Corso di Formazione Privacy

Privacy e Protezione dei dati aziendali alla luce del nuovo Regolamento Europeo 2016/679

Relatore: Privacy Officers Nino Papani

Data Protection Officer DPO0216
Norma UNI 11697:2017
Ente certificato da ACCREDIA

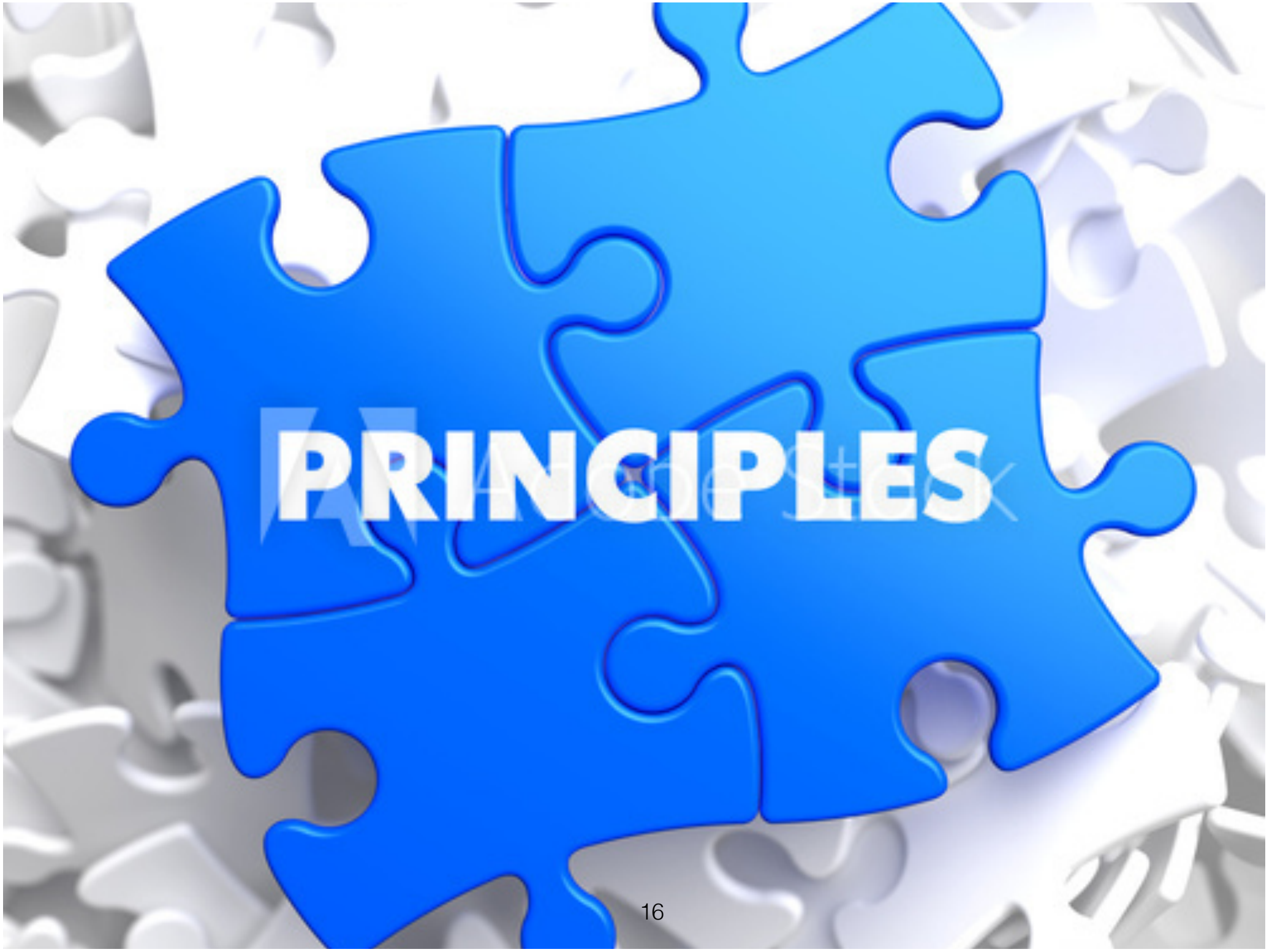
Data Proction Officer Certificato
n°reg. DPO_012

Privacy Officer Certificato
n°reg. CDP_025

2' parte

Parma 20 Maggio 2019

GLOBALPRIVACY
di Nino Papani


PRINCIPLES

Principi applicabili al trattamento di dati personali

art 5 Regolamento UE 2016/679

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

Principi applicabili al trattamento di dati personali

art 5 Regolamento UE 2016/679

f) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2) Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Accountability

Approccio basato sulla valutazione del rischio che premia i soggetti più responsabili

Il Titolare del trattamento è:

competente per il rispetto dei principi applicabili al trattamento di dati personali

in grado di comprovarlo «**responsabilizzazione**»

Ambito di applicazione

art 24 Regolamento UE 2016/679

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.

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

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

art 25 Regolamento UE 2016/679

1. 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, **sia al momento di determinare i mezzi del trattamento sia 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.

PRIVACY BY DESIGN

quindi prima che il trattamento inizi

Approccio risk based

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

art 25 Regolamento UE 2016/679

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la **quantità** dei dati personali raccolti, la **portata del trattamento**, il periodo di **conservazione** e **l'accessibilità**. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

PRIVACY BY DEFAULT

impostazione predefinita

Liceità del trattamento

art 6 Regolamento UE 2016/679

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è **necessario per la salvaguardia degli interessi vitali dell'interessato** o di un'altra persona fisica;

e) il trattamento è **necessario per l'esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è **necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Liceità del trattamento

art 6 Regolamento UE 2016/679

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e)dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Perché devo preoccuparmi della privacy?

Regolamento UE 2016/679

Per comprendere il funzionamento di una qualsiasi normativa è sempre bene partire dalla precisa definizione di alcuni termini - chiave che ci faranno da guida nel successivo esame dei diversi articoli che la compongono.

Nel Regolamento UE le definizioni che più ci interessano sono contenute nell'art. 4.

E' UN PO' **IL VOCABOLARIO DELLA PRIVACY**

Definizioni

art 4 Regolamento UE 2016/679

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come 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

Definizioni

art 4 Regolamento UE 2016/679

Dato personale

qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Definizioni

art 4 Regolamento UE 2016/679

Dati Genetici

tutti i dati, di qualsiasi natura, riguardanti le caratteristiche di una persona fisica che siano ereditarie o acquisite in uno stadio precoce di sviluppo prenatale

Dati relativi alla salute

qualsiasi informazione attinente alla salute fisica o mentale di una persona o alla prestazione di servizi sanitari a detta persona

Dati Biometrici

i dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona che ne consentono l'identificazione univoca, quali l'immagine facciale o i rilievi dattiloscopici

Definizioni

art 4 Regolamento UE 2016/679

Titolare

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

Responsabile

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

Definizioni

art 4 Regolamento UE 2016/679

Consenso

qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Violazione dei dati

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

Attori principali

TITOLARE

REFERENTE INTERNO

SOGGETTI AUTORIZZATI

INTERESSATO

Titolare del trattamento

1. Assume decisioni relative alle finalità del trattamento
2. Impartisce istruzioni
3. Controlla l'operato dei responsabili e degli incaricati

Trattamento sotto l'autorità del titolare o del responsabile del trattamento

art 29 Regolamento UE 2016/679

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali **non può trattare tali dati se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Responsabile del trattamento

art 28 Regolamento UE 2016/679

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.

2. Il responsabile del trattamento **non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento**. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Responsabile del trattamento

art 28.3 Regolamento UE 2016/679

I trattamenti da parte di un responsabile del trattamento **sono disciplinati da un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la **durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento**. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Responsabile del trattamento

art 28.4 Regolamento UE 2016/679

Quando un responsabile del trattamento **ricorre a un altro responsabile del trattamento** per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, **su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento** di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Soggetti autorizzati

Chi sono

- coloro che operativamente trattano i dati personali secondo le istruzioni del Titolare (il Codice Privacy li definisce "**Incaricati**" del trattamento)

Che cosa fanno

- Raccolgono i dati o comunque li trattano in ragione della finalità che caratterizza il loro lavoro (gestione del personale, gestione gare, sorveglianza sanitaria, gestione del contenzioso ecc. ...)

Incaricati del trattamento

Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla diret tiva 95/46/CE (e, quindi, al Codice italiano). Pur non prevedendo espressamente la figura dell´ **"incaricato"** del trattamento (ex art. 30 Codic e), il regolamento non ne esclude la presenza in quanto fa riferimento a **"persone autorizzate al trattamento dei dati personali sotto l´autorità diretta del titolare o del responsabile"** (si veda, in particolare, art. 4, n.10 , del regolamento).

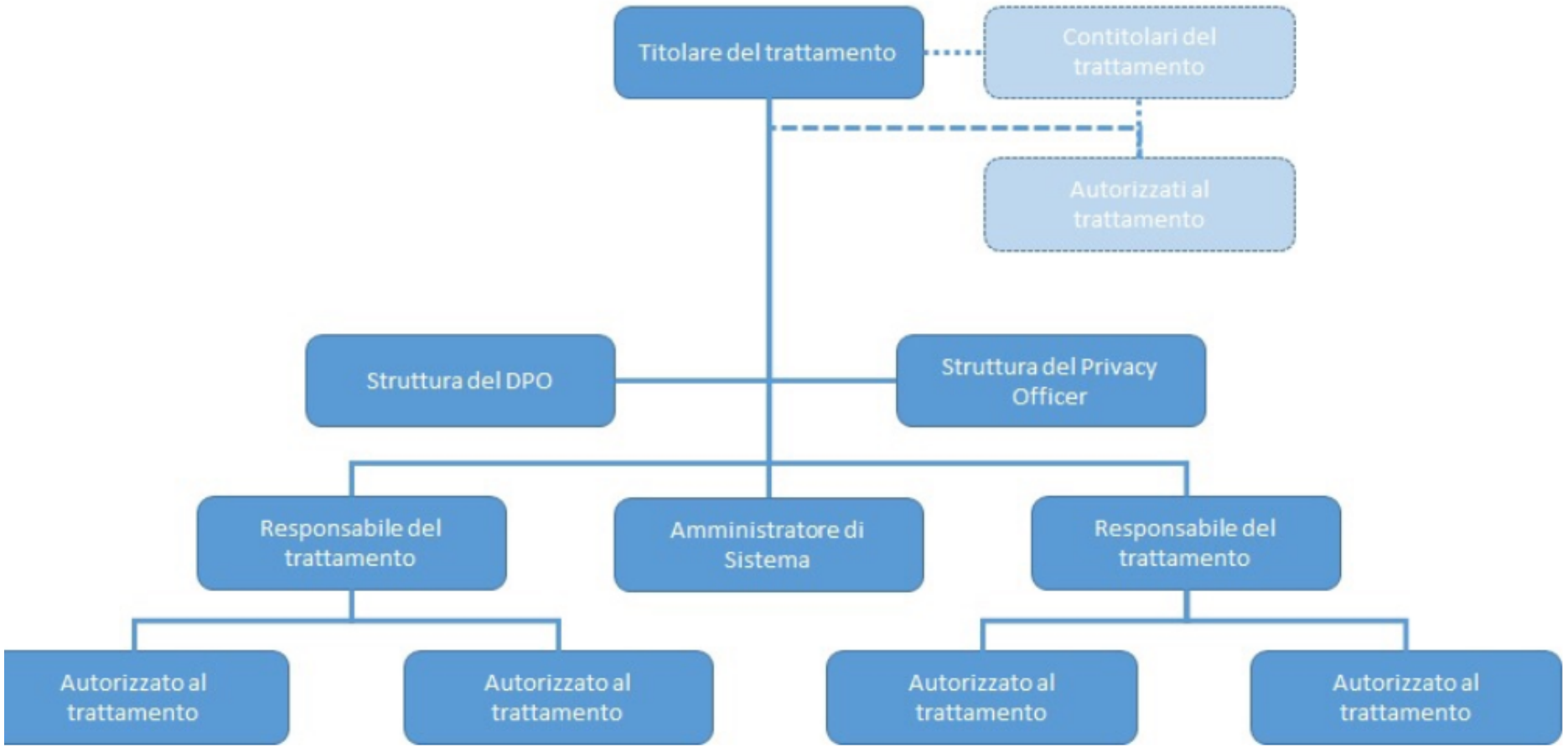
Incaricati del trattamento

art 2 quaterdecies D.lgs. 101/2018

(Attribuzione di funzioni e compiti a soggetti designati)

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al tra ttamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2. Il titolare o il responsabile del trattamento individuano le modal ità più opportune per autorizzare al trattamento dei dati perso nali le persone che operano sotto la propria autorità diretta.

Organigramma con DPO di una «grande impresa»



Responsabile protezione dei dati (RPD)

Regolamento privacy, come scegliere il responsabile della protezione dei dati
Newsletter del 15/09/17

Enti pubblici e società private dovranno quindi comunque procedere alla selezione del RPD, **valutando autonomamente** il possesso dei requisiti necessari per svolgere i compiti da assegnati

Regolamento UE 2016/679

Quali saranno i compiti del RPD?

1. Informare e fornire consulenza al titolare del trattamento o al responsabile
2. Sorvegliare l'osservanza del RGPD
3. Fornire un parere sulla valutazione di impatto sulla protezione dei dati
4. fungere da punto di contatto per l'autorità di controllo

E' ammessa la designazione congiunta di uno stesso RPD da parte di più soggetti?

E' possibile a un gruppo imprenditoriale di nominare un unico RPD a condizione che quest'ultimo sia "facilmente raggiungibile da ciascuno stabilimento" (art 37. 2)

Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato **per più autorità pubbliche o organismi pubblici**, tenuto conto della loro struttura organizzativa e dimensione (art. 37. 3)

Posizione del RPD

art 38 Regolamento UE 2016/679

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente **coinvolto in tutte le questioni riguardanti la protezione dei dati personali.**

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli **le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.**

3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati **non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti.** Il responsabile della protezione dei dati **non è rimosso o penalizzato** dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati **riferisce direttamente al vertice gerarchico** del titolare del trattamento o del responsabile del trattamento.

Posizione del RPD

art 38 Regolamento UE 2016/679

4 Gli interessati possono **contattare** il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

5. Il responsabile della protezione dei dati è tenuto **al segreto o alla riservatezza** in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un **conflitto di interessi**.

Mancata nomina del RPD

art 83.4 Regolamento UE 2016/679

…….. sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, **da 25 a 39**, 42 e 43;

b) ….


Cosa fare?
GLOBALPRIVACY
di Nino Papani

Contenuti dell'informativa

L'ordine del processo di legittimità del trattamento è il seguente:

INFORMATIVA

↓

CONSENSO

↓

RACCOLTA DATI

Non è sufficiente un'informazione generica che metta l'interessato a conoscenza dell'esistenza di un generico trattamento di dati personali che lo riguardano. Occorre che tale avviso contenga gli elementi **tassativamente** indicati dall'art. 13 GDPR.

Regolamento UE 2016/679

Informativa chiara e completa, concisa, trasparente, intelligibile per l'interessato e facilmente accessibile

Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a **icone**. Il regolamento ammette, soprattutto, l'utilizzo di icone ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

Diritti degli interessati

artt 15 - 21 Regolamento UE 2016/679

Diritto di accesso ai dati (art. 15)

Diritto di rettifica ed integrazione dei dati (art. 16)

Diritto di cancellazione o diritto all'oblio (art.17)

Diritto di limitazione di trattamento (art. 18) - *il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;*

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (art. 19)

Diritto alla portabilità dei dati (art. 20)

Diritto di opposizione per motivi legittimi e al marketing (art. 21)

Consenso

Regolamento UE 2016/679

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, **libero**, **specifico**, **informato** e **inequivocabile**, anche quando espresso attraverso mezzi elettronici, **NON è ammesso il consenso tacito o presunto** (no a caselle pre-spuntate su un modulo).

Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso), in quanto il consenso **DEVE** essere manifestato attraverso "**dichiarazione o azione positiva inequivocabile**".

Per i **dati "sensibili" il consenso DEVE essere "esplicito";**

lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la **profilazione** – art. 22).

Il consenso potrà essere revocato in ogni momento.

Il consenso di minori è valido a partire dai 16 anni

GLOBALPRIVACY
di Nino Papani

Trattamento di categorie particolari di dati

Art. 9 Regolamento UE 2016/679

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento …..
b) l trattamento è necessario per assolvere gli obblighi ed esercitare i diritti ….
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso

……

Trattamento di categorie particolari di dati

Art. 9 Regolamento UE 2016/679

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

Trattamento di categorie particolari di dati

Art. 9 Regolamento UE 2016/679

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ……..proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

3. I dati personali di cui al paragrafo 1 (categorie particolari di dati) possono essere trattati per le finalità di cui al paragrafo 2, lettera h (medicina preventiva e del lavoro, medicina preventiva….), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Trattamento relativo a condanne penali e reati

Art.10 Regolamento UE 2016/679

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Articolo 6 Liceità del trattamento

1. Il trattamento è lecito solo se ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Data Breach

Trattamento dei dati

deve garantire

esattezza
integrità
disponibilità dei dati
protezione dagli accessi non autorizzati
trattamenti non consentiti

Sicurezza

Privacy ≠ Sicurezza

Il rispetto della privacy presuppone un'adeguata sicurezza

La sola sicurezza non presuppone il rispetto della privacy

Sicurezza dei dati

L'evoluzione tecnologica impatta fortemente anche nel settore della Logistica

1996 → 2003 → 2018

MISURE DI SICUREZZA

1996

- 675/1996 prima legge sulla protezione dei dati che prevedeva l'adozione di misure «**minime**» di sicurezza

2003

- 196/2003 Allegato B Misure «**mimime**» di sicurezza, obbligatorie

2018

- 679/2016 Regolamento UE. Misure «**adeguate**» in base ai rischi che si corrono (valutazione dei rischi)

MISURE DI SICUREZZA ADEGUATE (679/2016 ART. 32)

MISURE TECNICHE E ORGANIZZATIVE ADEGUATE

per garantire un livello di sicurezza adeguato al rischio

Attenzione

«**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 (art.4 GDPR)

GLOBALPRIVACY
di Nino Papani

SICUREZZA DEL TRATTAMENTO

art. 32 Regolamento UE 2016/679

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;

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.

SICUREZZA DEL TRATTAMENTO

art. 32 Regolamento UE 2016/679

2. 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.

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.

SICUREZZA DEL TRATTAMENTO

art. 32 Regolamento UE 2016/679

4. Il titolare del trattamento e il responsabile del trattamento **fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento,** salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Approccio basato sul rischio

Considerando 74 Regolamento UE 2016/679

È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a **mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure.** Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Regolamento UE 2016/679

Violazioni dei dati

Incidenti informatici

obbligo di comunicazione al Garante

Rischi

Considerando 75 Regolamento UE 2016/679

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;

se sono trattati dati personali che **rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza**;

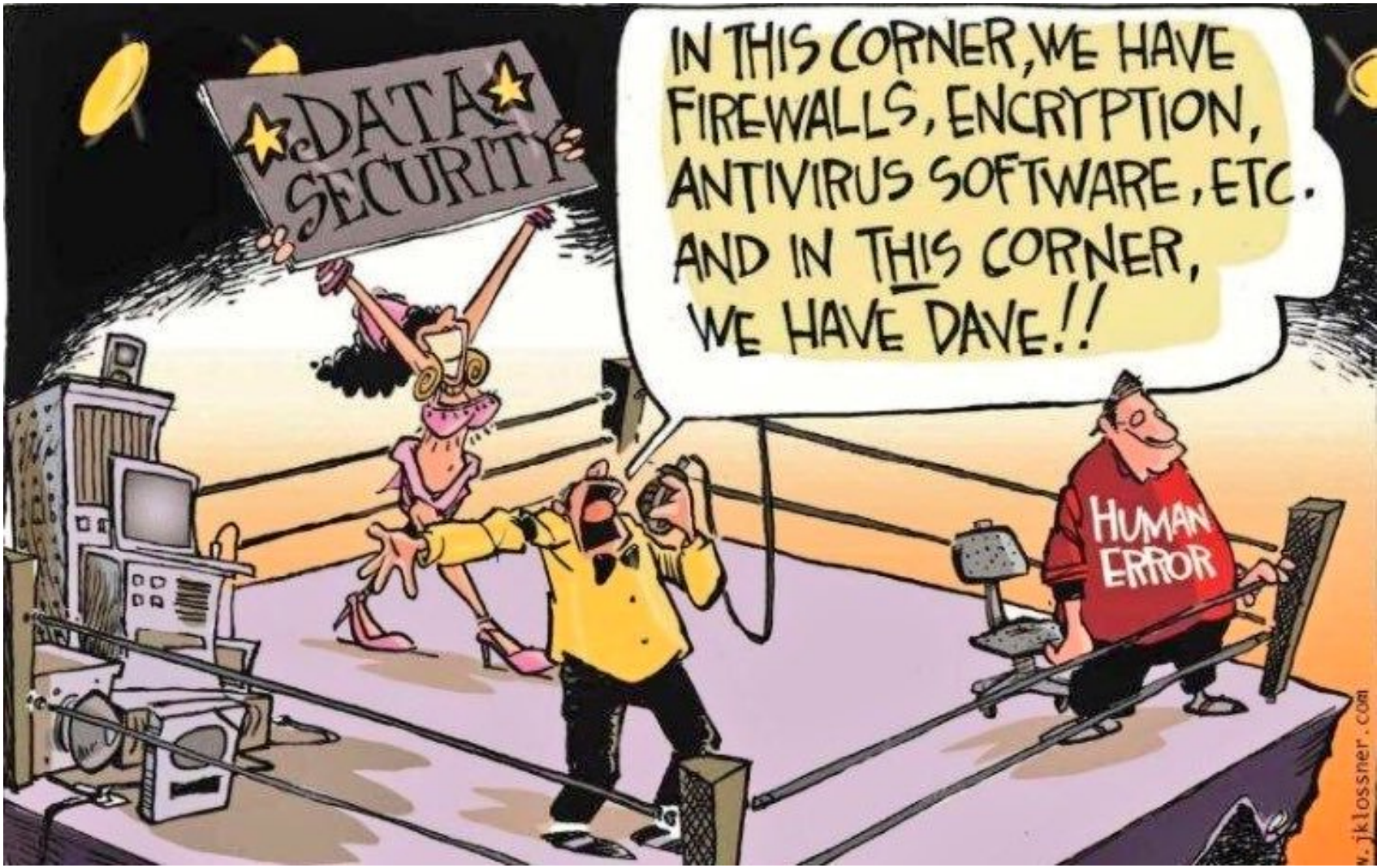
Rischi

Considerando 75 Regolamento UE 2016/679

in caso di valutazione di aspetti personali, in particolare mediante **l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;**

se sono trattati dati personali di persone fisiche vulnerabili, in particolare **minori**;

se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
w.jklossner.com

Attenzione

1. Bloccare il PC
2. Non lasciare post it con la password
3. Non lasciare incustoditi documenti cartacei
4. Uso fax e stampanti
5. Uso Mail
6. Mantenere le stanze chiuse
7. Non condividere le password
8. Navigare sui Social e…..

Whatsapp

GLOBALPRIVACY

di Nino Papani

INTERNET E SOCIAL MEDIA: CONNETTI LA TESTA.

RIVACY
Papani

È POSSIBILE CARICARE FOTO O ALTRE INFORMAZIONI RELATIVE A DEGENTI SULLA PROPRIA PAGINA DI FACEBOOK O DI ALTRI SOCIAL NETWORK?

Attenzione a non pubblicare dati personali, ad esempio nomi o fotografie, di estranei sulle proprie pagine social network. Anche se spesso si pensa di condividerle solo con amici, magari colleghi, si rischia invece di diffonderle a un numero imprecisato di utenti della rete, violando così la privacy delle persone coinvolte.

LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET

(GAZZETTA UFFICIALE N. 58 DEL 10 MARZO 2007)

PREMESSE:

compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le **modalità d'uso** nell'organizzazione dell'attività lavorativa e tenendo conto della disciplina in tema di diritti e relazioni sindacali;

spetta ad essi adottare **idonee misure di sicurezza** per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità

Il provvedimento si propone nella sostanza di dettare delle regole generali che disciplinano l'esercizio dei poteri di trattamento dei dati nel rapporto di lavoro.

VIRALITA’: caratteristica della rete

Invoco il diritto all’oblio, voglio eliminare da Internet ogni contenuto che mi riguarda

Sanzioni

Sanzioni penali: quando previste dalla legge Nazionale
Sanzioni pecuniarie: saranno Efficaci, Proporzionate e Dissuasive

Fino **a € 10 milioni** o al 2% del fatturato mondiale (se superiore)

- Es. Violazione obblighi in materia di consenso dei minori, misure di sicurezza
- Es. Violazione obblighi impartiti dal Titolare
- Es. Violazione obblighi di comunicazione per Data Breach

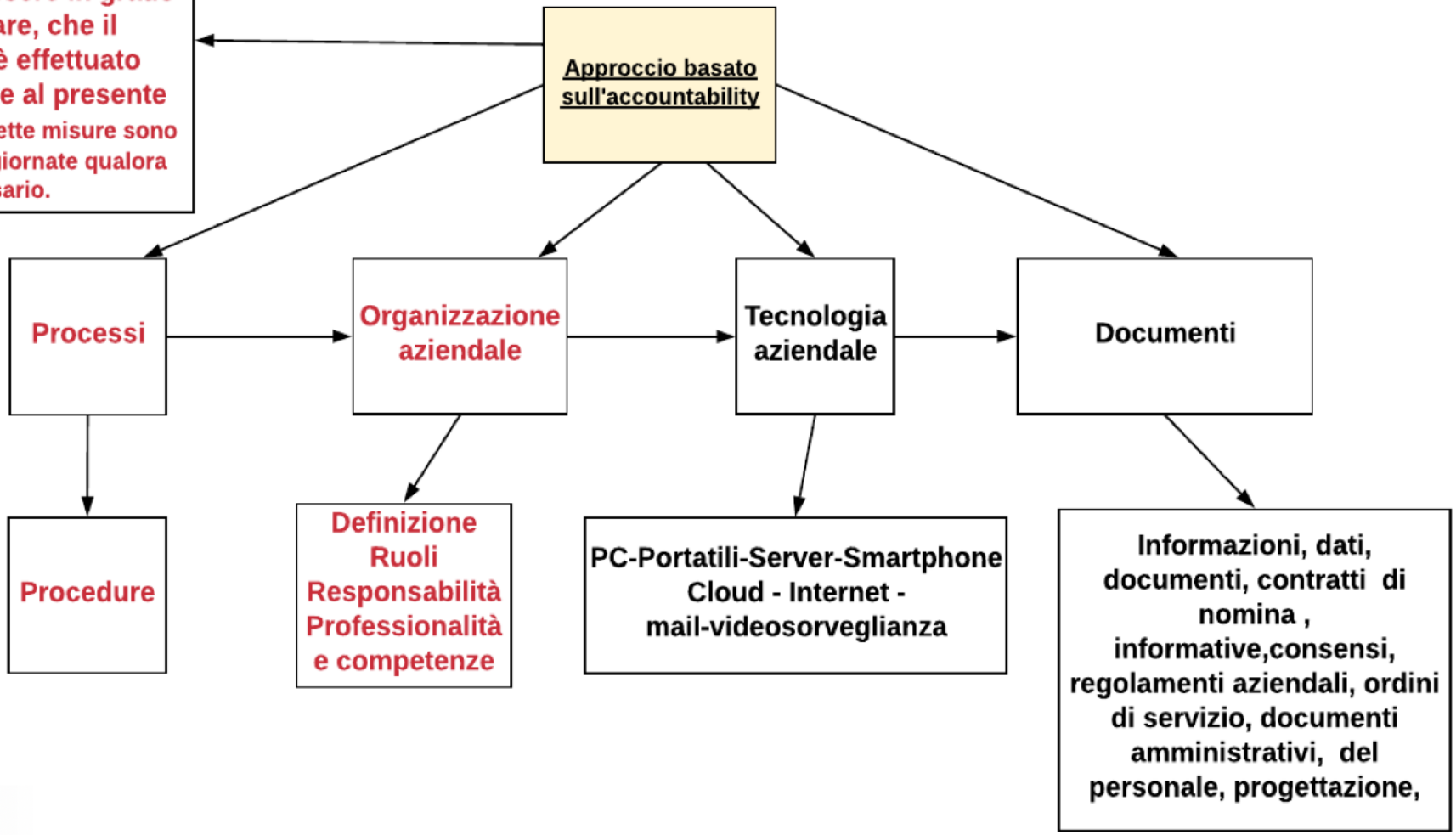
Fino a **€ 20 milioni** o al 4% del fatturato mondiale (se superiore)

- Es. Violazioni concernenti i diritti degli interessati, i principi cardine del trattamento (es. consenso) i trasferimenti ecc.
- Es. Violazioni di ordini o misure imposte dall'Autorità

Regolamento Europeo GDPR 679/2016

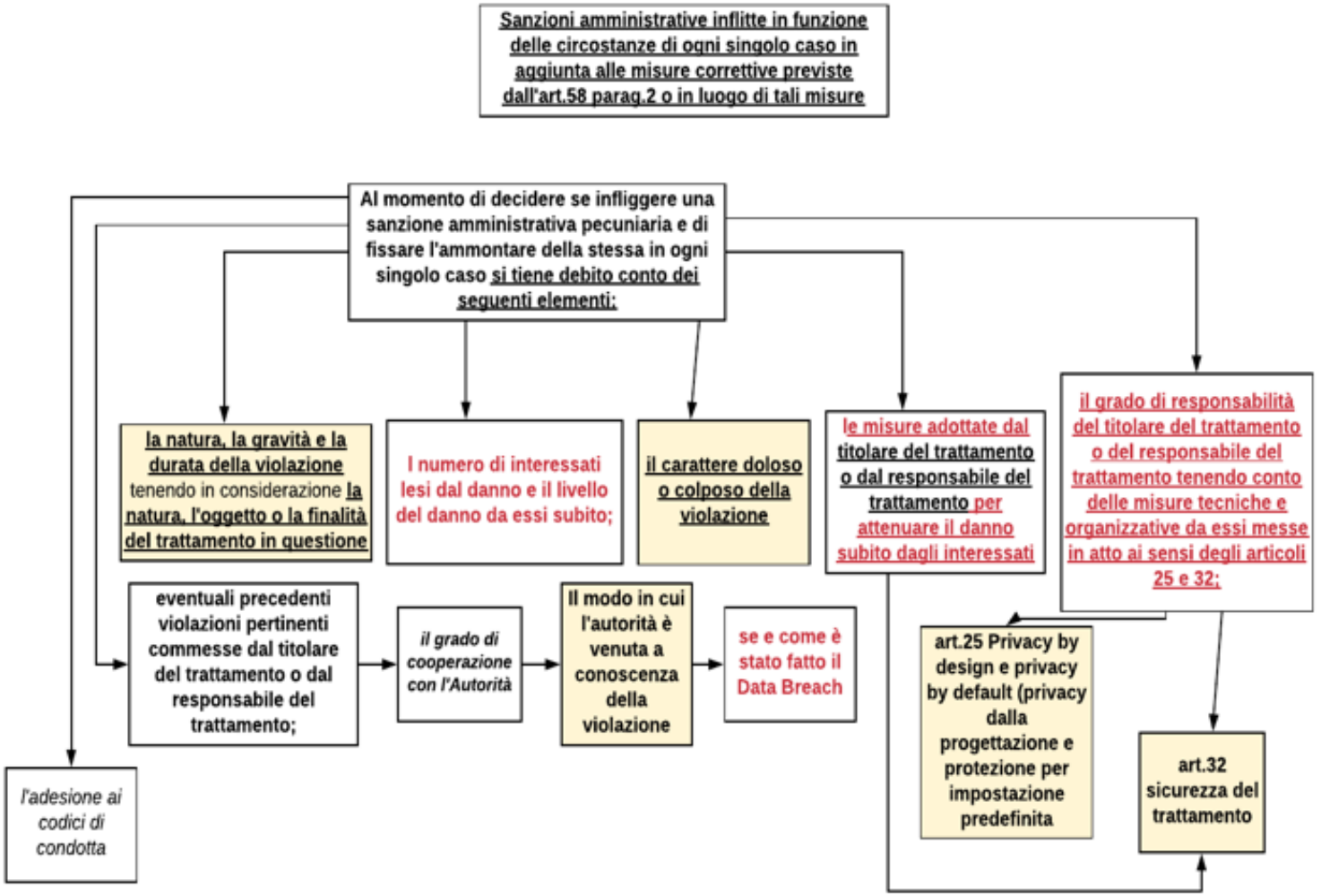
Impatto sull'organizzazione aziendale

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.

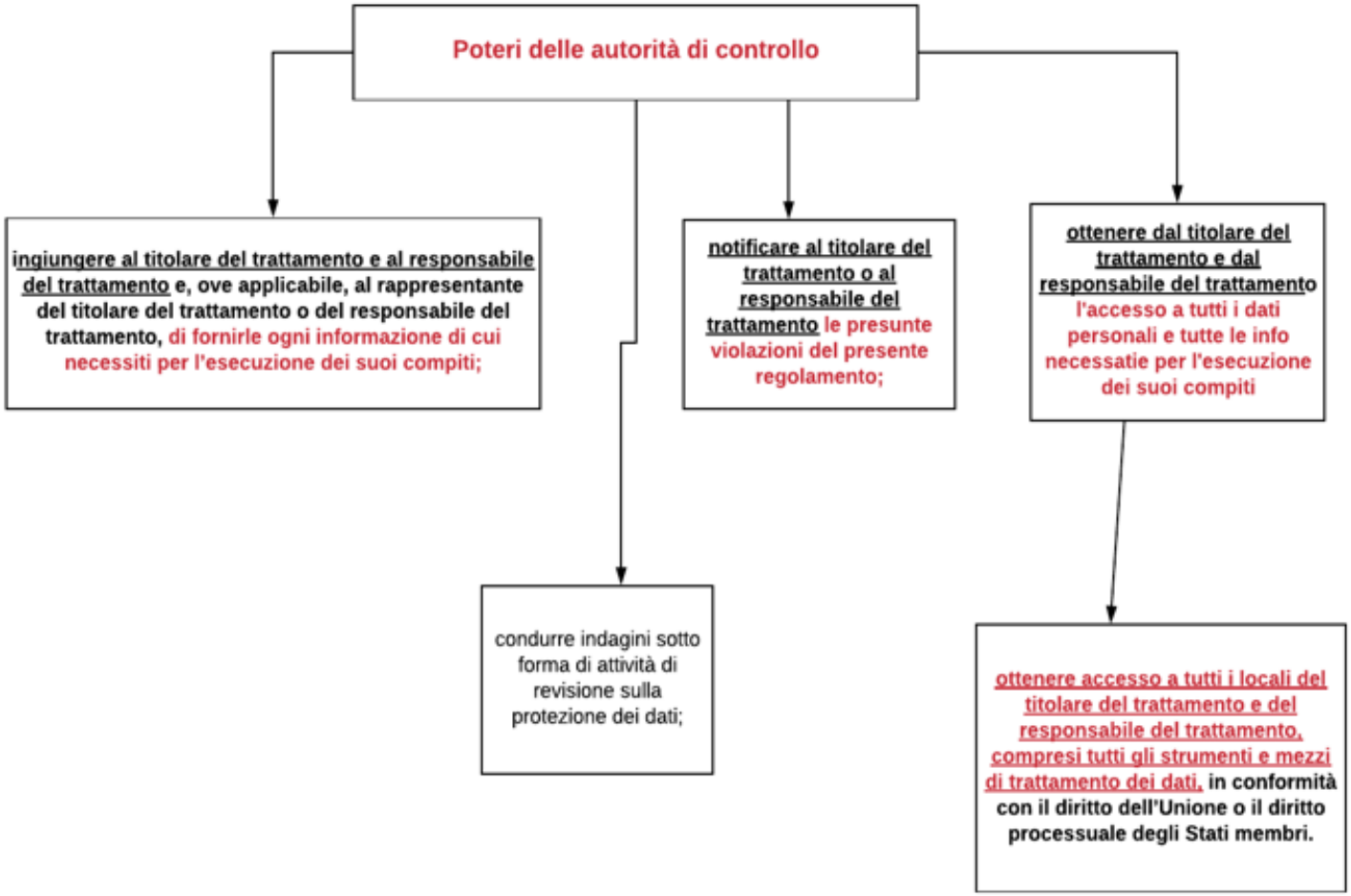


GLOBALPRIVACY
di Nino Papani

Sanzioni GDPR



GLOBALPRIVACY
di Nino Papani


Poteri delle autorità di controllo
ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;
notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;
ottenere dal titolare del trattamento e dal responsabile del trattamento l'accesso a tutti i dati personali e tutte le info necessatie per l'esecuzione dei suoi compiti
condurre indagini sotto forma di attività di revisione sulla protezione dei dati;
ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

Poteri correttivi dell'Autorità di controllo