ISACA
Al servizio dei professionisti dell'IT Governance
Rome Chapter

Capitolo di Roma

NUOVA REGOLAMENTAZIONE PRIVACY EUROPEA - IL QUADRO DEGLI OBBLIGHI E DELLE MISURE

SEMINARIO SICUREZZA E PRIVACY ISACA Roma

5 Maggio 2016

Luciano Delli Veneri
Gloria Marcoccio

Crediti ed attestati

Crediti ISACA

- 4CPE validi per il mantenimento delle certificazioni CISA, CISM, CRISC, CGEIT e per tutte le associazioni che riconoscono i CPE

Attestato di partecipazione ISACA

Abstract

La nuova regolamentazione privacy europea (General Data Protection Regulation GDPR) introduce un nuovo quadro di obblighi e misure, valide in ogni scenario di business, applicabili sia nel settore privato sia in quello pubblico, che devono essere rispettate dalle organizzazioni stabilite nella UE ed anche dalle organizzazioni extra UE che offrono servizi e/o effettuano attività di monitoring in ambito UE.

Il GDPR ha notevoli impatti per il business ed in caso di inadempienze sono previste elevate sanzioni pecuniarie.

Il seminario organizzato da ISACA ROMA fornisce una panoramica sulle novità introdotte dal nuovo Regolamento, con particolare riguardo agli aspetti che hanno un diretto impatto sulle necessarie misure tecniche organizzative e procedurali.

Di che si tratta?
Cosa cambia rispetto alla attuale normativa UE ed Italiana?
Quali i cambiamenti sul fronte dei Titolari di trattamento? e dei Responsabili di trattamento?
Quali nuovi processi di controllo occorre gestire?
Quali le novità sul piano pratico in termini di misure tecniche/organizzative/procedurali?
Data Breach?/Privacy by Design? Privacy by Default?

Programma

PRIMA PARTE - OVERVIEW

Il nuovo regolamento e sue relazioni con la direttiva europea sulla privacy 95/46/EC
Perché una nuova regolamentazione europea per la protezione dei dati personali
Aspetti temporali e di validità rispetto alle esistenti leggi e provvedimenti del Garante privacy in Italia
Campo di applicazione territoriale
Panoramica sulle nuove prescrizioni ed il quadro sanzionatorio
Le principali differenze rispetto la direttiva europea sulla privacy 95/46/EC

Break

SECONDA PARTE – ASPETTI ED APPROFONDIMENTI PRINCIPALI

Le responsabilità del Titolare di trattamento
Le responsabilità del Responsabile di trattamento
Il principio di Accountability (Responsabilizzazione) e la registrazione delle attività di trattamento
Profilazione
Privacy by design e privacy by default
Privacy Impact Assessment (Valutazione di impatto sulla protezione dei dati)
Prior Consultation (Consultazione Preventiva)
Data Breach (Violazione dei dati personali)
Misure di sicurezza ed analisi dei rischi
Informativa e consenso
La tutela dei minori
Esercizio dei diritti degli interessati (portabilità, diritto all'oblio,...)
La nomina del Data Protection Officer (Responsabile della protezione dei dati)

Q&A

Docenti

Luciano Delli Veneri – luciano.delliveneri@gmail.com

Privacy e Compliance Manager con oltre 10 anni di esperienza nell'applicazione della normativa sulla privacy maturata inizialmente nella articolata realtà della TLC, con complessità rilevanti e, successivamente, curandone l'applicazione presso società del terziario, del settore energetico, Università. Ha progettato, implementato e governato i sistemi privacy aziendali curando direttamente gli adempimenti e la valutazione preventiva della compliance dei nuovi prodotti/servizi. Ha gestito le relazioni con il Garante assicurando i riscontri ai provvedimenti, ai ricorsi, alle richieste di informazioni e nelle visite ispettive. Ha conseguito la certificazione "Privacy Officer e Consulente della Privacy" con TÜV Italia.

Gloria Marcoccio – gloria.marcoccio@glory.it

Dottore ingegnere con master in Information Technology Laws, esperta nella applicazione in contesti operativi delle normative nazionali ed internazionali applicabili ai servizi della information & networked society. Consulente senior nel settore TLC e difesa con 30 anni di esperienza maturata in molteplici contesti operativi presso primarie organizzazioni internazionali, tra cui la Commissione Europea e gruppi multinazionali nel settore delle telecomunicazioni e della difesa. Ha scritto numerosi articoli riguardo la protezione dei dati e privacy, articoli scientifici in materia di data fusion e algoritmi per l'elaborazione dei dati. Lead Auditor ISO27001 e certificata "Privacy Officer e Consulente della Privacy " con TÜV Italia.

Perché una nuova normativa privacy Europea

La legge cardine a livello UE in materia di protezione dati personali è la Direttiva 95/46/CE, adottata nel 1995 con l'obiettivo di:

proteggere i diritti fondamentali e garantire il libero flusso di dati personali tra i Paesi Membri UE

Nel tempo sono poi arrivate le normative privacy:

- **specifiche per il settore delle telecomunicazioni, la principale: Direttiva 2002/58/CE**
- **la normativa privacy apposita per le istituzioni UE: Regolamento 45/2001**

Il trattamento dei dati personali è inevitabilmente presente al 99% in tutti i settori della nostra vita sociale e professionale.

La creazione delle condizioni che agevolano e promuovono il business UE dipendono anche dalla normativa in materia di protezione dati personali, che gioca un ruolo essenziale - ora e nel futuro - per la Digital Agenda for Europe e più in generale per la Europe 2020 Strategy.

Perché una nuova normativa privacy Europea

Nel corso di questi anni

- **il trend della globalizzazione ed esternalizzazione dei servizi**
- **gli sviluppi tecnologici**
- **la nascita ed il successo di nuovi servizi della Information and Networked Society**

hanno totalmente cambiato il quadro di riferimento per le prescrizioni presenti nella direttiva privacy 95/46/EC entrate in vigore 20 anni fa.

La direttiva privacy 95/46/EC <u>con le sue 28 diverse trasposizioni nel paesi Membri UE</u> ha comportato e continua a comportare un quadro normativo frammentario e disomogeneo, che ha creato e crea squilibri, condizioni di sbilanciamento e diversità di regole per le organizzazioni (aziende, enti,...) che fanno business nella UE, ricomprese tra queste anche le organizzazioni extra UE.

Il nuovo pacchetto di norme privacy europeo

A partire dal 2012 la Commissione Europea ha quindi proposto al Parlamento ed al Consiglio Europeo una profonda revisione ed aggiornamento della normativa privacy europea

Il primo fondamentale obiettivo raggiunto – *approvato dal Parlamento Europeo il 14 Aprile 2016* - il Pacchetto di norme costituito da:

- **Il Regolamento Privacy Europeo per la protezione degli individui con riferimento al trattamento dei loro dati personali e relativo libero flusso nella UE**

  (abroga e sostituisce la Direttiva Privacy 95/46/EC)

- **La Direttiva privacy specifica per regolare la protezione dei dati personali da parte delle autorità competenti a fini di prevenzione, ricerca, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati**

  (in luogo della precedente apposita 'Framework Decision 2008/977/JHA')

Questo seminario focalizza l'attenzione sul Regolamento GDPR

Dalla Direttiva al Regolamento

La Direttiva 95/46/CE costituisce il primo corpo normativo che a livello comunitario è stato adottato per garantire la protezione dei dati personali

Direttiva e non Regolamento perché vi era una grossa disomogeneità tra i diversi paesi aderenti molti dei quali non avevano ancora nessuna norma specifica nel proprio ordinamento destinata a garantire la protezione dei dati personali e quindi si lasciarono più ampi margini al legislatore nazionale.

Entrata in vigore del Regolamento

- Approvazione ufficiale del Parlamento il **14 Aprile 2016**
- **Regolamento n. 2016/679 pubblicato in GUCE n. 119 del 4 maggio 2016**
- Entrata in vigore i**l ventesimo giorno** successivo alla pubblicazione nella Gazzetta ufficiale UE.
- Effettiva applicazione a decorrere **da due anni dalla sua entrata in vigore.**

Nonostante il Regolamento generale non sia da recepire con normative nazionali, ci saranno diversi aspetti che dovranno essere disciplinati dall'Autorità Garante nazionale.

Verosimilmente, il Garante dovrà, per ognuno dei Provvedimenti e Linee Guide di carattere generale emessi fino ad oggi, valutarne la "coerenza complessiva" e la conformità rispetto al Regolamento, dovendo quindi decidere se modificarli ovvero dichiararli non applicabili

Entrata in vigore del Regolamento

Text

ISSN 1977-0677

Official Journal **L 119**

of the European Union

English edition

Legislation

Volume 59
4 May 2016

Contents

I Legislative acts page

REGULATIONS

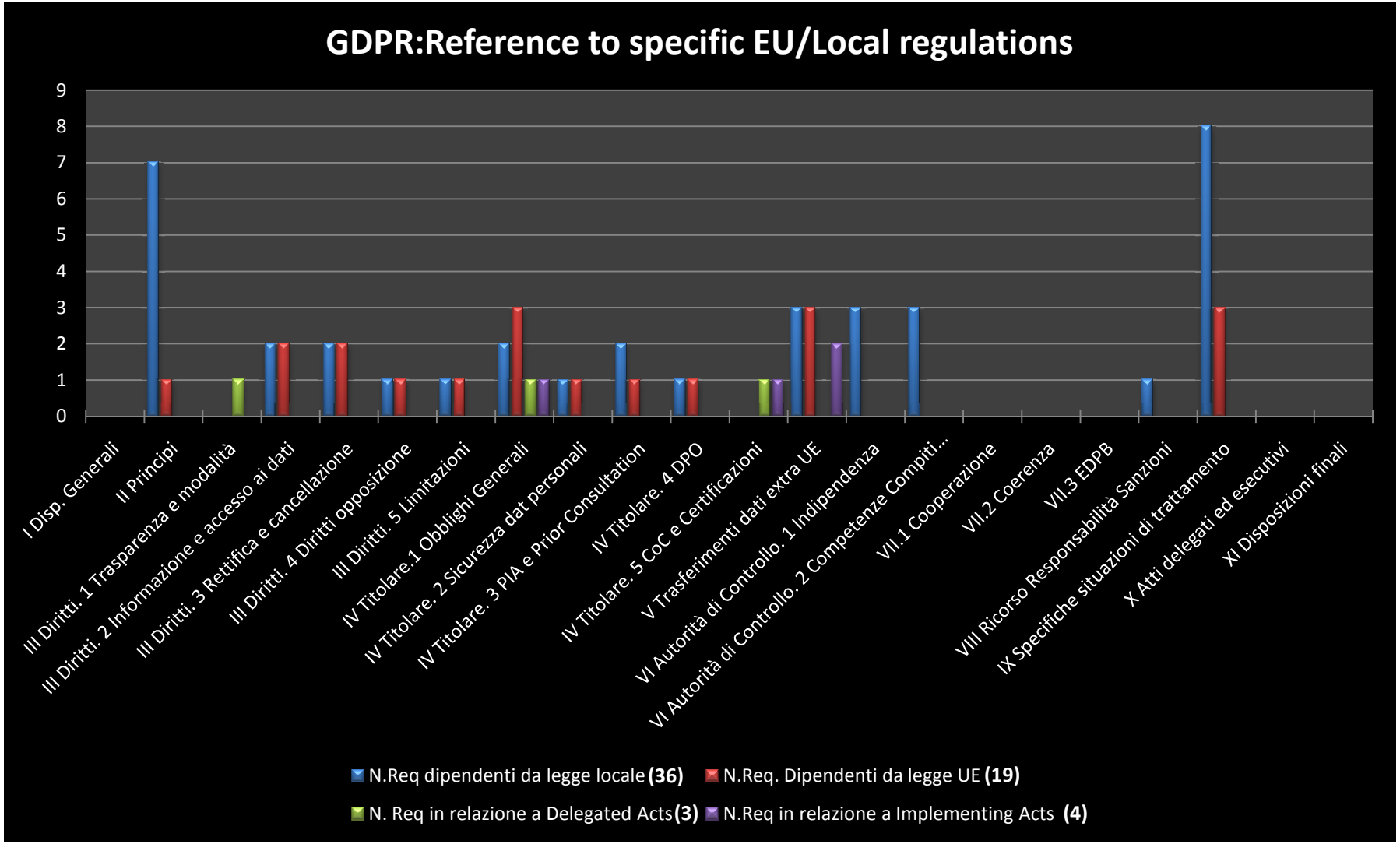
* **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ([1])** 1

DIRECTIVES

* **Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA** 89

* **Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime** 132

Entrata in vigore del Regolamento



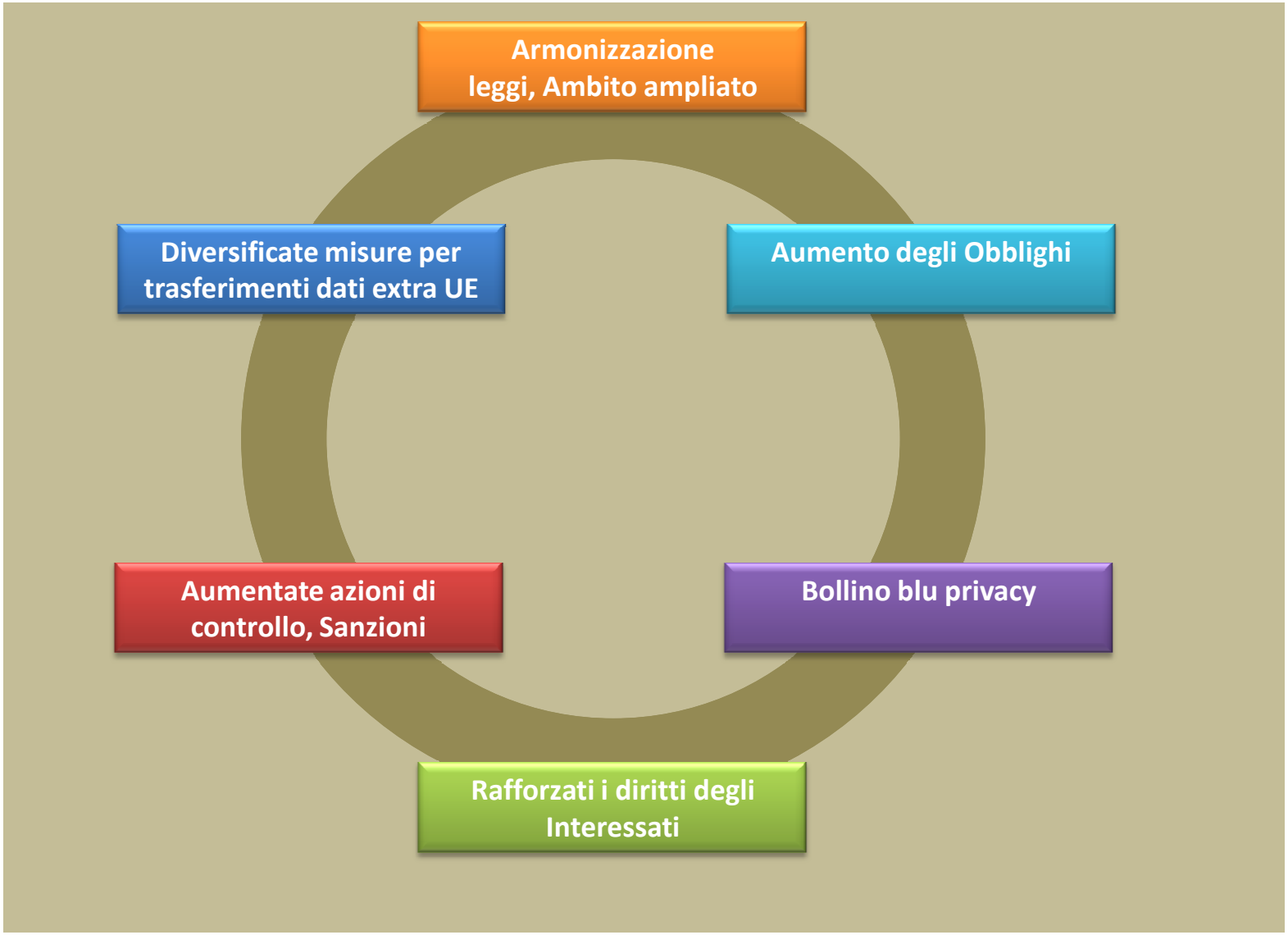
Entrata in vigore del Regolamento

Il Codice privacy non ha recepito solo la Direttiva 95/47/CE ma costituisce un testo organico che integra anche altre Direttive quali la 2002/58/CE

QUINDI

Sarà necessaria una attività ermeneutica per poter definire quali parti del Codice privacy vengono abrogati dal nuovo Regolamento comunitario

Panoramica dei punti chiave del GDPR



Panoramica dei punti chiave del GDPR

Armonizzazione leggi, Ambito ampliato

<u>Riduzione degli oneri amministrativi</u>
non richieste Notifiche di trattamento ai Garanti privacy

<u>One-Stop-Shop</u>
per le multinazionali, unico Garante privacy nella UE

<u>Interesse legittimo</u>
maggior spendibilità come base legale per effettuare trattamenti

<u>Ambito territoriale</u>
organizzazioni stabilite nella UE ed organizzazioni extra UE con business e/o attività di monitoring inidrizzati verso individui nella UE; Titolari e Responsabili extra UE devono nominare un loro Rappresentante UE per la privacy

Panoramica dei punti chiave del GDPR

Aumento degli Obblighi

Accountability
Obbligo per i Titolari di adempiere e dimostrare di adempiere ai principi ed alle misure richieste dal GDPR

Consenso
Rimane approccio Opt In, esplicito onere di dimostrare l'avvenuta acquisizione del consenso e di semplicità e chiarezza nel richiederlo UE, consenso parentale richiesto per i minori di anni 16 (con opzione per i paesi UE di spostare il limite a)

Privacy by design e by default
Misure da implementare preventivamente e durante l'esecuzione dei trattamenti

Privacy Impact Assessment
Analisi impatti privacy prima di effettuare un trattamento, in caso di Rischi Elevanti occorre richiedere la Prior Consultation del Garante

Data Breach
Notifica al Garante Privacy entro 72 ore, in alcuni casi necessario darne comunicazione anche agli Interessati

DPO Data Protection Officer
Nuova figura obbligatoria per le pubbliche amministrazioni e per le aziende (sia Titolari sia Responsabili) per particolari tipi di trattamento dati

Aumento degli impegni e responsabilità dirette dei Responsabili
Maggior oneri per i Responsabili (verso i Titolari, verso i propri Provider, nuovi adempimenti, responsabilità di fronte la legge)

Panoramica dei punti chiave del GDPR

Bollino blu privacy

<u>Codici di Condotta Privacy</u>

Il GDPR promuove la definizione ed utilizzo di Privacy CoC e le organizzazioni che li adotteranno potranno beneficiare dei vantaggi connessi alla valenza dei Codici quali evidenza della compliance rispetto ad alcuni adempimenti privacy (misure di sicurezza, trasferimento dati extra UE,…).

I Privacy CoC devono preventivamente essere approvati dalle autorità Garanti Privacy

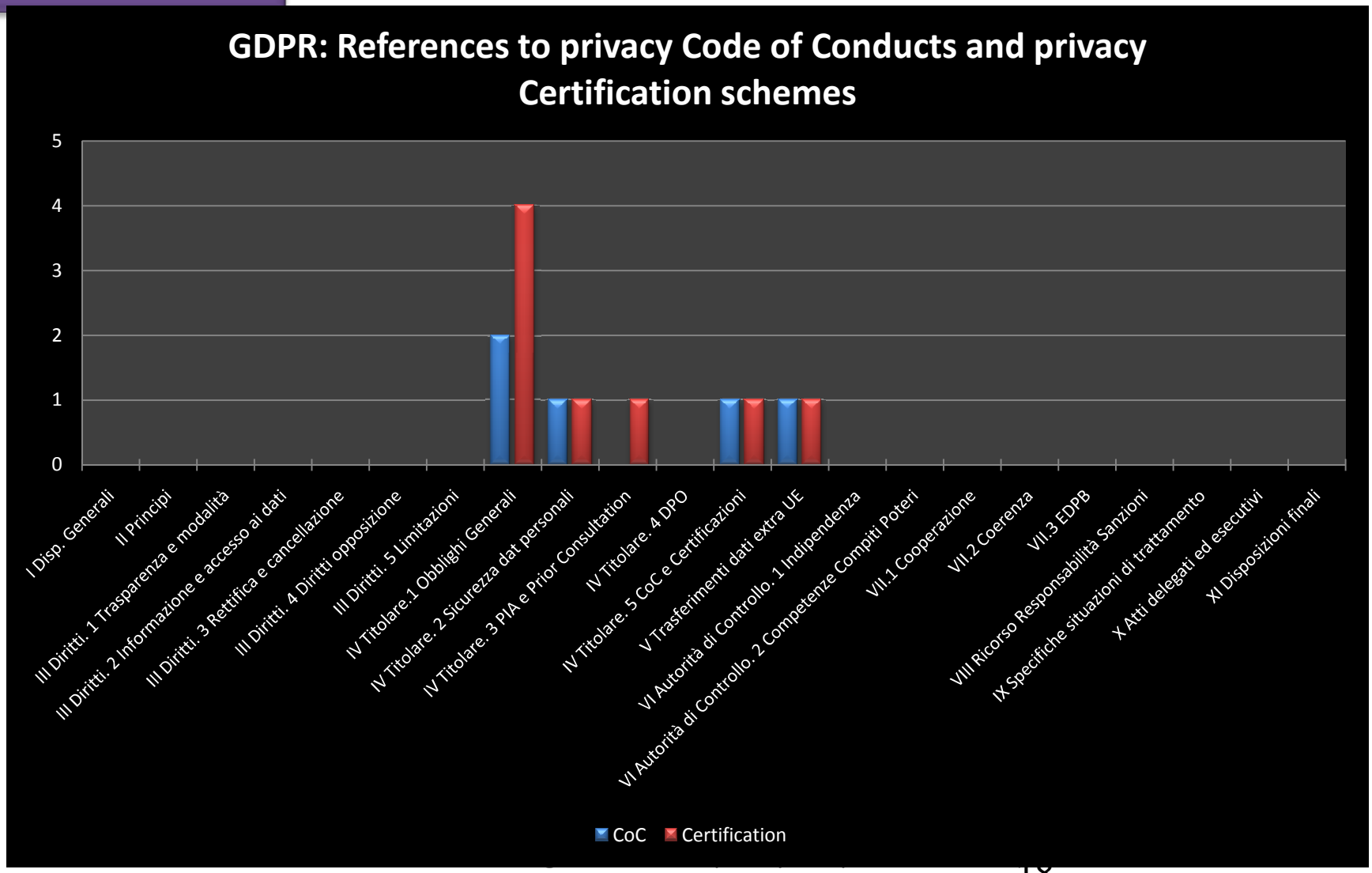
<u>Certificazioni Privacy</u>

Il GDPR promuove la definizione ed utilizzo di Certificazioni Privacy. Anche i questo caso le organizzazioni che si certificano dimostrano di essere compliant rispetto ad alcuni adempimenti privacy (caratteristiche di affidabilità dei Responsabili, misure di sicurezza, trasferimento dati extra UE,…).

I sistemi di certificazioni Privacy devono preventivamente essere approvati dalle autorità Garanti Privacy. È prevista la costituzione di enti di controllo ad hoc.

Panoramica dei punti chiave del GDPR

Bollino blu privacy



Panoramica dei punti chiave del GDPR

Bollino blu privacy

	TESTO ARTICOLO	CoC	Certification
Articolo 24 Responsabilità 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.	x	x
Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita	3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.		x
Articolo 28 Responsabile del trattamento	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.	x	x
Articolo 28 Responsabile del trattamento	6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.		x
Articolo 32 Sicurezza del trattamento	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.	x	x
Articolo 35 Valutazione d'impatto sulla protezione dei dati	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.		x
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.	x	
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.		x
Articolo 46 Trasferimento soggetto a garanzie adeguate	e) un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo 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; o	x	
Articolo 46 Trasferimento soggetto a garanzie adeguate	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.		x

Panoramica dei punti chiave del GDPR

Rafforzati i diritti degli Interessati

Informativa
Espressa diversificazione delle informative in caso di raccolta dei dati direttamente presso l'Interessati o meno, richiesto un maggior contenuto informativo ma allo stesso semplicità e chiarezza, promosso il ricorso a particolare ICONE semplificative stabilite/autorizzate delle autorità Garanti privacy

Diritti di Opposizione
Diritti di opporsi in ogni caso per motivi legittimi al trattamento e diritto di opporsi alla profilazione o al trattamento per legittimo interesse.

Data Portability
Diritto di ricevere indietro i dati in un formato standard e machine-readible senza oneri aggiuntivi, previsto anche la possibilità di richiedere il trasferimento diretto dei dati da un Titolaread un altro

Diritto all'oblio
Diritto di ottenere la cancellazione dei dati, anche se resi pubblicamente disponibile, salvo che non prevalgano diritti di altri (es diritto di cronaca, etc)

Profilazione
Maggior controllo degli Interessati su profilazioni in base alla raccolta dei loro dati personali

Panoramica dei punti chiave del GDPR

Aumentate azioni di controllo e Sanzioni

<u>Risarcimenti da parte di Titolari e Responsabili</u>
In caso di danni agli Interessati in relazione al trattamento dei loro dati personali

<u>Ricorsi verso Titolari e Responsabili</u>
Promossi dagli Interessati in caso di trattamenti dati non conformi al GDPR, presso le autorità Garanti Privacy o via giudiziarie ordinarie

<u>Aumentati poteri di controllo delle autorità Garanti Privacy</u>
Poteri investigativi, correttivi, autorizzativi e consultivi
Poteri di imporre sanzioni pecuniarie di elevato valore (milioni di euro)

<u>EDPB European Data Protection Board</u>
Nuovo organismo privacy a livello europeo dotato di personalità giuridica, nasce dal già presente Working Party 29, dotato di maggiori ambiti e poteri di intervento (es Consistency Mechanism)

Panoramica dei punti chiave del GDPR

Diversificate misure per trasferimenti dati extra UE

<u>Decisioni UE di adeguatezza privacy di paese terzo o organizzazione internazionale</u>
Stabilite con decisione UE , non necessitano di autorizzazione del Garante privacy nazionale

<u>Clausole Contrattuali Standard a livello UE</u>
Stabilite con Decisione UE, non necessitano di autorizzazione del Garante privacy nazionale

<u>Clausole Contrattuali Standard a livello nazionale</u>
Stabilite dal Garante privacy nazionale, sottoposte a check EDPB

<u>Clausole Contrattuali ad hoc a livello nazionale</u>
Stabilite dal Garante privacy nazionale ad hoc

<u>BCR Binding Corporate Rules</u>
Stabilite con procedura EDPB, riguardano il caso di multinazionali, sia per il caso Titolare che Responsabile

<u>Esenzioni</u>
Trasferimenti ammessi in caso di rapporti contrattuali e pre, consenso Interessati, …., per alcuni casi di legittimo interesse-trasferimenti saltuari ma a determinate, esistenza e dimostrata aderenza ad appositi Privacy CoC o Certificazioni Privacy

Ambito di applicabilità territoriale del GDPR

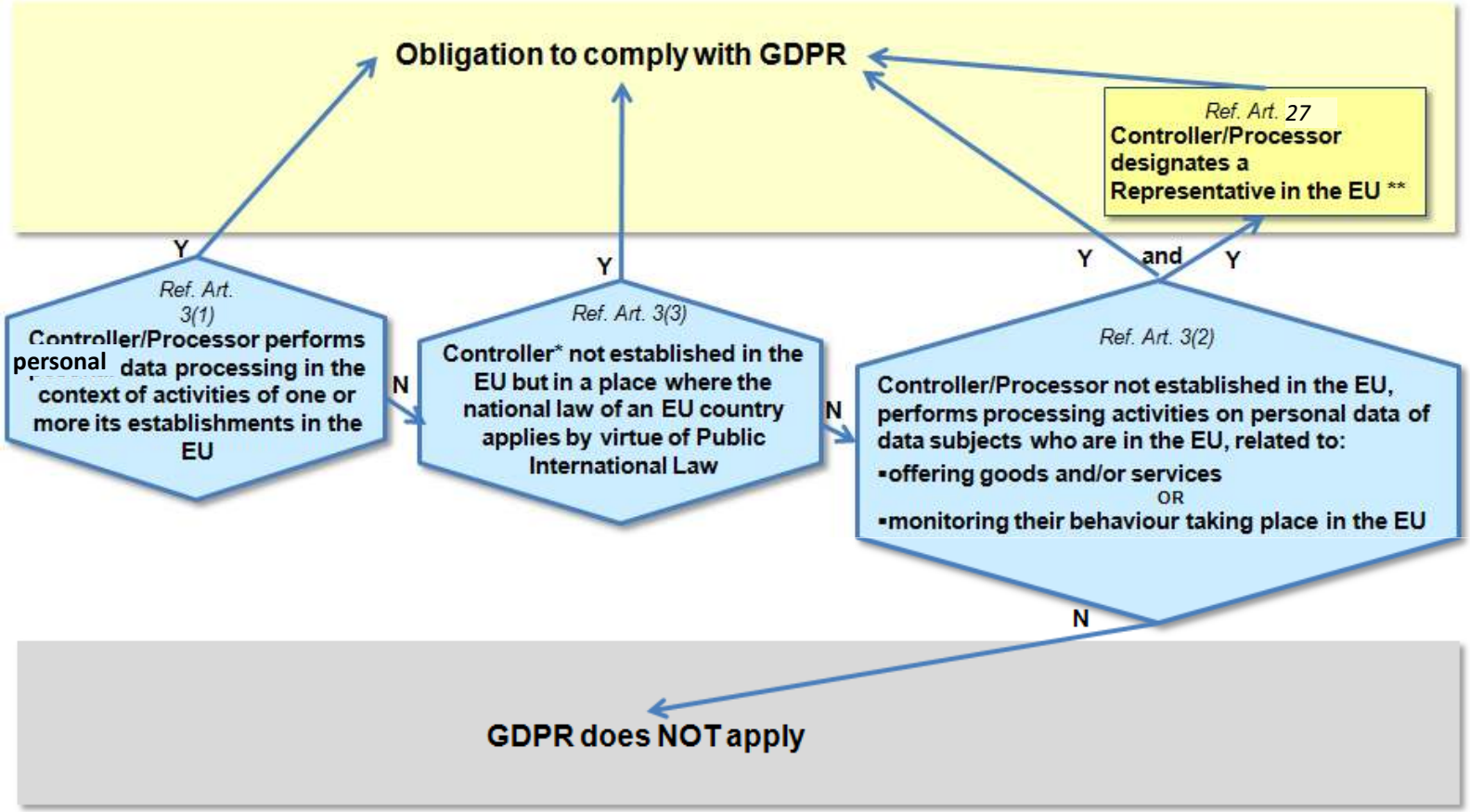
Le disposizioni del GDPR si applicano a Titolari e Responsabili:

- ✓ stabiliti con le proprie attività in uno o più Paesi Membri UE

- ✓ Stabiliti al di fuori della UE ma con attività di trattamento dati, di individui che si trovano nella UE, in relazione a:
  - Offerta di beni e/o servizi anche se non remunerati

  oppure
  - Attività di monitoraggio del comportamento

Ambito di applicabilità territoriale del GDPR



*Maybe a typo in the GDPR text officially available, since it is reasonable that such requirement is addressed both to Controllers and Processors

** This obligation does not apply to

- processing which is occasional, does not include, on a large scale, processing of special categories of data (sensitive data,…see Article 9(1)) or processing of data relating to criminal convictions and offences, and is unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing [please note: this requires accountable decision by relevant Controller/Processor]
- a public authority or body

Ulteriori commenti nell'articolo **"European General Data Protection Regulation - Territorial Scope at a glance"**

Quadro Sanzionatorio

Amministrative

Max10 milioni di euro [in caso di imprese fino al 2% del fatturato se superiore a 10 milioni di euro]

- Consenso per minori
- Misure di sicurezza
- Accountability
- Principi di Privacy by Design by Default
- Prior Consultation
- Adempimenti in generale del Titolare del Responsabile e del Rappresentante (di Titolare non UE)
- Data Breach notifica al Garante Privacy
- Privacy Impact Assessment
- Data Protection Officer
- Aderenza alle Certificazioni privacy

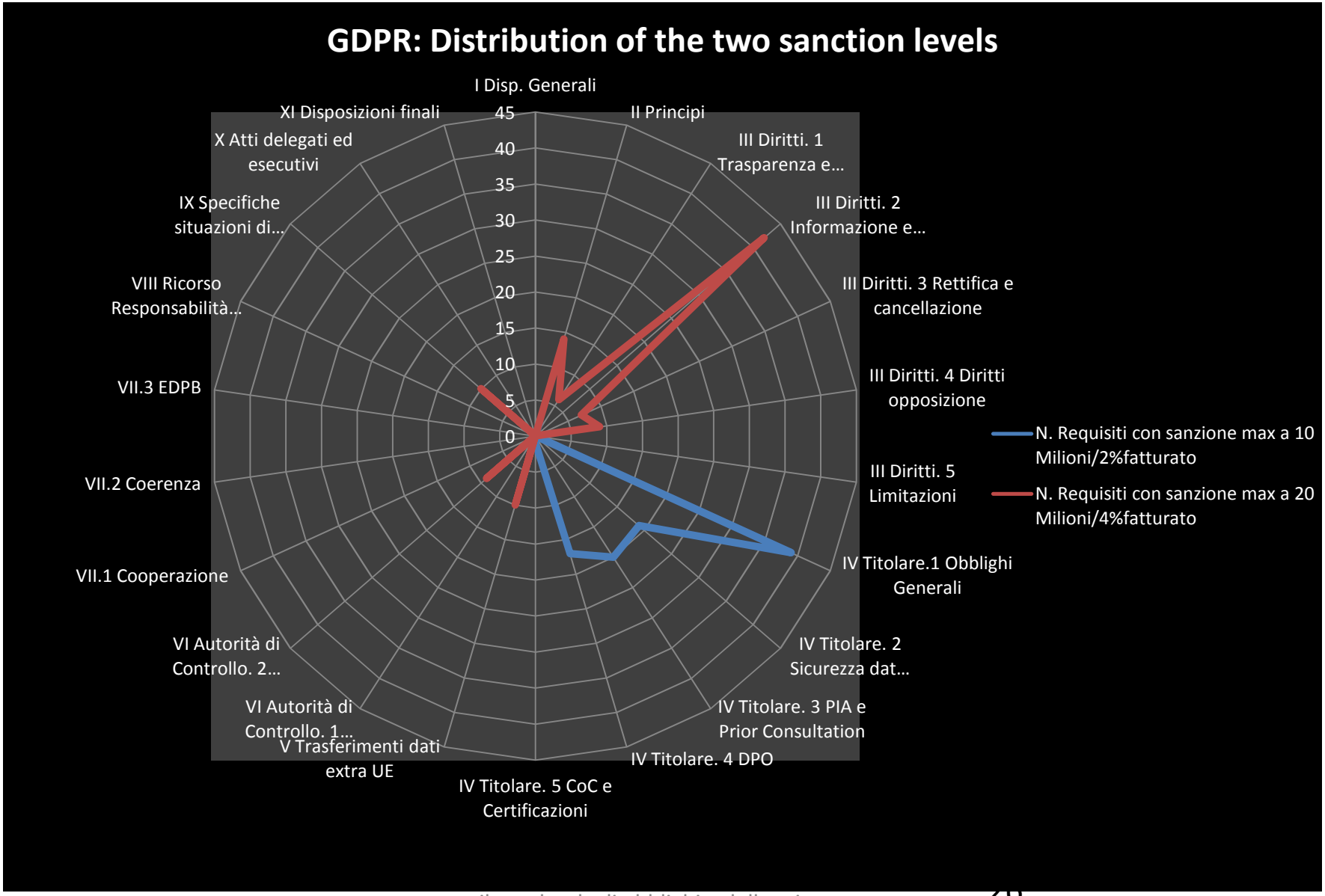
Max 20 milioni di euro [in caso di imprese fino al 4% del fatturato se superiore a 20 milioni di euro]

- Regole per raccolta e documentazione del Consenso
- Principi di correttezza e liceità dei trattamenti,
- Diritti degli Interessati
- Trasferimenti di dati extra UE
- Ordini emessi dal Garante privacy
- Data Breach comunicazione agli Interessati
- Rispetto specifici divieti di trattamenti
- Rispetto obblighi per specifici casi es. dati dei lavoratori nel contesto del rapporto di lavoro)

Penali

Il GDPR richiede agli Stati Membri di stabilire le sanzioni penali da applicare

Quadro Sanzionatorio



Punti di attenzione per azioni di adeguamento al GDPR

Gestione Accountability	**Attestazione documentata degli adempimenti privacy presi in carico; controllo sui trattamenti effettuati, responsabilità e compiti assegnati, misure di sicurezza implementate**
Gestione Data Breach	**Definizione ed implementazione di piani di gestione e relativa organizzazione e test, utilizzo di strutture informative per documentare gli eventi di Data Breach, organizzazione e mezzi per rispettare le tempistiche di legge**
PIA	**Definizione ed implementazione di metodi per condurre, documentare e gestire nel tempo le attività di PIA ed eventuali conseguenti Prior Consultation con il Garante Privacy**
Misure contrattuali Titolare-Responsabili	**Definizione/Aggiornamenti clausole ed istruzioni, gestione della casistica dei Responsabili in 'cascata'**
Misure contrattuali trasferimento dati extra UE	**Definizione//Review/Aggiornamenti degli strumenti legali adottati per il trasferimento dati, contrattualistica conseguente, inventory dei casi di trasferimento in essere**
Gestione esercizio dei diritti, consenso informato	**Review/Aggiornamento delle procedure e dei testi per gestione informativa e consensi Procedure integrate per l'esercizio dei diritti nel rispetto delle tempistiche di legge**
Formazione	**Formazione del personale preposto ai trattamenti dati personali**
Data Protection Officer	**Per le aziende che devono prevedere tale figura: assegnazione dei compiti e gestione delle comunicazioni ed operatività previste dal Regolamento**
Gestione one-stop-shop	**Per le aziende che fanno business in più Stati Membri UE: adozione ed implementazione di procedure per il rapporto con la Lead Privacy Authority**
Raccordi con normative correlate	**Gestione raccordi normativi nei riguardi degli adempimenti D.Lgs 231/01 e coordinamento con altre compliance aziendali (es. normativa giuslavoristica)**

Direttiva vs Regolamento

	Direttiva 95/46	**Regolamento sulla protezione dei dati personali**
CONSENSO	possibile sia regime di opt-in che opt-out quindi anche forme "implicite"	È necessario che vi sia un forma "esplicita" ed inequivocabile
NOTIFICAZIONE	previsto l'obbligo di notificare alcune tipologie di trattamenti	Nessun obbligo; tutto demandato alla accountability ed alla PIA
TIPOLOGIE DEI DATI	personali sensibili giudiziari	I dati Sensibili diventano "Particolari"; Viene introdotta la definizione dei dati: **genetici;** **biometrici;** **pseudo-anonimi**;
DIRITTI DELL'INTERESSATO	conferma del trattamento, accesso ai dati, rettifica,cancellazione, limitazione e/opposizione per determinate finalità o operazioni di trattamento	**Diritto all'oblio;** **Diritto alla portabilità dei dati;**

Direttiva vs Regolamento

	Direttiva 95/46	**Regolamento sulla protezione dei dati personali**
TITOLARE DEL TRATTAMENTO	Definizione e ambiti di responsabilità descritti in forma molto light	Indicati gli oneri connessi alla titolarità: Privacy by design e by default; Misure idonee in relazione ai trattamenti; Autonoma valutazione dei rischi (PIA); Documentazione dei trattamenti e self assessment periodico di verifica.
RESPONSABILE DEL TRATTAMENTO	Definizione e ambiti di responsabilità descritti in forma INDIRETTA	Accountability diretta del Responsabile anche in ordine al risarcimento del danno; Contratto o altro atto giuridico per regolare i rapporti con il Titolare; Possibile impiego di sub-fornitori con delega del Titolare.
DATA PROTECTION OFFICER	Figura non prevista	Obbligatorio per la PA e in caso di monitoraggio regolare e sistematico su larga scala e trattamento su larga scala di dati sensibili e giudiziari; “suggerito” per gli altri Titolari in quanto figura che svolge un ruolo di cerniera nei confronti della Autorità; Esperto di protezione dati sia per gli aspetti legali che tecnici. Dipendente o Consulente con ampi margini di autonomia

Break

Seconda parte

Il Data Controller – Titolare del Trattamento

Il Titolare del trattamento è tenuto a:

- **adottare soluzioni e strumenti "pensati" in ottica "privacy by design e by default";**
- i**mplementare opportune misure di sicurezza** che tengano conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche;
- **dimostrare la conformità delle operazioni di trattamento** rispetto ai principi sanciti dal Regolamento, ad esempio tramite:
  - misure tecniche e organizzative;
  - adeguate policy e procedure in materia di protezione dei dati;
  - registro delle categorie di attività di trattamento (per taluni casi è un obbligo);
  - adesione a codici di condotta approvati;
  - adesione a un meccanismo certificazione approvato;
  - Data Protection Officer (nel caso non sia obbligatoria la sua presenza).

Il Data Controller – Titolare del Trattamento

Il Titolare del trattamento è tenuto a:

- effettuare la **Privacy Impact Assessment** (PIA) in tutte le circostanze nelle quali la tipologia dei dati ed i relativi trattamenti lo rendano necessario;

- implementare strumenti e procedure atte a rilevare tempestivamente **violazioni nel trattamento dei dati personali** (Data breach) notificando entro 72 ore l'accaduto all'Autorità garante;

- notificare la violazione agli Interessati nel caso vi siano rischi rilevanti per la tutela dei loro dati personali nonché rischi per i loro diritti e libertà;

Il Data Processor – Responsabile del Trattamento

Il Responsabile del trattamento è tenuto a:

- trattare i dati personali eseguendo le istruzioni ricevute dal Titolare;
- assicurare che tutti coloro che trattano i dati personali su sue indicazioni si siano impegnate a rispettare i vincoli di riservatezza;
- implementare e mantenere tutte le misure tecniche e organizzative adeguate;
- cooperare con il Titolare del trattamento per la gestione delle richieste di diritto d'accesso e per gli altri obblighi imposti dal Regolamento;
- su richiesta del Titolare cancellare o restituire i dati personali al termine del trattamento;
- fornire al Titolare qualsiasi informazione necessaria per dimostrare il rispetto del Regolamento
- prevedere al presenza del Data Protection Officer ove prescritto o in vista delle caratteristiche dei trattamenti effettuati.

Il Data Processor – Responsabile del Trattamento

Il Responsabile deve essere individuato dal Titolare anche in funzione delle garanzie di professionalità e competenza che presenta per la corretta applicazione e l'adozione di misure tecniche ed organizzative richieste dal Regolamento.

Attenzione: l'affidamento di un trattamento al Responsabile del trattamento deve essere **regolamentato da un contratto o da altro atto giuridico** che indichi con chiarezza gli obblighi in capo al soggetto designato.

In particolare il contratto deve disciplinare quanto relativo a:

- Oggetto
- Durata
- Natura e finalità del trattamento
- Tipologia dei dati
- Categorie di interessati
- Obblighi e diritti del data controller

Il Data Processor – Responsabile del Trattamento

Quindi per il Regolamento il **Responsabile del trattamento** ha un ruolo nuovo e più ampio rispetto a quanto prevedeva la Direttiva 95/46/CE.

In particolare:

- svolge un ruolo di più stretta collaborazione con il Titolare del trattamento;
- assume maggiori rischi connessi ad una sua immediata e diretta responsabilità relativamente ai trattamenti a lui affidati;
- costituisce un diretto interlocutore sia per l'Interessato che per le Autorità di controllo;
- risponde dell'eventuale attività di terzi suoi fornitori dovendo garantire il rispetto dell'applicazione della normativa da parte di tali soggetti.

Il Data Processor – Responsabile del Trattamento

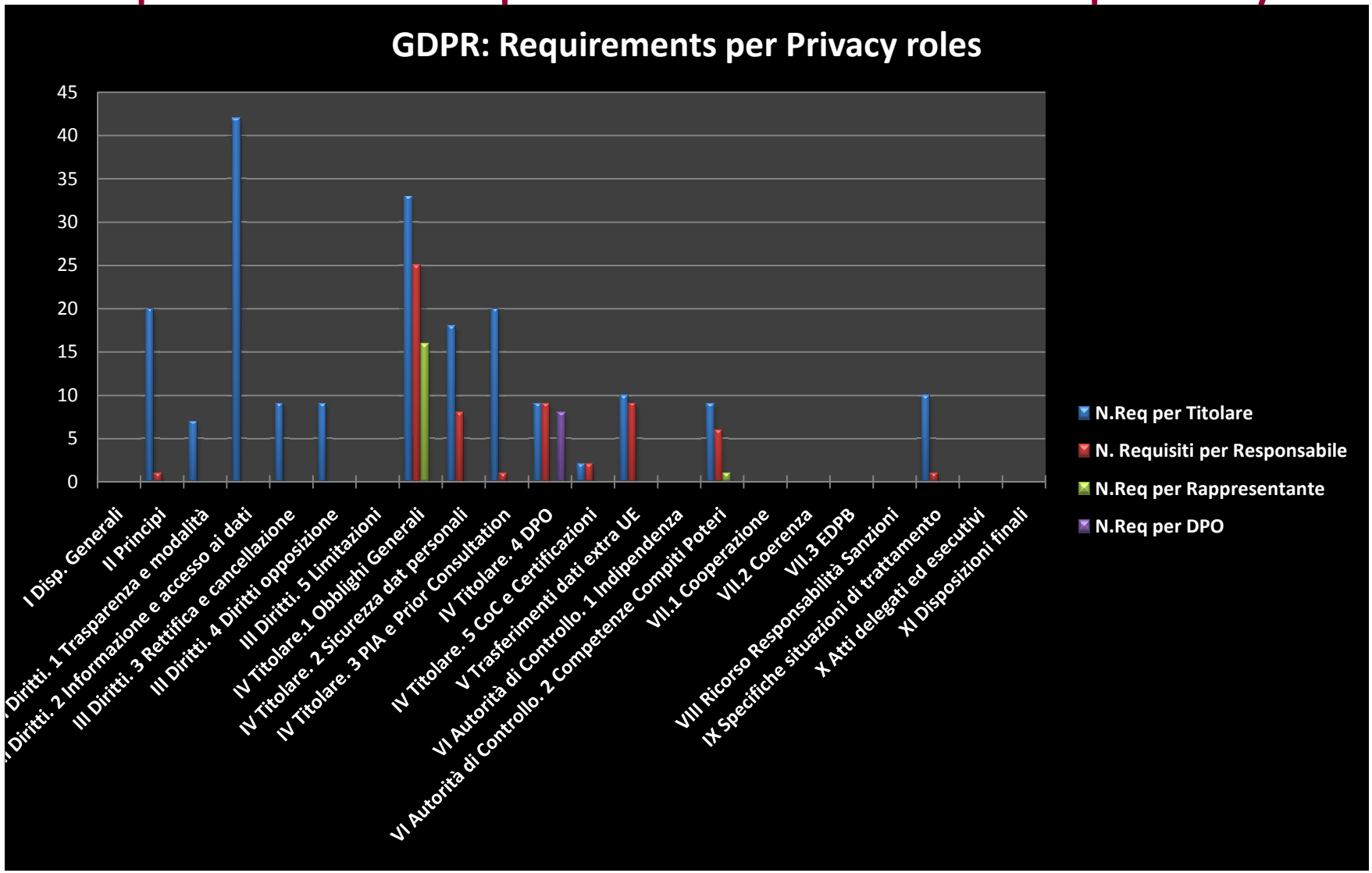
Il Responsabile del trattamento **può avvalersi di un altro soggetto** avendo ricevuto espressa e documentata autorizzazione dal Titolare del trattamento.

In una tale evenienza il Responsabile del trattamento è tenuto a:

- garantire che il proprio sub-fornitore (che dovrà essere designato Responsabile del trattamento) sottoscriva un documento contenente chiari e dettagliati obblighi in ordine al rispetto della normativa privacy;

- garantire che farà fronte, manlevando il Titolare, ad eventuali inadempimenti imputabili ad attività od omissioni dei propri sub-fornitori

Ripartizione requisiti GDPR tra i ruoli privacy



Accountability (Responsabilizzazione)

Prodotti e servizi resi ai Clienti

Processi di amministrazione interni all'Organizzazione

I Titolari devono:

1. effettuare i trattamenti dati personali conformemente ai principi privacy stability dal GDPR:
   a. liceità, correttezza e trasparenza
   b. Limitazione della finalità
   c. minimizzazione dei dati
   d. esattezza
   e. limitazione della conservazione
   f. integrità e riservatezza
2. ed essere in grado di comprovarlo

(art. 5)

Accountability è adempimento essenziale che consente all'Organizzazione di adempiere al GDPR in modo gestito, efficace ed efficente

Interessati

Autorità Garanti Privacy

Coordinazione e controllo all'interno della Organizzazione

Record of processing activities
(Registri delle attività di trattamento)

Titolari e Responsabili devono mantenere una registro - 'inventario'- in forma scritta da mettere a disposizione del Garante privacy ove richiesto,riguardo ai trattamenti dati effettuati sotto la propria responsabilità contenente almeno le seguenti informazioni:

- categorie di dati trattati,
- tipologia di trattamenti,
- classi di Interessati,
- informazioni sulle misure di sicurezza e
- su eventuali trasferimenti di dati extra UE,
- …

Sono esentate le organizzazioni con meno di 250 dipendenti, a meno che il trattamento possa presentare rischi per l'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (sensibili, giudiziari)

(art. 30)

Profilazione: cosa prevede il Regolamento

Definizione

"*qualsiasi forma di trattamento **automatizzato** di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*"

Cosa cambia rispetto alla Direttiva o al Codice privacy

Il concetto di profilazione non è più circoscritto alla propensione al consumo di prodotti e all'utilizzo di servizi ma il perimetro viene significativamente esteso facendovi rientrare **l'Interessato (persona fisica) e quanto a lui direttamente riferibile (età, sesso, situazione economica, stato familiare, etc.) ma anche quanto lo circonda o con cui interagisce**.

Profilazione: cosa prevede il Regolamento

Quindi perché si tratti di "profilazione" è necessario che:

- vi sia una attività di elaborazione "automatizzata" dei dati raccolti destinata a produrre un profilo dell'Interessato;

- la profilazione abbia conseguenze giuridiche, ossia produca delle valutazioni adottate "esclusivamente" sulla base di un trattamento automatizzato (art. 14 c. 1);

- non costituisce attività di profilazione il solo "tracciamento" della navigazione web dell'Interessato ma le attività di analisi "*volte alla profilazione dell'utente, in particolare per prendere decisioni che lo riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*" (Cons. 21).

Profilazione: cosa prevede il Regolamento

La “profilazione” è vietata quando:

- si riferisce ai minori;
- riguarda i dati “particolari” ossia quei dati che espongono a maggiori rischi i diritti e le libertà degli Interessati (salvo che non vi sia un legittimo interesse del Titolare, di portata almeno equivalente al diritto dell’interessato, e siano adottate adeguate misure di protezione dei dati)

E’ inoltre necessario che il Titolare “*utilizzi procedure matematiche o statistiche adeguate per la profilazione, metta in atto misure tecniche ed organizzative adeguate al fine di garantire in particolare che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori delle misure matematiche o statistiche [...]e che impedisca tra l'altro effetti discriminatori nei confronti di persone.....*

L’art. 35 prevede per la profilazione l’obbligo della preventiva PIA proprio perché si ritiene che il trattamento presenta rischi per i diritti e le libertà delle persone fisiche.

Profilazione: cosa prevede il Regolamento

L'Interessato ha il diritto:

- di essere informato dell'attività di profilazione;
- di conoscere le logiche applicate al trattamento quando questo possa originare conseguenze giuridiche sul suo status ovvero condurre a possibili situazioni discriminatorie (il Con. 58 fornisce come esempio il rifiuto della concessione di un prestito o il rigetto di una candidatura on-line "automatizzato");
- di revocare il consenso prestato alla profilazione con la conseguenze che il Titolare deve sospendere il trattamento salvo dimostrare un "legittimo interesse";
- nel caso di profilazione per finalità di marketing la revoca del consenso implica l'immediata cessazione di tali attività da parte del Titolare.

Privacy by Design and by Default
(Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,

By Design

Sia in fase di determinazione dei mezzi di trattamento sia nel corso del trattamento il Titolare adotta adeguate misure tecniche/organizzative/procedurali (citata come esempio la pseudoanonimizzazione) per soddisfare principi e requisiti del GDPR, incluso il rispetto dei diritti degli Interessati

By Default

Il Titolare adotta adeguate misure tecniche/organizzative/procedurali, tali che, siano trattati solo i dati personali necessari per ogni specif**come pre-impostazione,** ica finalità del trattamento, in termini di:

- quantità dei dati personali raccolti,
- l'estensione del loro trattamento,
- il periodo di conservazione e l'accessibilità.

L'adesione ad un sistema di certificazione privacy autorizzato come da GDPR può essere utilizzato per dimostrare la conformità ai requisiti Privacy By Design e By Default

(art. 25)

PIA Privacy Impact Assessment
(Valutazione d'impatto sulla protezione dei dati)

Una delle maggiori novità del GDPR

Richiede capacità di gestione e documentazione dei processi di PIA attivati/da attivare

Il processo di PIA può comportare la necessità di richiedere la 'Prior Consultation' del Garante Privacy

(art. 35)

Il trattamento può comportare un rischio elevato per diritti e libertà fondamentali degli Interessati?

Si

Prima di effettuare il trattamento il Titolare deve svolgere una PIA

La PIA evidenzia l'esistenza di rischio elevato qualora il Titolare non adotti misure a mitigazione del rischio?

Si

Prima di effettuare il trattamento il Titolare Deve avviare con il Garante privacy la 'Prior Consultation' ed attenersi alle indicazioni fornite dall'Autorità

PIA Privacy Impact Assessment
(Valutazione d'impatto sulla protezione dei dati)

Elementi essenziali delle prescrizioni PIA

Riguarda in particolare l'utilizzo di **nuove tecnologie**, e deve tenere in considerazione la natura dei dati, scopi, contesto e finalità dei trattamenti

È espressamente richiesta dal GDPR in caso di:

a) Analisi sistematica ed estesa di aspetti personali di individui basata su un trattamento automatizzato, profilazione inclusa, sulla quale si fondano decisioni che hanno effetti giuridici o incidono similarmente in modo significativo sugli individui
b) Trattamento, su larga scala, di categorie particolari di dati (dati sensibili, dati giudiziari)
c) Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

La aderenza a Codici di Condotta Privacy autorizzati come da GDPR è un elemento positivo da evidenziare nella PIA

<u>Il Garante privacy</u>

redige un elenco dei casi in cui la PIA è necessaria e lo comunica al EDPB

può redigere un elenco di casi in cui la PIA non è necessaria e lo comunica al EDPB

Quando tali elenchi contengono casi particolari di trattamento (offerta di beni o servizi o monitoraggio del comportamento in più Stati membri, o attività di trattamento suscettibili di incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione) EDPB applica il Consistency Mechanism per evitare disomogeneità tra Paesi Membri UE.

Prior Consultation
(Consultazione Preventiva)

La PIA evidenzia l'esistenza di rischio elevato qualora il Titolare non adotti misure a mitigazione del rischio?

Si

Prima di effettuare il trattamento il Titolare Deve avviare con il Garante privacy la 'Prior Consultation' ed attenersi alle indicazioni fornite dall'Autorità

Il Garante Privacy di regola risponderà:

- entro 8 settimane, termine prorogabile di 6 settimane nei casi complessi
- direttamente al Titolare (ed al Responsabile ove applicabile) in forma scritta, anche in base ai propri poteri di Indagine, di Correzione di Autorizzazione e Consultazione (poteri elencati all'art. 58)

Data Breach
(Violazione di dati personali)

"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

*(*punto12 dell'art. 4*)*

Obblighi UE di notifica violazione dati personali sono già esistenti in specifici settori:

- Servizi di comunicazioni elettroniche accessibili al pubblico (TLC, ISP) - art. 4 Direttiva 2002/58/EC e Regolamento 611/2013
- Trust services (firme elettroniche, ….) – art. 19 Regolamento 910/2014

Il GDPR istituisce obblighi di notifica violazione dati personali indipendentemente dal settore e dimensione dell'organizzazione

(art. 33 e 34)

Data Breach
(Violazione di dati personali)

Una violazione dati personali è stata:
1) rilevata e
2) valutata come suscettibile di comportare rischi per le libertà e diritti fondamentali degli individui ?

Si

Il Titolare:
1) Di norma notifica entro 72 ore al Garante Privacy
2) Avvia le attività di analisi, documentazione e contenimento

La violazione è suscettibile di presentare **rischi elevati** per i diritti e le libertà degli individui ?

Si

Il Titolare ha implementato:
- Misure EX ANTE adeguate, in particolare che rendono i dati non intelligibili ai non autorizzati **oppure**
- Misure EX POST che scongiurano il materializzarsi dei rischi elevati **oppure**
- Una comunicazione pubblica o simile iniziativa in quanto altre misure comportano sforzi sproporzionati

No

Il Titolare della comunicare la violazione dei dati personali agli Interessati senza indebito ritardo

Il Responsabile deve comunicare al Titolare la violazione dati personali senza indebito ritardo

Data Breach
(Violazione di dati personali)

Archivio delle violazioni dati personali

Il Titolare del trattamento deve documentare

- **le circostanze**
- **le conseguenze**
- **i provvedimenti adottati per porre rimedio alla violazione**

Tale documentazione può essere richieste dal Garante Privacy per poter verificare il rispetto delle prescrizioni del GDPR in materia di violazione dati personali

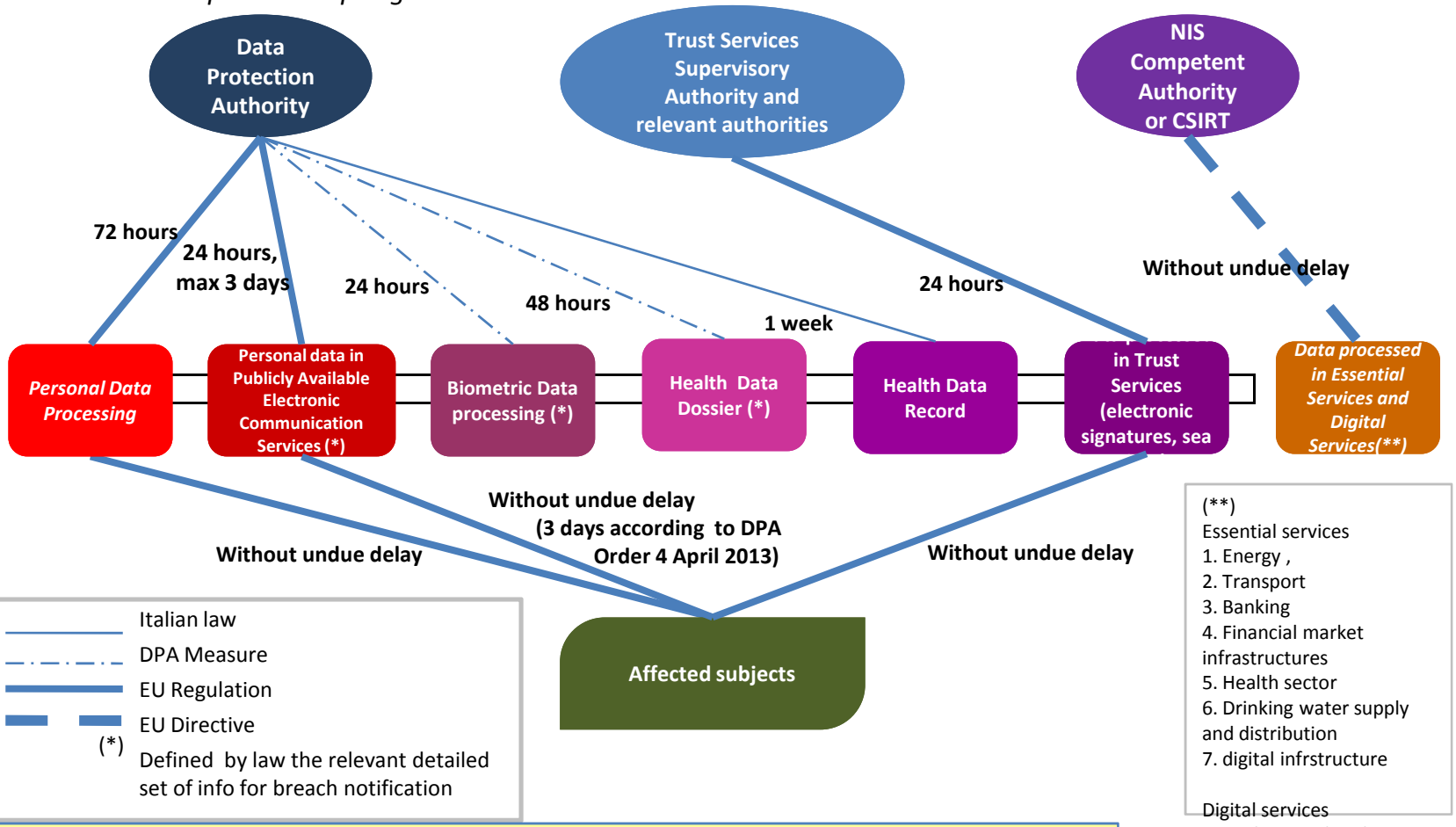
Comunicazione agli Interessati

Il Garante Privacy può in ogni caso richiedere al Titolare di effettuare la comunicazione di violazione dati agli Interessati

Data Breach – la situazione in Italia

Breach Notification obligations towards national Authorities and affected subjects: focus on EU and Italy, February 2016

EU Privacy Regulation and EU NIS Directive texts agreed in December 2015, to be formally approved by the EU Parliament - expected in Spring 2016



(**)
Essential services
1. Energy ,
2. Transport
3. Banking
4. Financial market infrastructures
5. Health sector
6. Drinking water supply and distribution
7. digital infrstructure

Digital services
A. On line marketplace
B. On line search engines
C. Cloud Computing services

Ulteriori commenti nell'articolo "**Data Breach notification obligations: summary overview of the current EU/Italy legal framework in light of the European General Data Protection Regulation and Network Information Security Directive**"

Informativa: cosa cambia con il Regolamento

Il Regolamento prevede che l'informativa contenga i seguenti campi essenziali (in grassetto le novità):

- l'identità e i dati di contatto del Titolare del trattamento e, **se designato, del DPO;**
- le finalità del trattamento;
- se il trattamento si basa su legittimi interessi perseguiti dal Titolare;
- i destinatari dei dati o le categorie di destinatari;
- se è previsto un trasferimento di dati all'Estero e **le garanzie esistenti** a tutela dei dati trasferiti;
- **i tempi previsti di conservazione dei dati o il criterio per determinarlo;**
- i diritti riconosciuti ai soggetti interessati;

Informativa: cosa cambia con il Regolamento

Il Regolamento prevede che l'informativa contenga i seguenti campi essenziali (in grassetto le novità):

- la possibilità di revocare il consenso in qualsiasi momento;
- **il diritto di proporre reclamo ad un'autorità di controllo diversa da quella riferibile al Titolare;**
- **l'indicazione se la comunicazione di dati personali è un obbligo legale o è necessario** per la conclusione di un contratto;
- se l'interessato ha l'obbligo di fornire i dati e le possibili conseguenze di un rifiuto;
- se l'interessato sarà oggetto di attività di **profilazione.**

Consenso: cosa cambia con il Regolamento

Il Regolamento prevede che il consenso sia:

- informato, prestato quindi dopo aver ricevuto una chiara "Informativa" sul trattamento dei dati;
- libero, svincolato da qualsiasi obbligo e forma, anche indiretta, di coercizione che ne renda inefficace il rilascio;
- limitato, sia per quanto attiene alla sua durata che per la tipologia del trattamento per il quale viene prestato il consenso;
- esplicito– opt-in, ossia non è più possibile che l'azione dell'Interessato, o maggior ragione la sua inattività, possa essere considerata come manifestazione del consenso;
- nel caso di profilazione il consenso deve essere raccolto separatamente da altre forme di consenso.

Consenso: cosa cambia con il Regolamento

Nel caso dei minori (16 anni) il consenso deve essere prestato dai genitori o da chi ne abbia la patria potestà. Il limite non può esser abbassato al di sotto dei 13 anni

Per il trattamento dei dati "particolari" di massima per il loro trattamento è necessario un consenso "***esplicito***" ed in alcune circostanze il loro trattamento può essere sottoposto ad ulteriori vincoli normativi nazionali. Resta da chiarire se, come previsto dalla normativa italiana il consenso "esplicito" possa, e in quali circostanze, richiedere la forma scritta.

Esercizio dei diritti dell'Interessato

Diritto all'oblio

- L'interessato ha diritto a che i propri dati personali siano cancellati.
- Il Titolare dovrà attivarsi, nel caso i dati personali siano stati "comunicati" ad altri soggetti, affinché anche costoro effettuino la cancellazione (salvo che tale attività non abbia costi eccessivi).

Il diritto all'oblio non è applicabile se connesso a:

- l'esercizio del diritto alla libertà di espressione e di informazione;
- l'adempimento di un obbligo legale;
- motivi e finalità di pubblico interesse;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Esercizio dei diritti dell'Interessato

Diritto alla portabilità dei dati personali

L'art. 20 prevede il diritto alla portabilità dei dati che si traduce nella possibilità di:

- chiedere al Titolare del trattamento di ricevere in formato strutturato, di uso comune e leggibile digitalmente i propri dati personali in suo possesso;
- chiedere al Titolare il trasferimento dei propri dati personali ad un altro Titolare, anche direttamente ove sia tecnicamente consentito.

Il diritto è esercitabile quando:

- il trattamento è effettuato mediante sistemi automatizzati;
- il trattamento si basa sul consenso;
- il trattamento si basa su un contratto.

Il diritto non è esercitabile nei confronti della PA o quando il trattamento avviene per un "pubblico interesse".

Data Protection Officer

Data Protection Officer

QUALI SONO I REQUISITI?

Il Data Protection Officer, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
2. adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;
3. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio .

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati personali le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Data Protection Officer

QUALI SONO I COMPITI?

Il Data Protection Officer avrà il compito di:

a) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

Data Protection Officer

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati personali dovrà:

c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

d) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

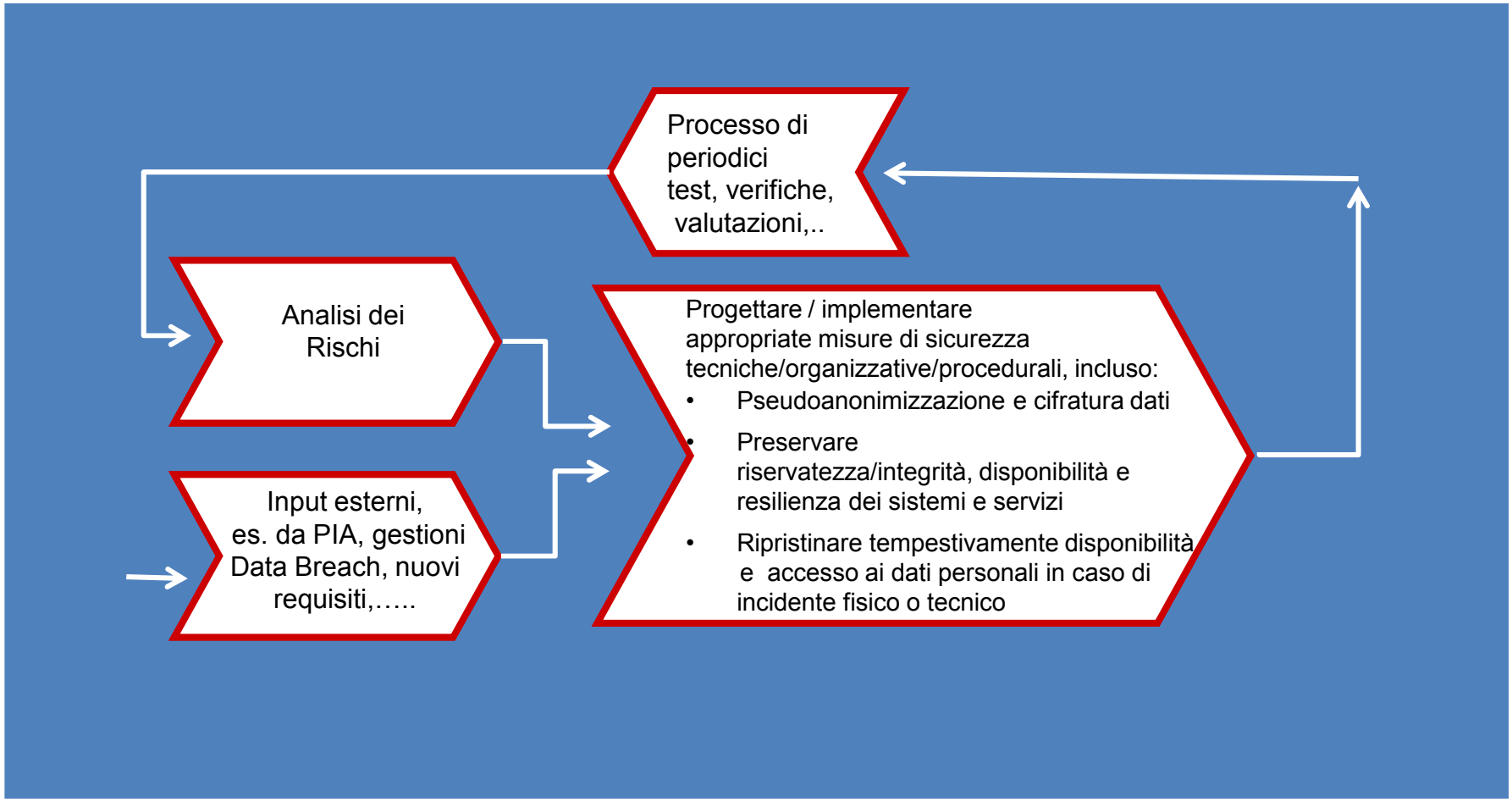
Data Protection Officer

IN QUALI CASI E' PREVISTO?
Dovranno designare obbligatoriamente il DPO:

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati;
c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Un titolare del trattamento o un responsabile del trattamento possono comunque designare un Responsabile della protezione dei dati personali anche in casi diversi da quelli sopra indicati.
Un gruppo di imprese o soggetti pubblici possono nominare un unico Responsabile della protezione dei dati.

Security of processing Art.32
(sicurezza del trattamento)



Security of processing Art.32
(sicurezza del trattamento)

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

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati

L'adesione a un codice di condotta privacy o a un meccanismo di certificazione privacy può essere utilizzata come elemento per dimostrare la conformità ai requisiti di approntare misure di sicurezza adeguate al livello di rischio

Security of processing Art.32
(sicurezza del trattamento)

"***pseudo-anonimizzazione***":

il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Q & A

http://www.consilium.europa.eu/it/policies/data-protection-reform/data-protection-regulation-infographics/

Q & A

http://www.consilium.europa.eu/it/policies/data-protection-reform/data-protection-regulation-infographics/

Q & A

http://www.consilium.europa.eu/it/policies/data-protection-reform/data-protection-regulation-infographics/

Fine del Seminario

Per eventuali approfondimenti sui temi trattati

Luciano Delli Veneri – luciano.delliveneri@gmail.com

Gloria Marcoccio – gloria.marcoccio@glory.it