Impact Analysis

Sezione 3

Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Articolo 35

Valutazione d'impatto sulla protezione dei dati

1. 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, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

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

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

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

luigi.pavani@rina.org

Privacy Impact Analysis

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

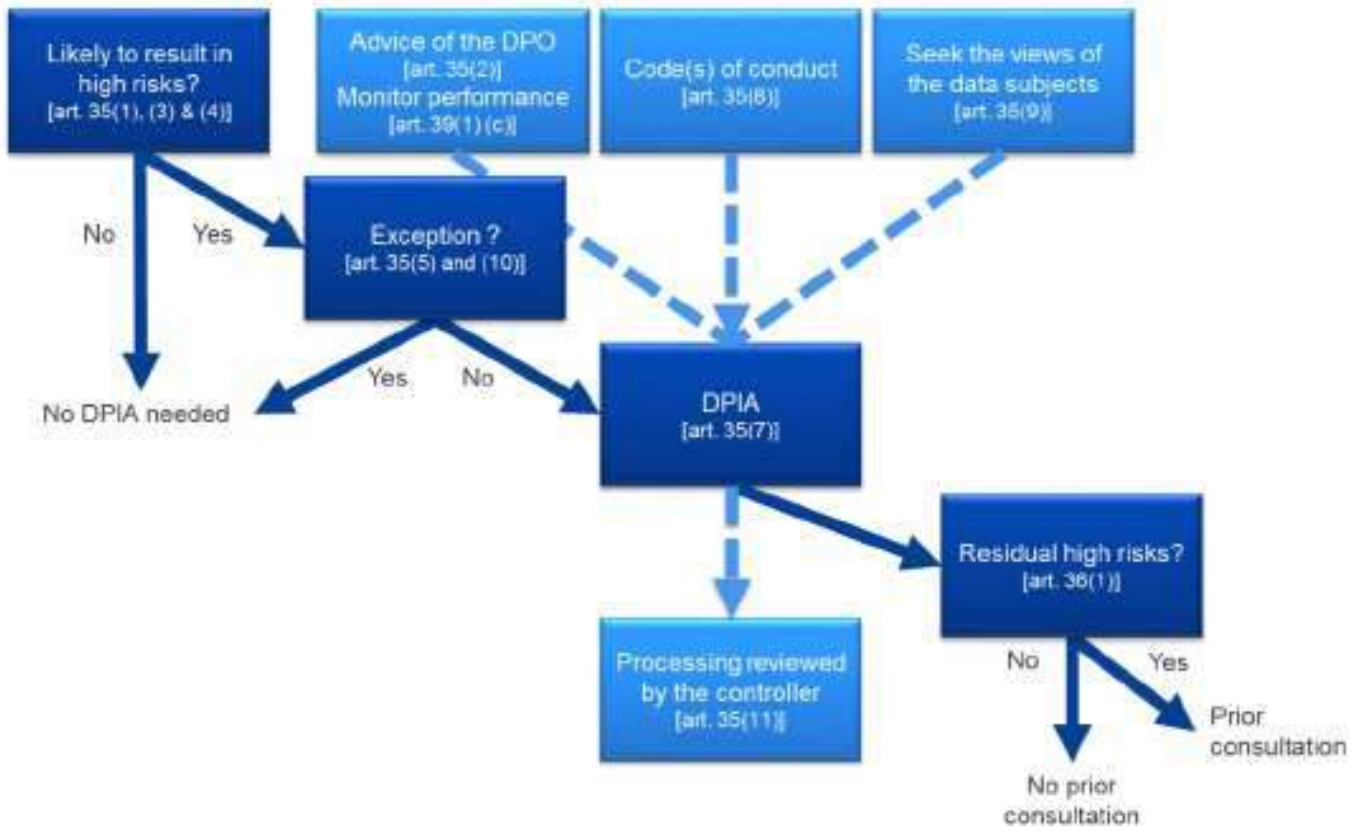
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Privacy Impact Analysis



luigi.pavani@rina.org

Privacy Impact Analysis

Linea Guida

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk the following criteria should be considered

1. Evaluation or scoring, including profiling and predicting

2. Automated-decision making with legal or similar significant effect

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "*a systematic monitoring of a publicly accessible area*"

Privacy Impact Analysis

Sensitive data: this includes special categories of data as defined in Article 9 (for example information about individuals' political opinions)

Data processed on a large scale:
a. the number of data subjects, either as a specific number or as a proportion of the relevant population;
b. the volume of data and/or the range of different data items being processed;
c. the duration, or permanence, of the data processing activity;
d. the geographical extent of the processing activity.

The controller (titolare) is responsible to ensure that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.

Luigi Pavani
Business Development Manager
RINA SERVICES S.p.A.

Via Corsica, 12
16128 Genoa - Italy
Ph. +39 010 5385619
Cell+39 335 6625047
luigi.pavani@rina.org
www.rina.org