BANCHE E NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY (GDPR):

il processo di adeguamento tra GDPR e norme di settore – rischi e opportunità

Convenia – Milano, 3 ottobre 2017

JAdp - DATA PROTECTION

IL DATA PROTECTION OFFICER (DPO) E IL MODELLO DI CONTROLLO INTERNO: RAPPORTI E FLUSSI INFORMATIVI

@EUROPRIVACY

JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

Avv. Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

RESPONSABILITA GENERALE PER UNA CONFORMITA DINAMICA, SU MISURA

Art. 28 GDPR: 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 («ACCOUNTABILITY»)

- **Obiettivi**:
  - rispetto dei diritti e libertà delle persone fisiche **= prevenzione adeguata ed efficace** del rischio insito nel trattamento
- **Indicazione degli strumenti per raggiungere gli obiettivi**

- **Responsabilità dei soggetti che operano il trattamento:**
  - **individuare** nei trattamenti progettati e realizzati l'esistenza di rischi di violazione dei diritti degli interessati
  - **valutare** natura, probabilità e gravità di tali rischi
  - **essere in grado di dimostrare** che il trattamento è conforme alle norme

RESPONSABILITA GENERALE DEI SOGGETTI CHE OPERANO IL TRATTAMENTO

Responsabilità aumentata, ma caratterizzata da contenuti più concreti e chiari oltre che adattabili – nella loro traduzione pratica – in funzione di scelte effettuate dal titolare sulla base della propria autonoma determinazione dei rischi connessi al trattamento

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

IL DPO: STRUMENTO DELL'ACCOUNTABILITY

Obbligo di **ATTUARE misure** tecnologiche ed organizzative **adeguate ed efficaci** di prevenzione del rischio di violazione delle norme

1. Individuazione del rischio
2. Valutazione della probabilità e gravità dell'impatto

Valutazione del rischio

Individuazione di strumenti per attenuare il rischio

Rischio attenuabile

Rischio non attenuabile

Obbligo di consultare l'Autorità di controllo

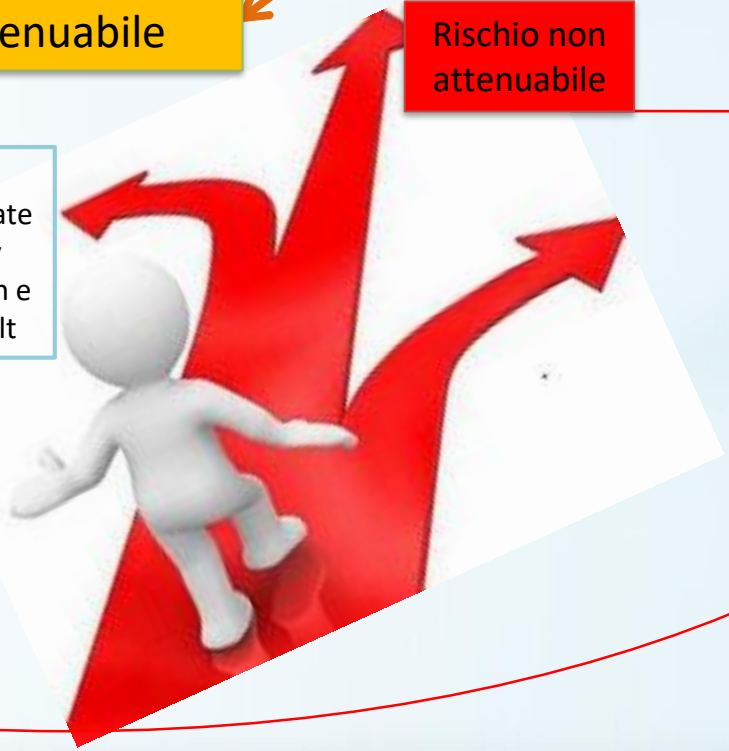
Adozione codici condotta approvati

certificazione

Pratiche improntate a privacy by design e by default

Adozione eventuali misure minime per speciali categorie di trattamenti

Nomina DPO



Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

IL DPO: POSIZIONE, PREROGATIVE E FUNZIONI

*…il titolare del trattamento o il responsabile del trattamento **dovrebbe essere assistito** da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento…* (*GDPR - Considerando 97)*

GDPR - Articolo 38 ***Posizione del responsabile della protezione dei dati***

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. *[…]*

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**.

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

GDPR Art. 39 - Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati **è incaricato** almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) **cooperare con l'autorità di controllo**; e

e) **fungere da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. *[…]*

GDPR Art. 38, c. 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.

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

DPO, COMPLIANCE E AUDIT INTERNO

SISTEMA DEI CONTROLLI INTERNI

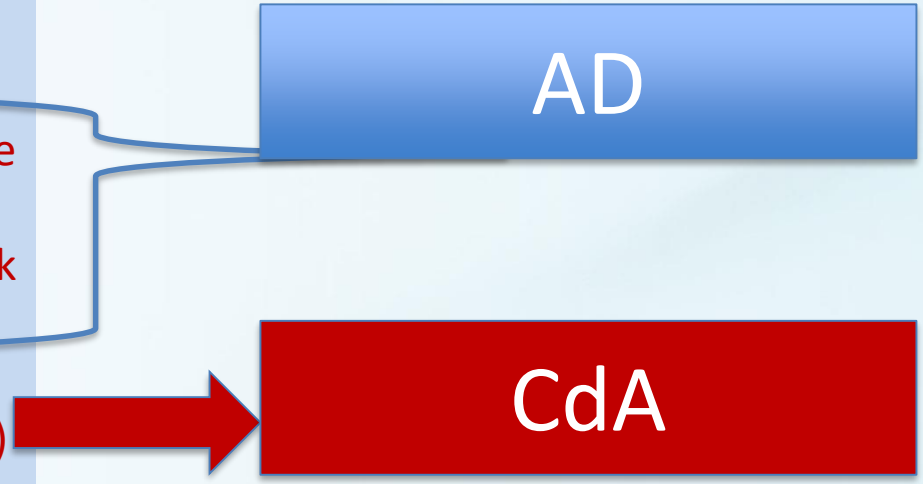
- *"controlli di linea"* - primo livello: controlli di tipo operativo sull'attività aziendale ordinaria nel contesto e nei limiti dei processi di gestione del rischio definiti aziendalmente
- *"controlli sui rischi e sulla conformità"* – secondo livello: controlli con focus sulla corretta attuazione dei processi di gestione del rischio definiti aziendalmente e sulla conformità dell'attività aziendale alle norme, anche interne (*risk management, compliance*…)
- *"revisione interna"* – terzo livello: controlli volti sia all'individuazione di violazioni di norme e regole, anche interne, sia a valutare l'efficienza, efficacia e affidabilità del sistema dei controlli interni e del sistema informativo (*internal audit*).

FUNZIONI AZIENDALI DI CONTROLLO

- la funzione di conformità alle norme (compliance)
- la funzione di controllo dei rischi (risk management function)

- la funzione di revisione interna (internal audit)

[Circ. 285/2013 Banca d'Italia]



Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

DPO

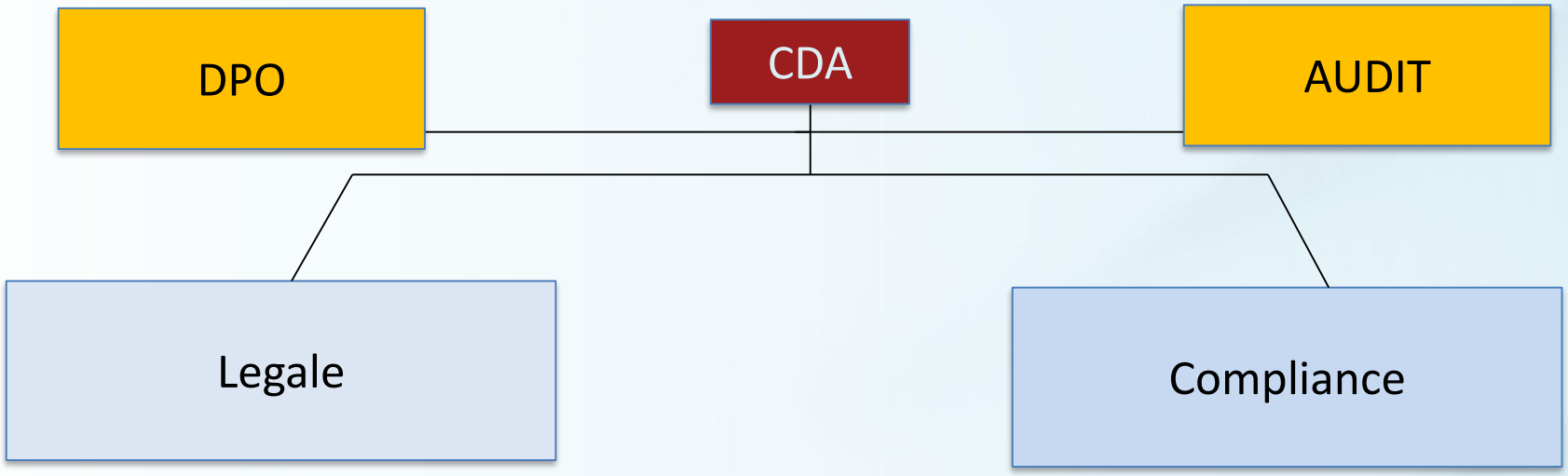
- **INDIPENDENTE**: (cons. 97) *«Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente»*
- **RIFERISCE AL PIU ALTO LIVELLO GERARCHICO** (art. 38, c. 3): *"Il responsabile della protezione dei dati riferisce **direttamente al vertice gerarchico** del titolare del trattamento o del responsabile del trattamento."*
- **SORVEGLIA L'OSSERVANZA DELLE NORME E DELLE POLITICHE DI TRATTAMENTO DEL TITOLARE/RESPONSABILE** *"compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo"* (art. 39 c.1, lett. b)

Vertice amministrativo: es. CdA
(Art. 29 WP)

DPO: CONTROLLORE DELLA CONFORMITÀ DI TUTTI I TRATTAMENTI AZIENDALI
compresi quelli attuati dalle strutture, di ogni livello, appartenenti al sistema di controllo interno

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

IL DPO: POSIZIONE, PREROGATIVE E FUNZIONI



Il DPO è una figura indipendente e quindi non dovrebbe essere assoggettabile a controlli (audit) da parte del Titolare.
Il posizionamento ad un livello pari a quello della Compliance o Legale renderebbe invece, salvo specifici accorgimenti, il DPO auditabile.

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

(contenuti mutuati da G. Butti - Nuovi Regolamenti e nuovi ruoli per le funzioni di controllo – Cetif, Milano 20.9.2017

ORGANISMI DI CONTROLLO: quale ruolo di trattamento?

- **OdV**: "*organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo*" sull'efficace attuazione da parte dell'ente del Modello di Organizzazione, Gestione e Controllo (art. 6.1, lett. b) D. Lgs. 231/2001);

- **Collegio Sindacale**: vigila – anche mediante atti di ispezione e di controllo che possono essere condotti dai sindaci tramite propri dipendenti ed ausiliari – sull'osservanza della legge e dello statuto nonché sull'adeguatezza e sul regolare funzionamento dell'assetto organizzativo, amministrativo e contabile della società di cui costituisce organo (artt. 2403 e 2403-bis Cod. Civ.).

- **INDIPENDENZA**: assenza conflitti di interesse
- **AUTONOMIA:** nessuna forma di interferenza o condizionamento da parte degli organi direttivi dell'ente di riferimento

ORGANO RESPONSABILI DEL TRATTAMENTO?

Il Responsabile agisce sempre secondo istruzioni fornite dal titolare nell'alveo di un trattamento le cui finalità e modalità sono definite da quest'ultimo

CONFLITTO DI INTERESSI tra:
- controllante (organo di controllo / responsabile)

e
- controllato (società / titolare).

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

ORGANISMI DI CONTROLLO: quale ruolo di trattamento?

SE L'ORGANISMO è TITOLARE DEL TRATTAMENTO:

- **autonomia o connessione** tra i trattamenti che attua e quelli dell'ente alla cui sorveglianza è preposto?

CORRELAZIONE STRUMENTALE

ORGANISMO DI CONTROLLO

FINALITÀ investigative e di sorveglianza del rispetto di norme specifiche, individuate *a priori* dalla legge che istituisce l'organismo e le sue caratteristiche

FINALITÀ generali di **gestione aziendale e governo societario**

ENTE

TITOLARI AUTONOMI CORRELATI DEI RISPETTIVI TRATTAMENTI FINALIZZATI – IN ULTIMO – ALLA COMPLIANCE DA PARTE DELL'ENTE ALLE NORME APPLICABILI

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

ORGANISMI DI CONTROLLO: quale ruolo di trattamento?

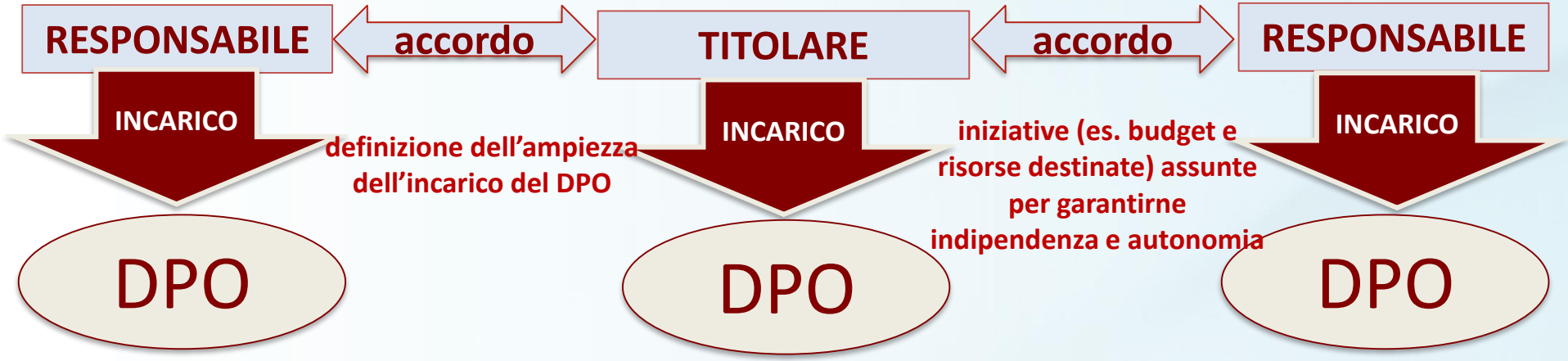
SE L'ORGANO È TITOLARE AUTONOMO CORRELATO CON L'ENTE DEL TRATTAMENTO:

➢ Su chi ricade la **responsabilità della conformità** dei trattamenti dell'organo?

- la **responsabilità di fornire l'informativa agli interessati** in capo all'organismo potrà essere assolta *in uno* con la propria dall'ente, che indicherà l'organo in questione tra i soggetti da esso utilizzati ai fini di adempimento delle norme (cfr. Provv. Garante 23.3.1998, doc. web 40999), facendo diretto riferimento alle specifiche finalità investigative e di sorveglianza e controllo proprie dell'organo stesso
- **gli altri adempimenti** restano invece **a totale carico dell'organismo** (es. misure di sicurezza, nomina responsabili, oneri legati all'attuazione dell'**accountability**)

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

IL DPO: POSIZIONE, PREROGATIVE E FUNZIONI



NATURA E CARATTERISTICHE

- l'adozione del DPO è una misura di attenuazione del rischio, volontaria od obbligatoria, secondo le circostanze
- è un organo CONSULTIVO, DI VIGILANZA E CONTROLLO;
- interno o esterno all'organizzazione aziendale, ma autonomo e indipendente
- figura terza, *a latere* di titolare e responsabile: non assume decisioni né responsabilità esterna per i trattamenti non conformi alle norme

FUNZIONI

- informare e consigliare il Titolare o il Responsabile in merito agli obblighi di protezione dei dati personali
- verificare l'applicazione e l'attuazione delle norme e delle politiche dettate dal titolare / responsabile
- fornire pareri
- fungere da punto di contatto con interessati e Garante

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

DPO e responsabilità del trattamento

L'OBBLIGO DI CONFORMITA RICADE ESCLUSIVAMENTE SULL'ENTE E IL DPO È TERZO RISPETTO AL TRATTAMENTO

CORRELAZIONE STRUMENTALE

DPO

FINALITÀ di assistenza e controllo della conformità al GDPR, individuate *a priori* dalla legge che istituisce l'organismo e le sue caratteristiche

FINALITÀ generale di conformità del trattamento al GDPR

ENTE

I trattamenti attuati dal DPO nello svolgimento delle proprie funzioni sono tutti imputabili direttamente all'*accountability* dell'ente di riferimento, che DECIDE:

- **l'ampiezza dell'incarico**
- **le iniziative a garanzia della indipendenza e autonomia del DPO**
- **nonché – nei casi di istituzione volontaria – la stessa decisione di dotarsi di quest'organo.**

BANCHE E NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY (GDPR):

il processo di adeguamento tra GDPR e norme di settore – rischi e opportunità

Convenia – Milano, 3 ottobre 2017

JAdp - DATA PROTECTION

LA GESTIONE DEI RAPPORTI CON I FORNITORI E GLI *OUTSOURCER*

@EUROPRIVACY

JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

Avv. Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

LA DISTRIBUZIONE DELLE RESPONSABILITA TRA GLI ATTORI DEL TRATTAMENTO

GDPR: Sistema di responsabilità di profilo individuale

Un titolare assume responsabilità per qualsiasi trattamento che effettua direttamente, con altri o che altri effettuino per suo conto: a ciascuno degli attori è riconosciuta responsabilità autonoma ma le diverse responsabilità assumono all'esterno veste unitaria, a garanzia dell'effettivo risarcimento dell'interessato.

Titolare

Contitolare

Responsabile

Responsabile che opera come titolare

Responsabilità «interna»: articolata secondo gli accordi tra le parti contrattuali (garanzie e manleve *in primis*), con rilevanza puramente interna

Responsabilità «esterna»: responsabilità autonome, che sotto il profilo dell'azionabilità dei diritti dell'interessato sono ricondotte *ad unicum* dalla scelta legislativa della prevalenza dell'unicità del trattamento rispetto alla diversità dei titoli di responsabilità degli agenti

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

LA RESPONSABILITA RISARCITORIA NEL GDPR: criterio soggettivo

Art. 82, comma 1 GDPR:

Chiunque subisca un danno *materiale o immateriale* ***causato da una violazione*** *del presente regolamento ha il diritto di ottenere il risarcimento del danno* ***dal titolare del trattamento o dal responsabile del trattamento****»*

- **imputazione individuale:**
- **specifica: collegata alla non conformità** del trattamento a **specifiche norme** del GDPR
- **soggettiva**: riconducibile a **specifici soggetti, formalmente individuati,** cui è imputabile non semplicemente il trattamento, ma la **violazione** che ha causato il danno (esplicito **esonero** per eventi dannosi **non imputabili** ai soggetti attivi: art. 82 c. 3))
- **responsabilità solidale** tra tutti gli agenti – formalmente individuati – coinvolti nella violazione cui è imputabile il danno (art. 82, co. 4 e 5 GDPR)

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

LA RESPONSABILITA RISARCITORIA NEL GDPR: conseguenze pratiche

DIFESA IN GIUDIZIO

basata sulla prova dell'esistenza, delle logiche e della coerenza con i fini di sicurezza e protezione dei dati, dei passaggi (analisi, progetti, azioni) che hanno caratterizzato la costruzione del proprio personale percorso di conformità alle norme.

Art. 82, co. 3: «*Il titolare del trattamento o il responsabile del trattamento è* ***esonerato dalla responsabilità*** *(…) se* ***dimostra*** *che l'evento dannoso non gli è in alcun modo imputabile*.»

Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

«1. Tenendo conto **DELLO STATO DELL'ARTE E DEI COSTI DI ATTUAZIONE** (…) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate (…) volte ad attuare in modo efficace i principi di protezione dei dati (…)»

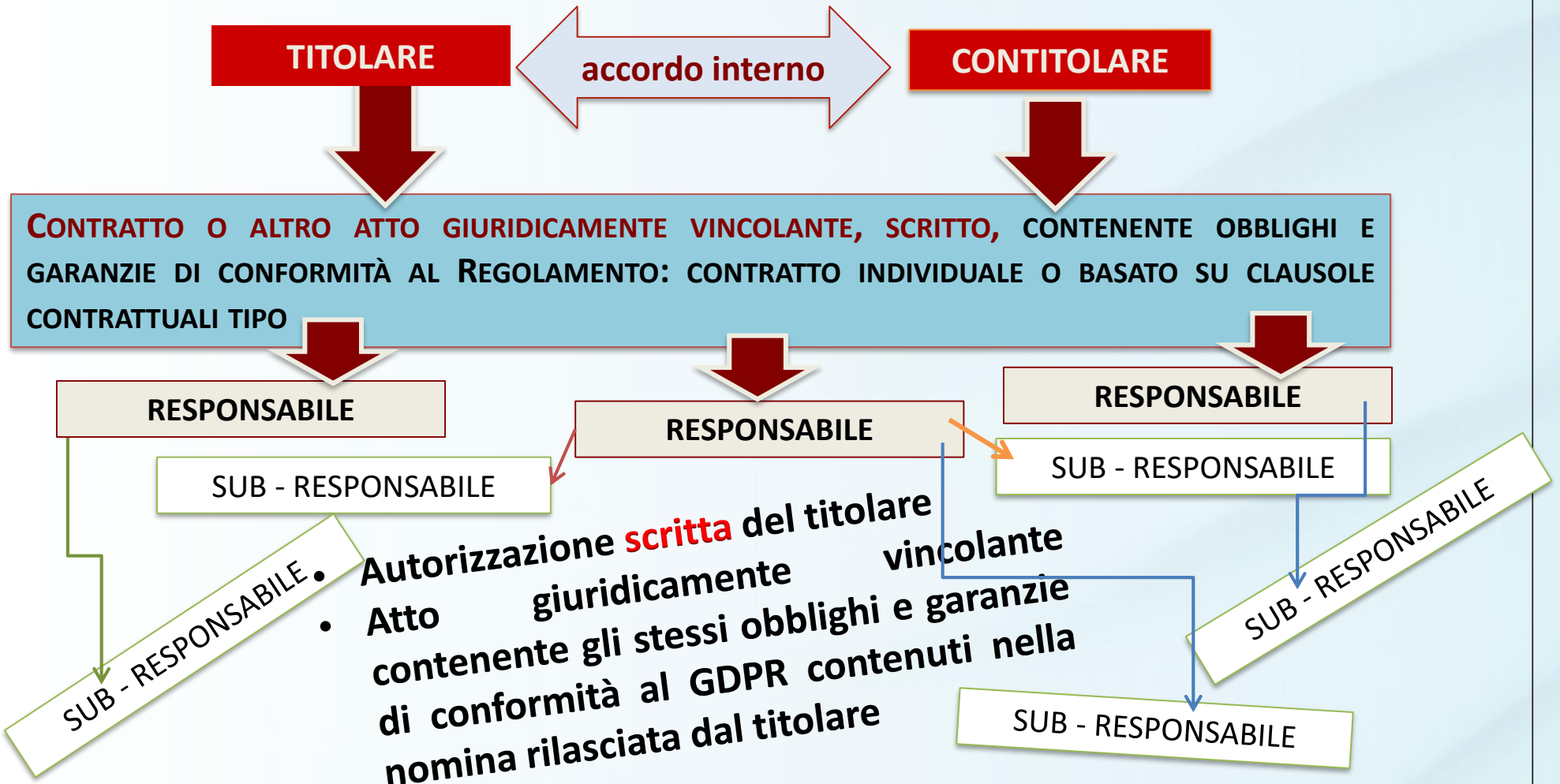
Art. 32 - Sicurezza del trattamento

Tenendo conto **DELLO STATO DELL'ARTE E DEI COSTI DI ATTUAZIONE**, (…) 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»

Avv Maria Roberta Perugini / Partner

mrperugini@jacobacci-law.com

LA RESPONSABILITA GENERALE: formalizzazione dei ruoli



Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

LE RESPONSABILITA PER LA VIOLAZIONE DEL GDPR: AUTONOMIA DEL RESPONSABILE

NOMINA DEL RESPONSABILE

Atto giuridicamente vincolante

indicazione dettagliata:

- ✓ delle circostanze del trattamento affidato
- ✓ degli obblighi e garanzie indicati dal Regolamento

Il Responsabile **risponde del danno se** ha agito in **difformità alle istruzioni** ricevute dal Titolare

Art. 28 c. 3 GDPR:

(…) **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 (…);
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 (…) 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 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 (…);
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.

LE RESPONSABILITA PER LA VIOLAZIONE DEL GDPR: AUTONOMIA DEL RESPONSABILE

NOMINA DEL RESPONSABILE

Atto giuridicamente vincolante

indicazione dettagliata:

- ✓ delle circostanze del trattamento affidato
- ✓ degli obblighi e garanzie indicati dal Regolamento

Il Responsabile **risponde del danno se** ha agito in **difformità alle istruzioni** ricevute dal Titolare

ALCUNI OBBLIGHI DIRETTI DEL RESPONSABILE

- trattare i dati personali eseguendo le istruzioni ricevute dal titolare e informando quest'ultimo immediatamente ove, a parere del responsabile, un'istruzione violi la legge
- implementare e mantenere tutte le misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio
- assistere il titolare nella gestione delle richieste di accesso e nel garantire il rispetto degli obblighi in materia di sicurezza
- fornire al titolare informazioni per dimostrare il rispetto degli obblighi
- designare DPO ove prescritto o in funzione delle caratteristiche dei trattamenti effettuati
- tenere, ove applicabile, un registro delle categorie di attività di trattamento svolte per il titolare

Il Responsabile **risponde del danno se** ha agito **violando gli obblighi che il GDPR pone a suo carico**

Il responsabile ha contemporaneamente

- ➢ **responsabilità derivante dal suo rapporto convenzionale con il titolare (= ove agisca in difformità alle istruzioni legittime del titolare)**
- ➢ **responsabilità autonoma collegata a propri obblighi legali diretti**

Avv Maria Roberta Perugini / Partner

mrperugini@jacobacci-law.com

LA FORMALIZZAZIONE DEI RUOLI E DELLE RESPONSABILITA': METODO, CONTENUTI ED EFFETTI

JAdp - DATA PROTECTION

GARANZIE

CARATTERISTICHE DI PROCESSO

Accordo quadro

MANLEVE

CLAUSOLE CONTRATTUALI TIPO

FUNZIONI E RUOLI DELLE PARTI

PIA

Rapporti con l'interessato

Dimostrazione della conformità

Strumenti per la conformità del trattamento

ACCOUNTABILITY

DEFINIZIONE FORMALE DI CRITERI PER LA CONFORMITA

TRADUZIONE IN BEST PRACTICE E PROCEDURE DOCUMENTALMENTE FORMALIZZATE

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

Disciplina dell'esternalizzazione bancaria (Circ. n. 263 (285)/2006)e GDPR:SINERGIE

Art. 24, c. 1 GDPR: «(…) **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**» **(Accountability)**

Individuazione e formalizzazione di:

- **criteri per la conformità** nello specifico contesto di trattamento
- **tipologia standard di contrattualistica** da applicare nel rapporto con responsabili e contitolari
- **clausole base di ripartizione della responsabilità**
- **modalità di formalizzazione delle deleghe interne**
- **contenuti delle istruzioni** per le varie operazioni di trattamento
- **modalità, misure e strumenti** da utilizzare per il trasferimento sicuro delle informazioni tra i vari attori del trattamento
- **strumenti per il controllo** dell'adempimento dei processi formalizzati **…**

Agg. n.15 del 2/7/2013 Circ. n. 263 (285)/2006, sez. IV art. 1:

In linea con il principio di proporzionalità, tale politica stabilisce almeno:

- il processo decisionale per esternalizzare funzioni aziendali (livelli decisionali; funzioni coinvolte; valutazione dei rischi, inclusi quelli connessi con potenziali conflitti di interesse del fornitore di servizi, e l'impatto sulle funzioni aziendali; valutazione dell'impatto in termini di continuità operativa; criteri per la scelta e la *due diligence* del fornitore);
- il contenuto minimo dei contratti di *outsourcing* e i livelli di servizio attesi delle attività esternalizzate;
- le modalità di controllo, nel continuo e con il coinvolgimento della funzione di revisione interna, delle funzioni esternalizzate;
- i flussi informativi interni volti ad assicurare agli organi aziendali e alle funzioni aziendali di controllo la piena conoscenza e governabilità dei fattori di rischio relativi alle funzioni esternalizzate;
- i piani di continuità operativa (clausole contrattuali, piani operativi, ecc.) in caso di non corretto svolgimento delle funzioni esternalizzate da parte del fornitore di servizi.

Avv Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com

Disciplina dell'esternalizzazione bancaria (Circ. n. 263 (285)/2006)e GDPR: SINERGIE

Agg. n.15 del 2/7/2013 Circ. n. 263 (285)/2006, sez. IV art. 1

(…) - la **sub-esternalizzazione** (ovverosia la **possibilità del fornitore di esternalizzare a sua volta una parte delle attività oggetto del contratto di esternalizzazione**) non deve mettere a repentaglio il rispetto dei principi e delle condizioni per l'esternalizzazione previste nella presente disciplina; a tal fine, il contratto con il fornitore di servizi prevede che eventuali rapporti di sub-esternalizzazione siano preventivamente concordati con la banca e siano definiti in modo da consentire il pieno rispetto di tutte le condizioni sopra elencate relative al contratto primario, inclusa la possibilità per l'Autorità di vigilanza di avere accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il sub-fornitore di servizi.

Art. 28, GDPR:

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.

4. 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.

BANCHE E NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY (GDPR):

il processo di adeguamento tra GDPR e norme di settore – rischi e opportunità

Convenia – Milano, 3 ottobre 2017

IL DATA PROTECTION OFFICER (DPO) E IL MODELLO DI CONTROLLO INTERNO: RAPPORTI E FLUSSI INFORMATIVI

LA GESTIONE DEI RAPPORTI CON I FORNITORI E GLI *OUTSOURCER*

JAdp - DATA PROTECTION

GRAZIE DELL'ATTENZIONE

@EUROPRIVACY

JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

Avv. Maria Roberta Perugini / Partner
mrperugini@jacobacci-law.com