The new General Data Protection Regulation (GDPR):

Ecco cosa cambia: come adeguarsi per essere conformi al nuovo decreto europeo

19 ottobre 2017 – WUERTH PHOENIX SRL

Avv. Luca De Muri
Adacta – Corporate Governance
l.demuri@adacta.it

Adacta
Tax & Legal

NUOVO REGOLAMENTO UE 2016

TRATTAMENTI (ANCHE EXTRA-UE) SVOLTI DA **SOGGETTI STABILITI UE**

TRATTAMENTI SVOLTI DA SOGGETTI **NON STABILITI UE, MA IN LUOGHI RICADENTE NEL DIRITTO DI UN STATO UE**

TRATTAMENTI SVOLTI EXTRA-UE (DA SOGGETTI STABILITI EXTRA UE), MA **RELATIVI ALL'OFFERTA DI BENI E SERVIZI A CITTADINI RESIDENTI NELLA UE**

TRATTAMENTI SVOLTI EXTRA-UE, TALI DA CONSENTIRE IL **MONITORAGGIO DEL COMPORTAMENTO DI CITTADINI RESIDENTI NELLA UE**, se il comportamento ha luogo nella UE

ANCHE LE SOCIETA' STRANIERE CHE SI PROPONGONO COMMERCIALMENTE NELLA UE DEVONO ADEGUARSI

CAMPO DI APPLICAZIONE «AMPLIATO»

(es. controllate/ controllanti estere)

L’ «ADEGUATO ASSETTO ORGANIZZATIVO» PRIVACY-IT È’ UN OBBLIGO NEL CODICE CIVILE…

Adacta Tax & Legal

Art. 2381 co. 5 c.c.: «***Gli organi delegati curano che l'assetto organizzativo (…) sia adeguato*** *alla natura e alle dimensioni dell'impresa (…).*

Gli amministratori sono tenuti ad agire in modo informato; ciascun amministratore può chiedere agli organi delegati che in consiglio siano fornite informazioni relative alla gestione della società.»

ADEGUATO ASSETTO ORGANIZZATIVO «PRIVACY & IT» (artt. 2381 co. 5 e 2403 c.c.)

L'Assetto Organizzativo Adeguato in area privacy-IT **è il risultato di *tre variabili* congiunte**, accomunate dal principio di cd. «approccio basato sul rischio»:

- **Struttura Organizzativa**
- **Distribuzione dei poteri**
- **Sistemi operativi (infrastruttura IT, ecc.)**

ADEGUATO ASSETTO ORGANIZZATIVO «PRIVACY & IT» (artt. 2381 co. 5 e 2403 c.c.)

L'»Adeguato Assetto Organizzativo» privacy-IT è quel **sistema coordinato di *processi*, *funzioni* e *regole operative* in grado di ricondurre entro una soglia (pre)definita come «accettabile» i rischi privacy-IT.**

La soglia di rischio si definisce «accettabile» quando ulteriori presidi e controlli rispetto all'esistente, avrebbero un *costo superiore al danno* potenzialmente derivante dal verificarsi degli eventi negativi da prevenire o mitigare.

ADEGUATO ASSETTO ORGANIZZATIVO «PRIVACY & IT» (artt. 2381 co. 5 c.c.)

La Privacy Compliance e l'IT Risk Governance

1) si occupano della **gestione:**
   - **dei *presidi*** (es. interventi, procedure, ecc.) **e dei *controlli*** (es. verifiche) **relativi ai processi** aziendali impattati dalla normativa privacy **e ai sistemi** IT, **e**
   - **delle *decisioni* correlate a tale gestione**,

   con la finalità di soddisfare **DUE OBIETTIVI PRINCIPALI**:
   a) **l'allineamento dei processi privacy e dei sistemi IT agli obiettivi di business**
   b) **la gestione dei rischi** (correlati alla normativa/operatività) privacy e IT

2) sono dunque «un insieme di logiche e strumenti finalizzati alla ***creazione di un assetto strutturale*** e di un ***contesto di governo* dei processi privacy e del sistema informativo aziendale** (organizzativo) che rendano gli stessi costantemente ***coerenti con le esigenze aziendali, in un contesto di economicità*** (utilizzo/allocazione *più efficace* del capitale e delle risorse umane e tecniche)

NUOVO REGOLAMENTO UE 2016

ANALISI DEI RISCHI

Quali rischi privacy-IT rilevano?

- RISCHI NORMATIVI
- RISCHI OPERATIVI
- RISCHI FINANZIARI

- RISCHI REPUTAZIONALI

.

Adacta Tax & Legal

La gestione dell'adeguato assetto organizzativo privacy & IT deve essere:

- **EMBEDDED** = parte integrante (nativa) dei processi dell'organizzazione;
- **TAYLOR-MADE** in base a dimensioni aziendale, settore di attività, natura e modalità di perseguimento dell'oggetto sociale, obiettivi di business, tipologie di dati e informazioni trattate, finalità dei trattamenti;
- **STRUTTURATA** = sistematica e tempestiva;
- **CONTINUA** nel suo divenire in base all'evoluzione dei prodotti e servizi, della tecnologia, delle normative.

Va quindi verificata con regolare periodicità da parte dei soggetti individuati.

DATE LE DIVERSE VARIABILI IN GIOCO NON ESISTONO, ASSETTI ORGANIZZATIVI "ADEGUATI" IT-PRIVACY IN OGNI CIRCOSTANZA

L'ASSETTO ORGANIZZATIVO PRIVACY-IT E LA DIGITAL TRASFORMATION

Nello scenario della Digital Economy la trasformazione digitale diventa un fattore critico di successo per le organizzazioni di qualsiasi dimensione e settore. Si tratta di un fenomeno "disruptive" abilitato dalla convergenza dei nuovi paradigmi tecnologici. La Digital Trasformation si declina su tre aree principali, ciascuna fondamentale per costruire un disegno coerente

CUSTOMER EXPERIENCE

Il "customer journey" è sempre più multicanale.

L'azienda deve essere in grado di attuare una gestione omnichannel del cliente e fornire una user experience sempre più personalizzata lungo tutti i canali di contatto.

MODELLI DI BUSINESS

La tecnologia digitale modifica le regole e I confini del settore di appartenenza, rendendo necessario per l'azienda un ripensamento in chiave digitale del proprio modello di business, con l'opportunità di evolvere l'offerta con la creazione di nuovi prodotti e servizi.

PROCESSI E ORGANIZZAZIONE

Ridisegnare i processi operativi grazie all'ausilio delle tecnologie per renderli più flessibili e veloci. Creare nuovi modelli organizzativi, competenze e figure professionali. Investire sullo sviluppo di competenze specifiche sul digitale, sulla creazione di team cross/funzionali diretti ad integrare le competenze id diverse funzioni aziendali, tecnologiche e funzionali.

L'ASSETTO ORGANIZZATIVO PRIVACY-IT E LA DIGITAL TRASFORMATION

La Digital Trasformation complica il quadro organizzativo aziendale, affiancando ai "vecchi" rischi in ambito privacy-IT (già di per sé non sempre ben percepiti) nuove categorie di rischio legate alla multicanalità, ai nuovi modelli di business e ai nuovi processi organizzativi

CUSTOMER EXPERIENCE

Rischi connessi alla *multicanalità* e alla *tailorizzazione* del customer journey. L'azienda deve adeguatamente gestire i rischi connessi ai diversi canali di contatto con il cliente (web, social network, device mobili, gps, sms, apps, cloud, ecc) e deve gestire correttamente i dati personali che è necessario trattare per personalizzare la user experience.

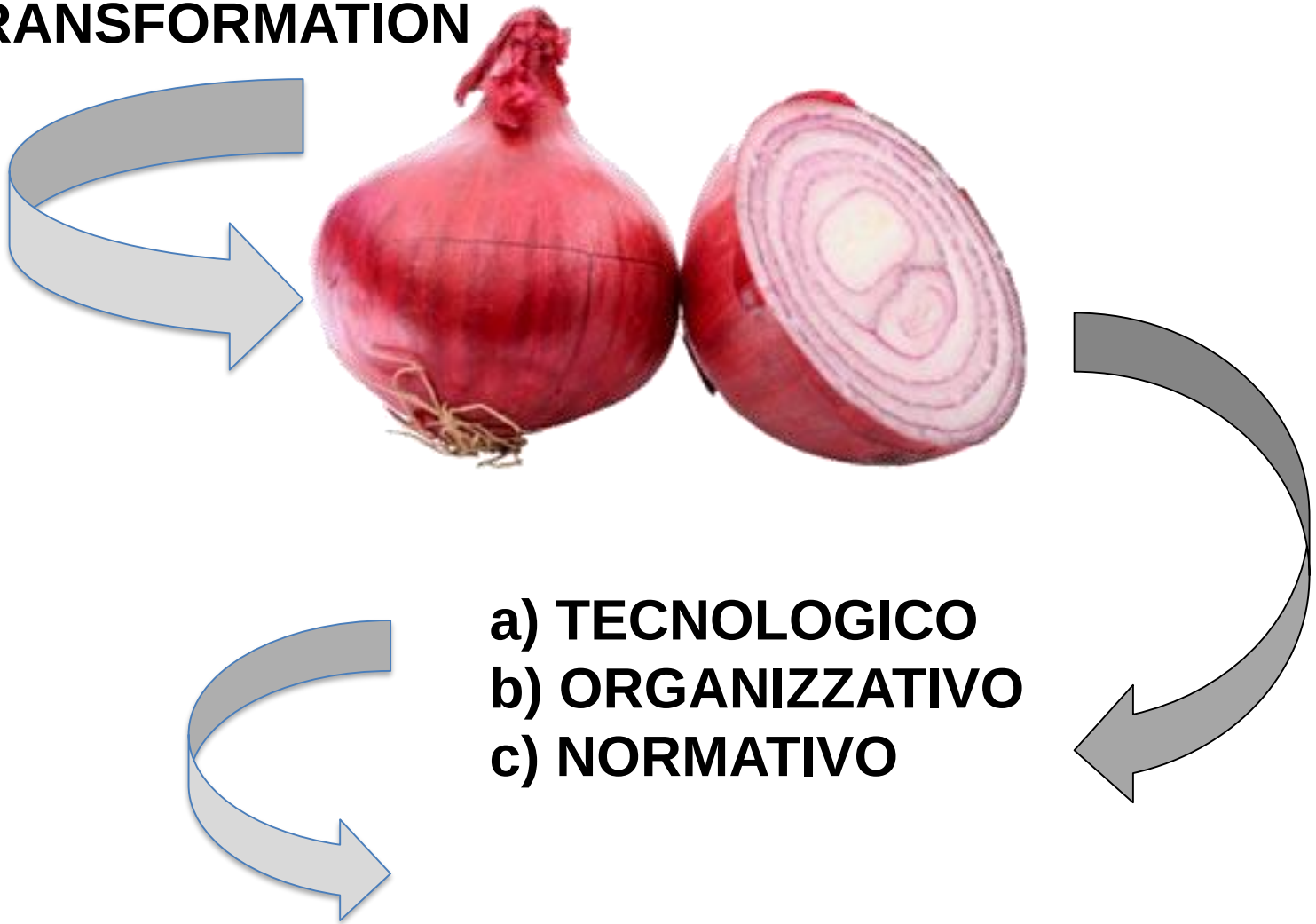
MODELLI DI BUSINESS

Il ripensamento in chiave digitale del modello di business e lo sviluppo dell'offerta di nuovi prodotti e servizi, impone di fatto all'azienda di acquisisre la capacità di gestione secondo criteri efficenti ed efficaci – cioè adeguati - *ambiti innovativi e diversificati di rischio privacy e IT* (operativo, normativo, ecc) ,

PROCESSI E ORGANIZZAZIONE

Il reengineering tecnologico dei processi e dei modelli gestionali e organizzativi, l'ingresso di nuove figure professionali "digitali", l'outsourcing dei servizi IT, esigono una idonea governance per l'idoneo coordinamento di ruoli, funzioni e responsabilità, e per garantire presidii e controlli adeguati dei relativi rischi tecnici e legali, tra cui la privacy.

I «TRE STRATI» DELLA DIGITAL TRANSFORMATION



a) TECNOLOGICO
b) ORGANIZZATIVO
c) NORMATIVO

VANNO GESTITI IN MODO INTEGRATO.

REGOLAMENTO UE 679/2016: CONFERMA E SVILUPPI DELL'OBBLIGO DI ADEGUATEZZA PRIVACY-IT

NUOVO REGOLAMENTO UE 2016

INTRODUCE ALCUNI PRINCIPI

SOLO RELATIVAMENTE NUOVI

(PREVISTI

- **IN PARTE DALLA NORMATIVA ANTERIORE,**
- **IN PARTE DALLE BEST PRACTICES IN MATERIA DI ADEGUATEZZA ORGANIZZATIVA**
- **IN PARTE DALLE METODOLOGIE CERTIFCATE DI GESTIONE DELLE INFORMAZIONI)**

PRIVACY BY DESIGN

= GESTITA «NATIVAMENTE» (NON EX POST) NEI PROCESSI OPERATIVI

PRIVACY BY DEFAULT

= INCLUDE MENO DATI PERSONALI POSSIBILI

«EFFETTIVITA'» DELLA GESTIONE PRIVACY

(COME GIA' PREVISTO IN AMBITO MODELLI ORGANIZZATIVI 231 DALLA NORMATIVA ITALIANA)

ACCOUNTABILITY

= NON BASTA *ADEMPIERE* ALLA NORMA, OCCORRE ANCHE ATTREZZARSI IN MODO DA *DIMOSTRARE* L'ADEMPIMENTO

Adacta Tax & Legal

Art. 31 D. Lgs. 196/2003. Obblighi di sicurezza.

I dati personali devono essere

CUSTODITI **CONSERVATI**

anche in relazione

alle conoscenze acquisite in base al progresso tecnologico

alla natura dei dati

alle caratteristiche le trattamento

in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di

Distruzione e perdita anche accidentale

Accesso non autorizzato

Trattamento non consentito

Trattamento non conforme alle finalità

Attuale regime privacy (fino al 24.05.2018)

Misure *minime* di sicurezza privacy:

- **Tassativamente elencate** dalla legge (art. 33 e 58 c. 3 T.U. + "Disciplinare Tecnico" Allegato B + provv.ti ad hoc Garante);
- Obbligatorie a prescindere dalle concrete caratteristiche organizzative del Titolare

Misure *idonee* di sicurezza:

- Da individuarsi **caso per caso** (tendenzialmente discrezionali ma obbligo di diligente valutazione) in base all'analisi dei rischi esistenti
- dipendono dalle concrete caratteristiche organizzative del Titolare

  (NB: esistono varie normative tecniche standard: es. ISO/IEC 27001, UNI/ENV 12924 (sanità), ma nessuna è adottato ufficialmente

NUOVO REGOLAMENTO UE 2016

NB: Molti princìpi 2016 UE replicano la Direttiva 95/45/CE

~~**D.LGS. 196/2003 VIENE ABROGATO**~~

~~**VENGONO FORMALMENTE ABROGATE LE MISURE DI SICUREZZA "MINIME"**~~

OBBLIGO MISURE DI SICUREZZA PRIVACY "ADEGUATE" AI RISCHI

(IDONEITA' IN CONCRETO = EFFICACIA)

Ma rimarranno rilevanti anche dopo il 2018 varie fonti:

Art. 2381 co., 5 c.c.
Obbligo adeguatezza organizzativa IT-privacy

Provvedimenti Generali, Autorizzazioni e Decisioni del Garante

Best Practices

Adacta Tax & Legal

NUOVO REGOLAMENTO UE 2016 → **In vigore dal 5/2018**

"Anche se in Italia le imprese stentano ancora a concepire la privacy come una due diligence, **il nuovo Regolamento UE privacy 2016** richiederà una protezione dei dati sostanziale.
Tuttavia **il nuovo testo normativo non contiene una lista preconfezionata di misure di sicurezza, che dovranno essere invece individuate dalle stesse aziende**, effettuando previamente una **valutazione d'impatto** sulla protezione dei dati.
Per poter svolgere queste attività ad un livello adeguato, oltre a professionisti che conoscano bene la normativa, serviranno anche esperti con skills e competenze per gestire i dati e le informazioni con un elevato livello di sicurezza.“

(*Fonte: Federprivacy – 2016*)

Quindi **la personalizzazione delle misure di sicurezza in ottica di adeguatezza in concreto, viene confermata come obbligo inderogabile** (benchè già sussistente in base alle norme del codice civile, artt. 2381 co. 5 c.c. e 2403 c.c.)

NUOVO REGOLAMENTO UE 2016

OBBLIGO MISURE DI GESTIONE PRIVACY "ADEGUATE" AI RISCHI

(*IDONEITA' IN CONCRETO = EFFICACIA*)

Cosa occorre fare?

Migrare da un approccio prescrittivo-formalistico all'impostazione della responsabilità aziendale finalizzata ad un modello «effettivo in concreto» cioè *efficace* (= allineato ai requisiti normativi e agli obiettivi aziendali) ed *effettivo*.

Le Misure Adeguate di sicurezza includeranno almeno le Misure Minime fino a oggi obbligatorie, più altre necessarie misure **individuate caso per caso** dal Titolare in base al **«risk-based approach»**.

Adacta Tax & Legal

PRIVACY BY DESIGN E BY DEFAULT = Ribaltamento dell'approccio tradizionale (basato su verifiche di conformità *a valle* del processo di progettazione o produzione)
Resta come in passato l'inversione dell'onere probatorio

Esigenza di un APPROCCIO (STRUTTURATO E CONTINUO) ai processi aziendali e alle procedure/misure di tutela dei dati personali e delle informazioni

Esigenza di approccio TAYLOR MADE: personalizzazione delle procedure e della documentazione di supporto (policy, istruzioni, ecc).

VALORIZZAZIONE DELLE BEST PRACTICES: occorre non limitarsi alla pura normative, ma ricercare volta per volta le soluzioni operative che consentano il giusto compromesso tra esigenze di business e formalizzazione

NUOVO REGOLAMENTO UE 2016 → **In vigore dal 2018**

OBBLIGO DI PROVA DELLE MISURE DI GESTIONE »ADEGUATE» (art. 24):

(il titolare)

«tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche» (…) mette in atto misure tecniche e organizzative ***adeguate*** per garantire, ed **essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al presente regolamento**.

Dette misure sono riesaminate e aggiornate qualora necessario (…).

Se ciò è proporzionato (…) le misure (…) includono l'attuazione di politiche ***adeguate*** in materia di protezione dei dati (…)». (c.d. «accountability»)

NUOVO REGOLAMENTO UE 2016 → **In vigore dal 2018**

OBBLIGO DI PRIVACY BY DESIGN (= Protezione dai dati fin dalla progettazione): art. 25.1

Il titolare (…)

«tenuto conto dello stato dell'arte e dei costi di attuazione, nonchè della natura, campo di applicazione, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche» **sia al momento di determinare i mezzi di trattamento sia all'atto del trattamento** (…)

mette in atto misure tecniche ed organizzative *adeguate* (es. minimizzazione, pseudonimizzazione, cifratura, data recovery, n.d.r..)

volte ad attuare i principi di protezione dei dati (…) in modo *efficace*, e ad integrare nel trattamento le necessarie garanzie

al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati (…)»

NUOVO REGOLAMENTO UE 2016 → **In vigore dal 2018**

OBBLIGO DI PRIVACY BY DEFAULT (= Protezione dei dati per impostazione predefinita): art. 25.2

Il titolare

«(…) mette in atto misure tecniche ed 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 di dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità (…)»

- NB: l'adeguamento dei processi aziendali deve partire fin da ora, perché può comportare impegni operativi importanti a vari livelli e necessità di budget, quindi una tempestiva ed idonea pianificazione delle attività dei soggetti coinvolti
- Un meccanismo di certificazione può essere utilizzato come elemento per dimostrare la conformità ai requisiti predetti (art. 25.3)

NUOVO REGOLAMENTO UE 2016 → **In vigore dal 2018**

OBBLIGO DI MISURE DI SICUREZZA »ADEGUATE» (art. 32.1):

(il titolare e il responsabile)

«tenuto conto dello **stato dell'arte** e dei **costi** di attuazione, nonchè della **natura**, campo di **applicazione**, del **contesto** e delle **finalità** del trattamento, nonché del **rischio** di varia probabilità e gravità **per i diritti e le libertà delle persone fisiche**» (…) **mettono in atto misure tecniche e organizzative *adeguate* per garantire un livello di sicurezza adeguato** al rischio (…)»

Art. 32.2: «nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi** presentati da trattamento dati derivanti in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque trattati».

Adacta Tax & Legal

OBBLIGO DI ADEGUATEZZA PRIVACY-IT E PRESUPPOSTI DI RESPONSABILITA' PRIVACY

L'attuale Codice privacy non impone solo il rispetto delle misure *minime* di sicurezza, bensì anche un più generale **obbligo** di **"custodire e controllare i dati personali oggetto di trattamento,** anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, **in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.** Si tratta delle cd. misure *idonee* di sicurezza (ulteriori cioè rispetto alle misure minime).

L'onere della prova (di non colpevolezza) spetta all'azienda che tratta i dati. Essa deve dimostrare di aver adottato "tutte le misure idonee ad impedire che il danno si verificasse"; altrimenti risarcisce il danno (responsabilità oggettiva).

L'obbligo di adeguatezza organizzativa privacy-IT va adempiuto nell'ottica di consentire la suddetta «prova contraria» in relazione alla suddetta gestione dei rischi. **Tale impostazione resta valida anche con il Regolamento UE privacy 679/2016.**

L’adeguatezza implica di saper *riconoscere e valutare preventivamente:*

- SE e COME le attività ed I processi aziendali verso e da DIPENDENTI, FORNITORI, CLIENTI e PARTNER, rilevano ai sensi della normativa privacy-IT,
  (per individuare, prevenire e/o ridurre i rischi e assumere decisioni in piena consapevolezza).

La centralità delle informazioni in ogni processo aziendale si compagna infatti al carattere «pervasivo» ma non sempre «visibile», della normativa privacy, con il rischio di incorrere in violazioni dovute ad una *non corretta o non completa percezione del concreto ambito di applicazione* della normativa**.**

- le relazioni tra normative privacy e standard di sicurezza IT (organizzativi e tecnici), e tra queste due tematiche e gli obiettivi di business
  (per attivare i necessary presidi e controlli in modo coordinato ed efficiente).

PRIVACY BY DESIGN & BY DEFAULT

LATO CLIENTI

NUOVA GESTIONE TECNICA INTERNA

= OBBLIGO DI ANALISI DEI SOFTWARE/SERVIZI IT DI TERZI FORNITORI, PER VERIFICARE EVENTUALI GAP DI CONFORMITA' E/O ESIGENZE DI ADEGUAMENTO AI PRINCIPI NORMATIVI IN ESAME

INDIVIDUAZIONE DEI RESP.LI DELL'ASSESSMENT (HR, MKT, IT, PRIVACY, ecc.) + COINVOLGIMENTO DEL NUOVO DATA PRIVACY OFFICER

PIANIFICAZIONE E ATTUAZIONE DI BUDGET, (RI)NEGOZIAZIONE CON FORNITORI SW, SCOUTING DI NUOVI FORNITORI SW

PRIVACY BY DESIGN & BY DEFAULT

LATO SOFTWARE HOUSE

NUOVA GESTIONE TECNICA INTERNA

= OBBLIGO DI ANALISI DEI SOFTWARE/SERVIZ IT EROGATI, PER VERIFICARE EVENTUALI GAP DI CONFORMITA' E/O ESIGENZE ED OPPORTUNITA' DI ADEGUAMENTO AI PRINCIPI NORMATIVI IN ESAME

DIALOGO CON CLIENTI (SVILUPPI APPLICATIVI) (es. CRM, Commerciale, Gestionale, web/mobile, post-vendita)

NUOVO DRIVER COMMERCIALE (RIVISITAZIONE/VALORIZZAZIONE DELL'OFFERTA)

L’ANALISI DEI RISCHI PRIVACY-IT: APPROCCIO DI METODO

NUOVO REGOLAMENTO UE 2016

OBBLIGO MISURE DI SICUREZZA PRIVACY "ADEGUATE"

(= EFFICACI) ...

A cosa dare priorità?

... principale effetto è innanzitutto l'intensificazione dell'obbligo di analisi dei rischi IT/privacy:

… a sua volta funzionale alla necessaria *adozione di un approccio basato sul rischio* nell'assetto organizzativo aziendale ex art. 2381 co. 5 c.c.

Adacta Tax & Legal

NUOVO REGOLAMENTO UE 2016

OBBLIGO DI VALUTAZIONE D'IMPATTO

Che cosa analizzare?

La VALUTAZIONE D'IMPATTO (o analisi preventiva) dovrà essere operata in relazione non solo alle misure di sicurezza, ma in generale alle modalità di gestione della privacy (e quindi inevitabilmente anche IT)

NUOVO REGOLAMENTO UE 2016

OBBLIGO DI

- **ANALISI PERIODICA**
- **PROVA DI EFFICACIA**

DELLE MISURE DI SICUREZZA E DI GESTIONE DELLA COMPLIANCE

Ma «analizzare» non basta: occorre conformarsi e provarlo!

Art. 30 (Accountability):

«Il titolare mette in atto **misure** tecniche e organizzative **adeguate** per garantire un livello di sicurezza **adeguato** al rischio, che comprendono, tra l'altro (…)

«una **procedura per provare, verificare e valutare regolarmente l'efficacia delle misure** tecniche e organizzative al fine di garantire la sicurezza del trattamento».

Adacta Tax & Legal

NUOVO REGOLAMENTO UE 2016

OBBLIGO DI ANALISI DI IMPATTO DELLE ATTIVITA' SULLA PRIVACY = PIA

Casi obbligatori di analisi:

ATTIVITA" DI **TRATTAMENTO SU LARGA SCALA, DI CATEGORIE PARTICOLARI DI DATI EX ART. 9 (DATI SENSIBILI, SANITARI O RELATIVI ALLA VITA SESSUALE, GENETICI, BIOMETRICI, O GIUDIZIARI)** (es. sanità, sorveglianza, elaborazione buste paga, marketing con profilazione degli interessati)

ATTIVITA" DI **VALUTAZIONE SISTEMATICA E GLOBALE DI ASPETTI PERSONALI** DI PERSONE FISICHE, **BASATA SU TRATTAMENTO AUTOMATIZZATO,** COMPRESA LA PROFILAZIONE, E **DA CUI DISCENDONO DECISIONI** CHE HANNO EFFETTI GIURIDICI O INCIDONO ALTRIMENTI SIGNIFICATIVAMENTE SULLE PERSONE

SORVEGLIANZA SISTEMATICA DI UNA ZONA ACCESSIBILE AL PUBBLICO

Adacta Tax & Legal

NUOVO REGOLAMENTO UE 2016

OBBLIGO DI ANALISI DI IMPATTO DELLE ATTIVITA' SULLA PRIVACY = PIA

Casi obbligatori di analisi:

La preoccupazione del legislatore comunitario è stata quella di esentare dall'analisi dei rischi priVacy-IT le piccole e piccolissime realtà aziendali.

Fatte salve le suddette situazioni, per il principio generale di «adeguatezza organizzativa» previsto sia dal codice civile che dal Reg. ue 679/2016),
l'analisi dei rischi è di fatto un obbligo per ogni azienda di dimensione organizzativa apprezzabile.

Adacta Tax & Legal

NUOVO REGOLAMENTO UE 2016 + ART. 2381 CO. 5 C.C. + BEST PRACTICES

OBBLIGO DI ANALISI DEI RISCHI + ADEGUATEZZA ORGANIZZATIVA

«mettere la testa sotto la sabbia» non è la soluzione

Adacta Tax & Legal

TRAMITE L'ANALISI DEI RISCHI PRIVACY/IT, L'AZIENDA:

- **INDIVIDUA I RISCHI** PRIVACY-IT (TIPOLOGIE DI EVENTI RISCHIOSI E DI IMPATTI POTENZIALI

- **VALUTA I RISCHI** PRIVACY MEDIANTE UN MECCANISMO DI ATTRIBUZIONE DI UNA SCALA NUMERICA (DA 1 A 4) SIA ALLE *PROBABILITA*' DEL RISCHIO CHE ALLA *GRAVITA*' DEL RELATIVO IMPATTO

- INTERFACCIA AD OGNI RISCHIO INDIVIDUATO LE RELATIVE CONTROMISURE ADOTTATE (una stessa misura talora può avere effetto su diversi rischi)

- **IDENTIFICA E VALUTA I G**AP DI CONFORMITA'

- DISPONENDO DI UNA BASE **MISURABILE E MONITORABILE** NEL TEMPO (accountability) PER PIANIFICARE, ATTUARE E VERIFICARE PERIODICAMENTE LE AZIONI DI ADEGUAMENTO DELLA **GESTIONE** PRIVACY

RISK MANAGEMENT

Si intende per Risk Management

l'insieme delle attività dirette a individuare, valutare, gestire e controllare tutti i tipi di eventi (rischi ed opportunità).

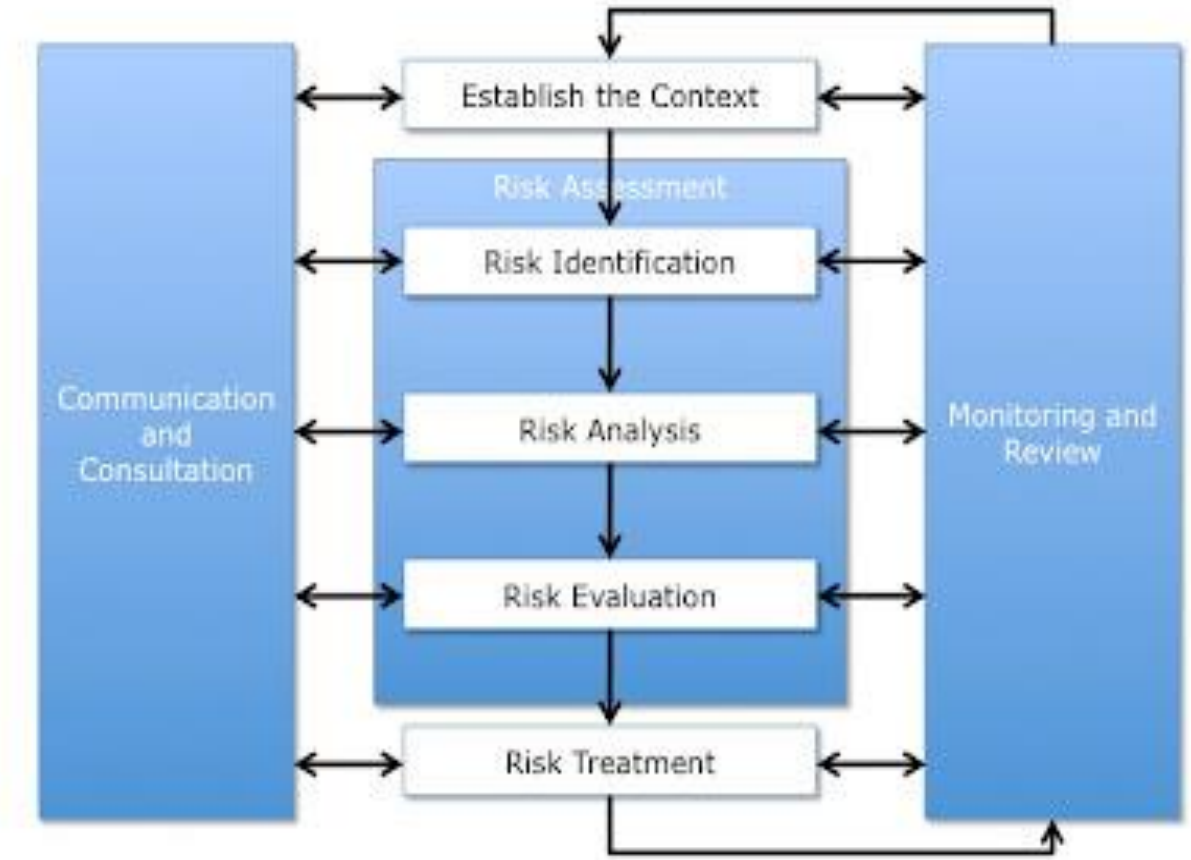
Il processo di risk management può essere suddiviso in tre principali macro-attività:

- Individuazione dei rischi
- Valutazione dei rischi
- Gestione dei rischi (identificazione e attuazione delle attività miranti a prevenire o ridurre i rischi)

LA NORMA ISO 31000: GESTIONE DEL RISCHIO - PRINCIPI E LINEE GUIDA

La norma ISO 31000 è stata sviluppata con l'obiettivo di stabilire un framework generale (in 7 fasi) per l'identificazione, l'analisi, la valutazione, la gestione e il monitoraggio del rischio.

A prescindere dalla eventuale adozione della ISO 31000, vi è l'obbligo di fotografare e gestire il rischio IT-privacy in modo «adeguato».



Le **categorie di rischio** individuate, vengono associate a gradi crescenti di **Probabilità** e di **Impatto**, determinando così una graduatoria numerica per ciascun rischio. Probabilità e Impatto sono influenzati dall'efficacia delle Misure di sicurezza attuate

R = p x i

R = valore del **rischio inerente** (quantificazione numerica del rischio)

p = (**probabilità**) stima della **possibilità** del verificarsi dell'evento di rischio. Di regola viene espressa in termini percentuali o decimali. E' il fattore che misura l'**incertezza** dell'evento fonte di rischio.

i = (**impatto**) quantifica **l'intensità delle conseguenze** dell'evento di rischio. Può essere espresso in unità monetaria, tempo, quantità o performance.

Probabilità e Impatto sono influenzati dall'**efficacia** delle misure di sicurezza e/o altre attività di gestione attuate. Il definisce **Rischio residuo** il valore del rischio inerente dopo l'applicazione allo stesso della riduzione derivante da tali misure/azioni.

$$R' = p \times i - e$$

R' = valore del **rischio residuo** (quantificazione numerica del rischio, al netto delle misure di protezione e azioni di gestione applicate allo stesso)

e = (**efficacia dei presidi e controlli**): valore che indica la riduzione del rischio inerente per il tramite dei presidi e controlli implementati con riguardo ad una determinata fonte (evento) di rischio

Le **categorie di rischio** individuate, vengono associate a gradi crescenti di **Probabilità** e di **Impatto**, determinando così una graduatoria numerica per ciascun rischio. Probabilità e Impatto sono influenzati dalle Misure di sicurezza attuate

Codice Rischio	TIPOLOGIA DI EVENTO	Descrizione evento	Impatto/ Gravità (1-4)	Probabilità (1-4)	Rischio da abbattere IxP (1-16)	Rischio residuo (*post misure, vedi oltre colonne di dx*)

RISCHIO RESIDUO:	Il rischio che permane dopo l'applicazione delle misure di sicurezza. Tale rischio deriva dalla moltiplicazione del valore "gravità dell'impatto" (da 1 a 4) con il valore "probabilità dell'evento" (da 1 a 4) e si classifica in:	
	rischio trascurabile (0-4)	Tale categoria di rischio necessita solo di un'attività di monitoraggio, non richiede alcun intervento, tuttavia non si escludono miglioramenti tecnici e organizzativi
	rischio basso (5-8)	In questo caso la sola attività di monitoraggio non è sufficiente, ma deve essere integrata con interventi pratici atti all'eliminazione o riduzione del rischio
	rischio medio (9-12)	L'intervento correttivo deve essere immediato, la gravità e la probabilità legate a questa tipologia di rischio creano una situazione pericolosa
	rischio alto (13-16)	L'intervento correttivo deve essere immediato, la gravità e la probabilità legate a quata tipologia di rischioi creano una situazione estremamente pericoloso

Tipologia di rischio	RISCHI SUI TRATTAMENTI RELATIVI AI DATI					
Tipologia di evento	Accesso esterno non autorizzato ai documenti	Accesso non autorizzato degli incaricati ai dati (cartacei od elettronici)	Manomissione/Cancellazione non autorizzata di dati	Errori umani nella gestione della sicurezza fisica	Carenza di consapevolezza, disattenzione o incuria	Co fr
Descrizione evento	Persone non autorizzate possono accedere a documenti e dati cartacei (es. protocollo, personale, ecc.) incustoditi presenti su scrivanie, scaffali a vista, armadi non chiusi, archivi correnti o archivi storici, o sottraendo credenziali di autenticazione possono accedere ad archivi elettronici.	A causa della mancanza di consapevolezza, incuria, distrazione o per cause tecniche gli utenti possono accedere a dati al cui trattamento non sono autorizzati	Persone autorizzate o non autorizzate possono volontariamente operare la immissione, la manomissione/alterazione o la cancellazione o distruzione (danneggiamento) non autorizzata di dati	Badge, chiavi o altri strumenti di accesso ad aree ad accesso limitato, possono essere sottratti da soggetti malintenzionati e impropriamente utilizzati per accedere ai locali/aree dove sono conservati dati cartacei	A causa di incuria, disattenzione o scarsa conoscenza degli ambiti di trattamento autorizzati (es. dovuta a scarsa formazione) gli operatori possono digitare dati errati, non pertinenti o incompleti od operare trattamenti o comportamenti non congrui	G po ill ap ec co da
Codice rischio	R10	R11	R12	R13	R14	
Impatto/ Gravità (1-4)	3	3	4	3	4	
Probabilità (1-4)	2	3	4	2	2	
Rischio da abbattere IxP (1-16)						
Rischio residuo (*post misure*)	6	9	16	6	8	

Misure di sicurezza dei dati e dei sistemi

- **Organizzative** (es. nomina del responsabile privacy, designazione di responsabili «secondari», nomina di incaricati, formazione, emanazione di line guida, istruzioni, ecc.)
- **Fisiche** (es. controllo di locali di custodia di archivi cartacei e pc/server)
- **Logiche** (es. autenticazione utenti, sistema di autorizzazione, firewall, antivirus, cifratira dei dati, ecc.)

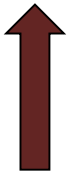
Potenziali criticità di sicurezza

• **Comportamenti degli operatori** (es. condotte errate, violazioni intenzionali di istruzioni, ecc.)

• **Ambiente fisico o tecnico** (es. errori o mancato aggiornamento del software, vulnerabilità della rete,

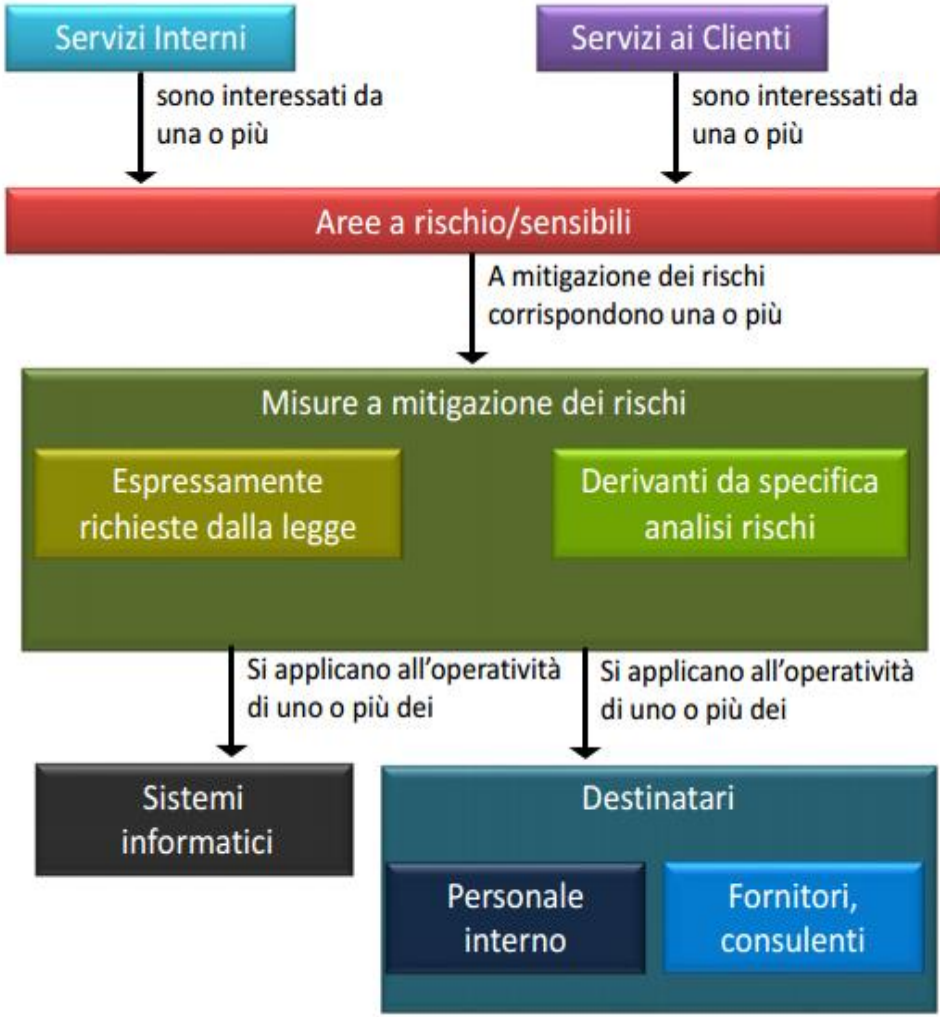
• **Disfunzioni organizzative** (es. logistica inadatta, carenze di direttive o di controlli)

134	Mantenere privacy policy	MISURA AGGIUNTIVA	0	N/A	N/A
135	Mantenere privacy policy	Verificare i casi di (eventuale) obbligo di Notifica dei trattamenti al Garante. Esecuzione della notifica online al Garante privacy sui trattamenti di profilazione degli utenti in internet; verifica annuale degli sviluppi organizzativi per verificare l'insorgere di nuove fattispecie che impongano l'estensione della notifica suddetta ad altri trattamenti	NB: Obbligo abrogato dal 24.05.2018	MM	No
136	Mantenere privacy policy	Verificare se la Società svolge trattamenti che comportino l'obbligo di richiedere al Garante una verifica preliminare (Consultazione Preventiva obbligatoria)	36	MM	Rev.
137	Mantenere privacy policy	Verifica dell'eventuale esistenza di codici di condotta ai sensi dell'art. 38 Reg. UE 679/2016, cui la Società possa aderire	40	N/A	N/A
138	Mantenere privacy policy	Verificare la liceità delle procedure di trattamento di dati penali (giudiziari)	24, 25, 32, 30.1g	ID2	No
139	Integrare la Privacy nei processi operativi	CARTACEO - Impartire istruzioni scritte per il controllo e custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, di atti e documenti contenenti dati sensibili o giudiziari da parte degli incaricati, per evitare accessi di persone non autorizzate, e restituzione dei medesimi al termine delle operazioni affidate	5.1f, 24.1-2, 25 All. B - 27 (penale)	MM	Rev.
140	Integrare la Privacy nei processi operativi	CARTACEO - Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione	5.1f, 24.1-2, 25 All. B - 27 (penale)	MM	Rev.
141	Integrare la Privacy nei processi operativi	CARTACEO - Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate	5.1f, 24.1-2, 25 All. B - 28 (penale)	MM	Si



Incrociando le misure di sicurezza / attività di gestione privacy-IT esistenti (classificate ad hoc) con le categorie di rischio individuate, si determina e valuta il rischio residuo, punto di partenza per ogni successiva azione organizzativa.

MODELLO PRIVACY BASATO SUL «RISK APPROACH»



Reati, sanzioni amministrative e responsabilità civile privacy

Differenze tra una «P.I.A.» e una «B.I.A.»

«P.I.A.» = Privacy Impact Analysis

- **E' un obbligo legale** in presenza di determinati presupposti di fatto
- **Valuta il livello di conformità tecnico-organizzativa** aziendale rispetto alla normativa privacy
- La valutazione dell'impatto economico delle eventuali non conformità rilevate è un elemento non obbligatorio per legge ma utile

«B.I.A.» = Business Impact Analysis

- **Non è un obbligo legale** ma una best practice
- **Valuta l'impatto economico** di eventuali non conformità organizzative. Comprende la privacy e la trascende
- Richiede sempre una stima finanziaria

NUOVO REGOLAMENTO UE 2016

OBBLIGO DI ANALISI DEI RISCHI

La PMI spesso incontra un'oggettiva difficoltà nell'identificare in autonomia le **pratiche «QUICK-WIN»** cioè che ***con modalità lean garantiscono un upgrade rilevante*** in termini di compliance IT-privacy.

Vi è il concreto rischio di **errata stima dei costi di messa in sicurezza**. Ma sottostimare l'esigenza di incrementare la compliance-sicurezza, causa rischi enormi.

E' in realtà possibile **individuare pratiche «a priorità alta»** = insieme di azioni di gestione che consentono di innalzare il livello di sicurezza/compliance aziendale ad un valore accettabile (=«idoneo»).

Processi/aree funzionali aziendali maggiormente coinvolti nella prassi

- DIREZIONE (+Segreteria di Direzione)
- PERSONALE (HR)
- COMMERCIALE/MARKETING (italia-estero)
- LEGALE
- AMMINISTRAZIONE
- IT
- SAFETY/SECURITY (RSPP, VIDEOSORVEGLIANZA)

- ACQUISTI
- LOGISTICA
- + Gestione Rapporti infragruppo (nazionali / internazionali)

LA MAPPATURA DEI TRATTAMENTI

L’analisi dei rischi privacy-IT richiede anche la **Mappatura (o inventario/elenco) dei trattamenti** di dati personali operati dal titolare:

- Categorie di **database** (archivi dati e tipologie di dati), sw e hw, servizi
- Categorie di **interessati**
- **Modalità** di trattamento
  - informatiche
  - cartacee
- **Finalità** di trattamento
- Ambiti di **comunicazione** e diffusione
- Profili di autorizzazione degli incaricati
- **Termini ultimi di cancellazione**
- Ecc..

La **mappatura (e classificazione) dei trattamenti** è il «**file rouge**» che consente al titolare l'adempimento di ulteriori obblighi:

- l'individuazione, adozione ed aggiornamento nel tempo delle **misure di sicurezza «adeguate».**

- Riscontro alle **richieste di esercizio dei diritti** dell'interessato (accesso, rettifica, portabilità, cancellazione e oblio, opposizione, deciisoni automatizzate e profilazione, ecc.)

- Costruzione di **idonee Informative privacy** verso gli aventi diritto

- Gestione della **governance privacy-IT interna ed esterna** (gestione della contrattualistica/modulistica verso co-titolari, responsabili del trattamento, incaricati, data privacy officer, ads, fornitori, ecc)

- Gestione degli obblighi relativi ai **trasferimenti di dati all'estero** (UE, Extra-UE) (binding Corporate Rules, data transfer agreeements, ecc)

Focus: gli **obblighi relativi ai trasferimenti di dati all'estero** (UE, Extra-UE

Principio generale per il trasferimento (art. 44)

Qualunque trasferimento di dati personali oggetto di trattamento (o destinati a essere trattati dopo un trasferimento verso l'estro) è possibile solo se il titolare e il responsabile del trattamento rispettano le condizioni previste dal Regolamento UE:

- Esistenza di una **decisione di adeguatezza della Commissione UE** (garanzia di un livello di protezione adeguata) (NB: con controllo su base continuativa degli sviluppi nel Paese estero e possibile revoca o sospensione della decisione) (art. 45)

- Art. 46: In mancanza di una tale decisione: esistenza di **garanzie adeguate (anche senza un'autorizzazione specifica da parte di una Autorità di controllo**), es. binding corporate rules (norme vincolanti d'impresa), clausole standard di protezione, codici di condotta ex art. 40 o meccanismi di certificazione + impegno vincolante del titolare o del responsabile ad applicare adeguate garanzie

Focus: gli **obblighi relativi ai trasferimenti di dati all'estero** (UE, Extra-UE

- Art. 47: In presenza di una necessaria **autorizzazione specifica da parte di una Autorità di controllo: binding corporate rules** (norme vincolanti d'impresa), che siano

  a) giuridicamente vincolanti per l'impresa e e applicabili a tutte le società del gruppo d'impresa che svolgono un'attività economica comune, compresi i dipendenti

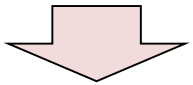
  b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento, e

  c) soddisfino i requisiti di cui al comma 2 dell'art. 47 (esplicitando, tra l'altro: mappatura dei dati, applicazione dei principi generali di trattamento, diritti degli interessati, ecc)

- **Consenso** dell'interessato

IL MODELLO ORGANIZZATIVO PRIVACY-IT «ADEGUATO»

La gestione dei rischi di «(in)adeguatezza» delle misure di sicurezza e di compliance, per legge va commisurata anche ai «costi di adeguamento» (se una misura non è particolarmente costosa, significa che tendenzialmente dovrebbe essere adottata) e allo «stato dell'arte» e/o al «progresso tecnico»



Il legislatore impiegando espressioni come «stato dell'arte» e progresso tecnico», rinvia ad «altri» la determinazione concreta del «quanta» sicurezza applicare ad un sistema di trattamento dei dati personali e del «come» implementarla.

L'APPROCCIO DI RISK MANAGEMENT DELL'IMPRESA IN AREA «PRIVACY-IT» PUO' ASSUMERE VARIE FORME ORGANIZZATIVE:

a) Modello Certificato (es. ISO 27001, ISO 27018, ITIL, ecc.)
b) Modello Organizzativo Privacy-IT (MOP) ex D. Lgs. 196/2003
c) Modello Organizzativo 231 su reati informatici
d) Modelli misti (MOP + ……) non certificati
e) Modello di gestione informale (nulle o scarse policies)

In base alle circostanze concrete **anche modelli non certificati (salvo il caso "e") possono reputarsi "adeguati".**
Tuttavia, tale giudizio di adeguatezza consegue solo ad una attenta considerazione della **qualità** dei contenuti e delle **concrete modalità di implementazione** di ciascun modello, a partire dal suo ambito di effettiva estensione ed efficacia.

Information Security & Privacy Security Standards: esempi

- **ISO 27001 –** Information Security Management System
- **NIST 800-52 –** Security and Privacy Controls
- **UK Cyber Essential Scheme –** UK-GOV
- **SAN Top 20 –** Critical Security Control
- **COBIT 5 (ISACA) –** Control Obiectives for Information […]
- **CISA – CCM –** Cloud Control Matrix
- **PCI – DSS –** Payment Card Industry Data Security Standard
- **FRAMEWORK NAZIONALE PER LA CYBER SECURITY 2015 –** CYBER INTELLIGENCE AND INFORMATION SECURITY CENTER – UNIVERSITA' SAPIENZA DI ROMA – CINI CYBER SECURITY NATIONAL LAB
- ECC…

PROCEDURE/PROTOCOLLI/MISURE IT-PRIVACY: CHECK-LIST SU CRITICITA' PIU' FREQUENTI

ASSETTO DEI PRESIDII PRIVACY-IT

***GESTIONE A "SILOS"*:**

DEI PRESIDII E CONTROLLI PRIVACY DELLE AREE

IT, PRIVACY

SISTEMA GESTIONE QUALITA',

PROTEZIONE DELLE INFORMAZIONI RISERVATE,

231

(rischio duplicazioni, omissioni, spreco risorse, ecc.)

- OMESSA MAPPATURA INTEGRATA DEI PRESIDII (FRAMMEMTAZIONE)
- OMESSA ANALISI DEI RISCHI O UTILIZZO DI ANALISI DEI RISCHI PRIVACY/IT SCARSAMENTE SIGNIFICATIVE (MODELLI "INCOMPLETI")
- OMESSA/INCOMPLETA FORMALIZZAZIONE DI PRESIDII E CONTROLLI (POLICIES)
- MANCATI FLUSSI INFORMATIVI ORGANO AMMINISTRATIVO / ORGANO DI CONTROLLO (COLLEGIO SINDACALE, ODV) – IT MANAGER - AMMINISTRATORI DI SISTEMA

- SCARSA CONSAPEVOLEZZA DEI RISCHI PRIVACY DA PARTE DEL MANAGEMENT (focalizzazione sui soli aspetti tecnici IT e/o commerciali)
- CARENZA DI FORMAZIONE LEGALE DEGLI ADS, DEI RESPONSABILI INTERNI E DEGLI INCARICATI (SCARSA CONSAPEVOLEZZA DELLE IMPLICAZIONI NORMATIVE)
- INSUFFICIENTE BUDGET SU PRIVACY-SICUREZZA (VISTA SOLO COME COSTO ANZICHE' OPPORTUNITA')
- USO DI TOOLS INADEGUATI DI TERZI FORNITORI

Adacta Tax & Legal

LA GOVERNANCE PRIVACY-IT «ADEGUATA»

Per «GOVERNANCE PRIVACY-IT» intendiamo qui l'adeguata **pianificazione, attuazione e gestione dell'assetto dei poteri** attribuiti dal management aziendale ai soggetti interni ed esterni, in tali materie.

La «GOVERNANCE PRIVACY-IT» è quindi una delle tre macro-componenti principali che consentono di strutturare un «adeguato assetto organizzativo» (le altre due sono l'infrastruttura IT e l'organizzazione dei processi operativi in area privacy-IT).

Art. 31 co. 4 Reg. Ue 679/2016

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

Ne consegue che la corretta formalizzazione della governance privacy-IT assume un'importanza centrale.

COSTRUIRE L'ADEGUATA GOVERNANCE PRIVACY-IT

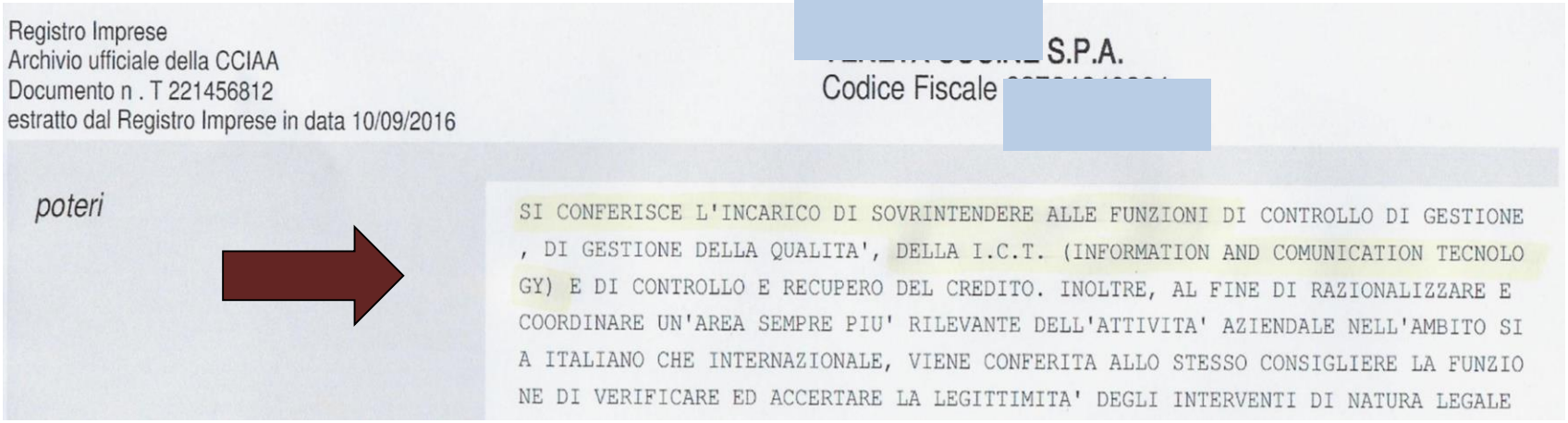
Nuovo approccio alle job description dei ruoli aziendali coinvolti ai diversi livelli (apicali e subordinati) dei processi e delle procedure privacy-IT, e al loro coordinamento

Necessità di più assidue forme di collaborazione tra funzioni aziendali per perseguire l'obiettivo di organigramma privacy conforme

Impostazione del modello organizzativo nei riguardi di terze parti, appartenenti al gruppo societario o ad esso estranee (es. outsourcers IT, responsabili esterni del trattamento dei dati personali)

Sistema di vigilanza sul Sistema/Modello strutturale IT-privacy: DPO – Data Protection Officer o altra figura da nominare ad hoc

Adacta Tax & Legal



Registro Imprese
Archivio ufficiale della CCIAA
Documento n . T 221456812
estratto dal Registro Imprese in data 10/09/2016

[redacted] S.P.A.
Codice Fiscale [redacted]

poteri

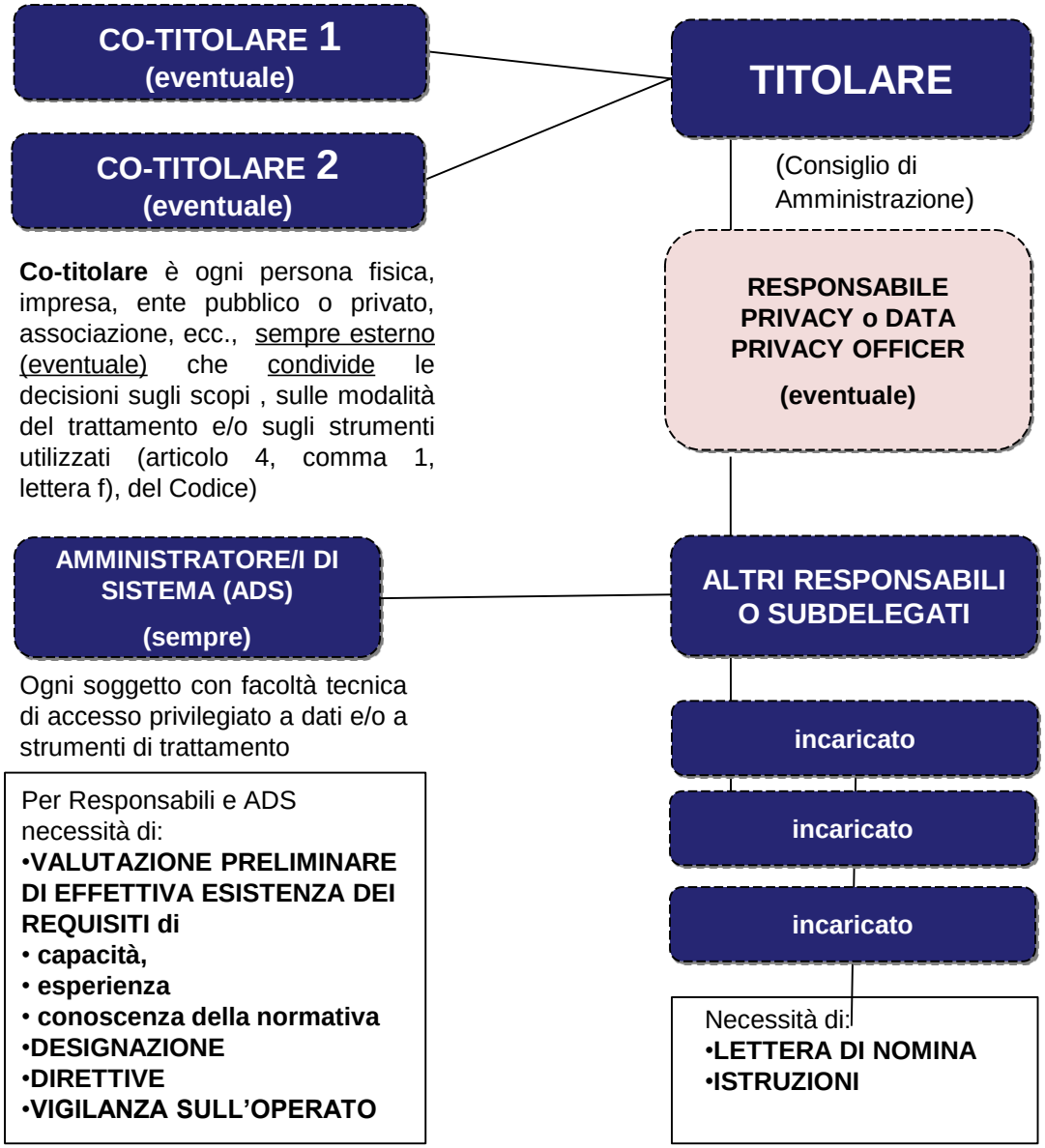
SI CONFERISCE L'INCARICO DI SOVRINTENDERE ALLE FUNZIONI DI CONTROLLO DI GESTIONE , DI GESTIONE DELLA QUALITA', DELLA I.C.T. (INFORMATION AND COMUNICATION TECNOLO GY) E DI CONTROLLO E RECUPERO DEL CREDITO. INOLTRE, AL FINE DI RAZIONALIZZARE E COORDINARE UN'AREA SEMPRE PIU' RILEVANTE DELL'ATTIVITA' AZIENDALE NELL'AMBITO SI A ITALIANO CHE INTERNAZIONALE, VIENE CONFERITA ALLO STESSO CONSIGLIERE LA FUNZIO NE DI VERIFICARE ED ACCERTARE LA LEGITTIMITA' DEGLI INTERVENTI DI NATURA LEGALE

Es. spesso le **deleghe apicali aziendali privacy-IT** risultano inadeguate/Inefficaci, perché non assicurano la chiara definizione delle macro-attività concretamente delegate che definiscono altresì il perimetro in relazione al quale il delegante (es. cda) deve continuare a vigilare e il soggetto vigilato deve garantire il reporting periodico al delegante.

Tale deficienza originaria rischia di riverberarsi su tutte le deleghe dipendenti.

«Adeguatezza» significa verificare il testo di tutte le deleghe, nomine, ecc. apicali e non, per **conformarne i contenuti** al principio di adeguatezza.

ELEMENTI PER LA COMPRENSIONE DELL'ORGANIGRAMMA PRIVACY



Co-titolare è ogni persona fisica, impresa, ente pubblico o privato, associazione, ecc., sempre esterno (eventuale) che condivide le decisioni sugli scopi , sulle modalità del trattamento e/o sugli strumenti utilizzati (articolo 4, comma 1, lettera f), del Codice)

Ogni soggetto con facoltà tecnica di accesso privilegiato a dati e/o a strumenti di trattamento

Per Responsabili e ADS necessità di:
•VALUTAZIONE PRELIMINARE DI EFFETTIVA ESISTENZA DEI REQUISITI di
• capacità,
• esperienza
• conoscenza della normativa
•DESIGNAZIONE
•DIRETTIVE
•VIGILANZA SULL'OPERATO

Titolare è la persona fisica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., cui spettano le decisioni sugli scopi e sulle modalità del trattamento, oltre che sugli strumenti utilizzati (articolo 4, comma 1, lettera f), del Codice)

Responsabile è la persona fisica, la società, l'ente pubblico o privato, l'associazione o l'organismo cui il titolare affida, anche all'esterno della sua organizzazione, specifici e definiti compiti di gestione e controllo del trattamento dei dati (articolo 4, comma 1, lettera g), del Codice). La designazione del responsabile è facoltativa (articolo 29 del Codice)

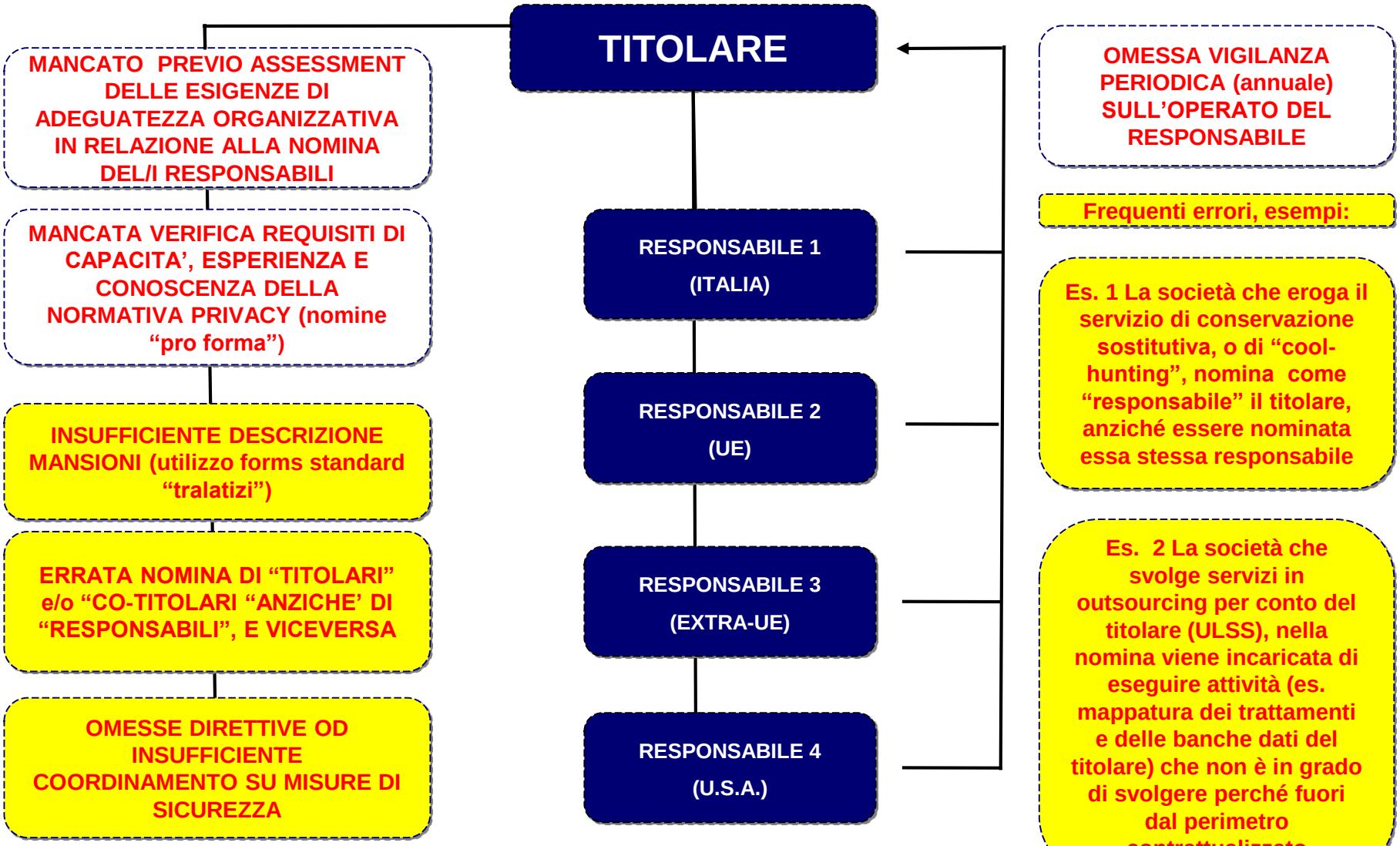
Il Responsabile principale può **delegare lo svolgimento di alcune attività** (esempio vigilanza su determinate aree funzionali) **ad ulteriori soggetti** (interni e/o esterni)

Incaricato è ogni persona fisica che, per conto del titolare, elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare e/o dal responsabile (articolo 4, comma 1, lettera h), del Codice)

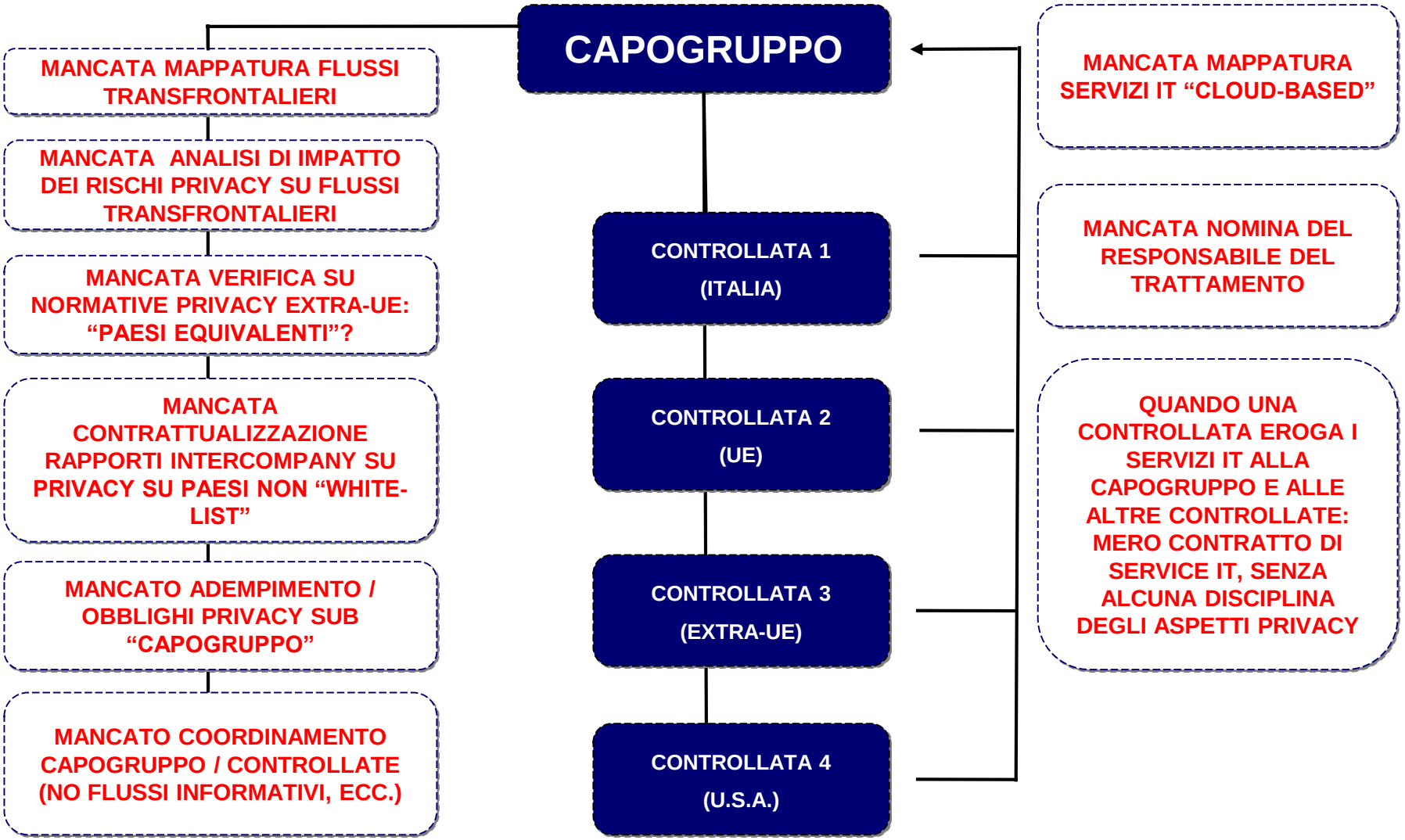
GOVERNANCE PRIVACY-IT: CHECK-LIST SU ALCUNE CRICITA' PIU' FREQUENTI

- MANCATA MAPPATURA DELEGHE IT-PRIVACY
- INADEGUATA DEFINIZIONE DELL' ORGANIGRAMMA PRIVACY-IT
- INADEGUATA / INFORMALE VALUTAZIONE DEI REQUISITI CAPACITIVI DEI RESPONSABILI DEL TRATTAMENTO NOMINATI
- INSUFFICIENTE PERCEZIONE DEL REALE PERIMETRO DEGLI OBBLIGHI LEGALI DI GOVERNANCE
- GESTIONE NON COORDINATA TRA GOVERNANCE PRIVACY E GOVERNANCE IT (SILOS, SOVRAPPOSIZIONI, ECC.)
- INADEGUATA DESCRIZIONE DELLE MACRO-ATTIVITA' OGGETTO DI EVENTUALI DELEGHE
- FORMALIZZAZIONE CARENTE (PRASSI NON DOCUMENTATE) SPECIE VERSO GLI OUTSOURCERS
- CARENTE VIGILANZA CONCRETA SUI DELEGATI (CLAUSOLE DI STILE)

RESPONSABILE DEL TRATTAMENTO: CHECK-LIST SU CRITICITA' PIU' FREQUENTI

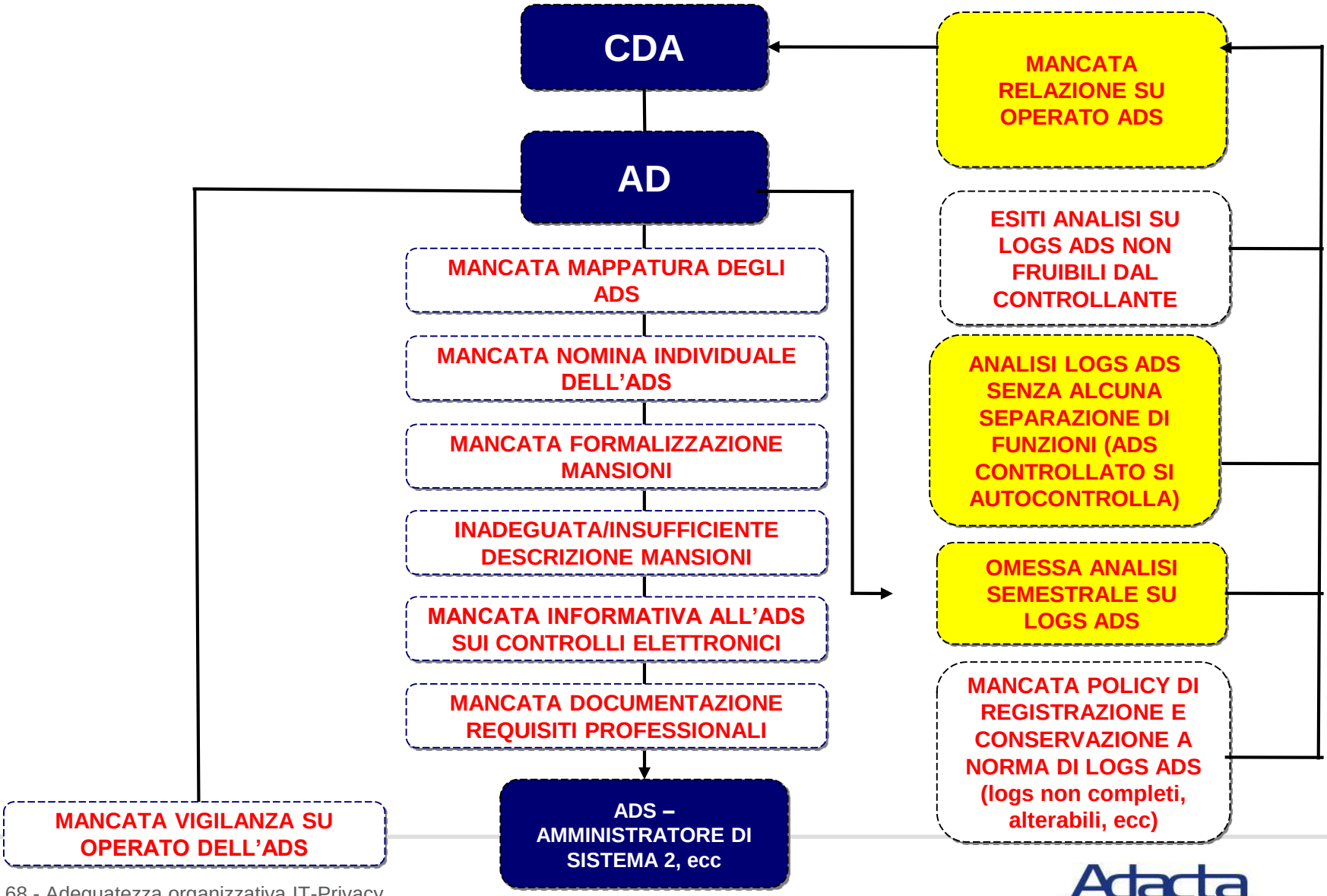


PRIVACY NEI GRUPPI SOCIETARI: CHECK-LIST SU CRITICITA' PIU' FREQUENTI



Adacta Tax & Legal

AMMINISTRATORI DI SISTEMA: CHECK-LIST SU VIOLAZIONI DI LEGGE PIU' FREQUENTI



Adacta Tax & Legal

LA GOVERNANCE DEL TRATTAMENTO DATI IN OUTSOURCING

TRATTAMENTO IN SUB-OUTSOURCING: QUALI OBBLIGHI?

NB:

Il Responsabile esterno (che agisce sotto l'autorità del titolare del trattamento) che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso del titolare del trattamento (salvo che lo richieda il diritto della UE o degli Stati membri)

Diventa quindi punibile anche l'eventuale inerzia del Responsabile esterno che non si cura di sollecitare al titolare del trattamento istruzioni circa il perimetro del trattamento autorizzato…

TRATTAMENTO IN SUB-OUTSOURCING: QUALI OBBLIGHI?

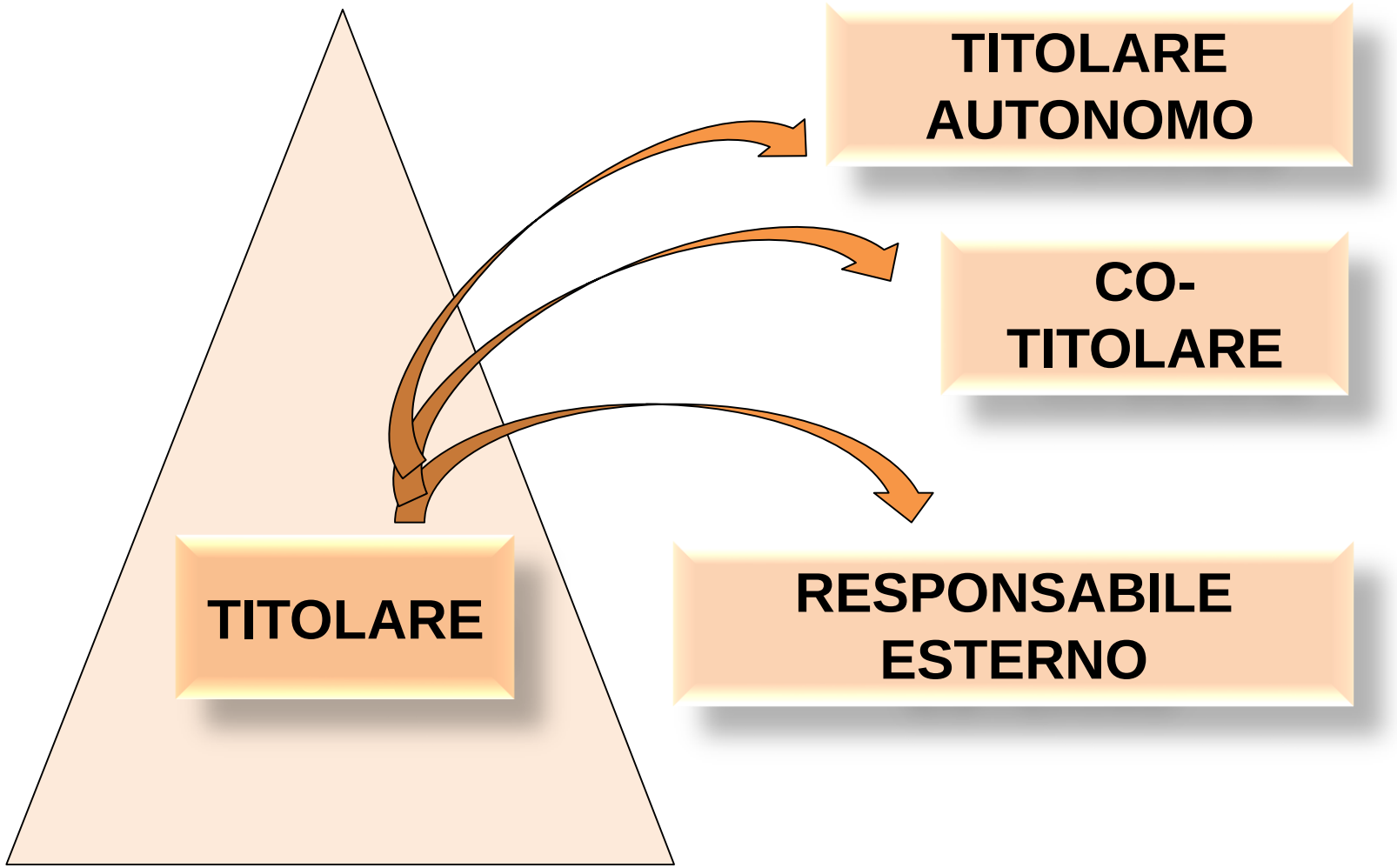
NB:

Se il Responsabile esterno viola uno qualsiasi degli obblighi previsti a suo carico del nuovo art. 28 GPDR, è automaticamente considerato quale titolare del trattamento in questione.

Sono fatte salve le sanzioni previste dagli artt. 82-8-3-84 GPDR.

Occorre quindi che il Responsabile esterno «cambi pelle» e si strutturi adeguatamente per gestire in modo idoneo i nuovi rischi.

Gerarchie esterne privacy (tre ipotesi possibili)



TRATTAMENTO IN OUTSOURCING: QUALE VESTE PRIVACY DEL TERZO?

Il Titolare che affida il trattamento di dati personali a un terzo deve **decidere quale specifica veste privacy** attribuirgli («responsabile esterno» o «co-titolare» o «titolare autonomo».)

La scelta dipende dalla **valutazione di un insieme di fattori**. Tanto più è ampio il livello dell'**autonomia organizzativa effettiva** concessa al terzo riguardo le finalità (ulteriori?) del trattamento, le misure di sicurezza da adottare e/ i relativi controlli in relazione ad esso, tanto più sarà possibile una «titolarità».

Il Titolare ha **l'obbligo di stipula di un accordo interno** per:

- Specificare i compiti dell'outsourcer, tramite l'atto di designazione (determinazione delle reciproche responsabilità circa l'adempimento degli obblighi legali)
- Fornire istruzioni sui trattamenti
- Chiarire gli obblighi relativi alle misure di sicurezza e regolare reciprocamente le altre condizioni privacy del rapporto (durata dei trattamenti, finalità, categorie di dati e di interessati, ambiti di comunicazione e diffusione autorizzati, restituzione dei dati, data breach, facoltà di audit, accountability)

TRATTAMENTO IN SUB-OUTSOURCING: QUALI OBBLIGHI?

Il REGOLAMENTO UE PRIVACY 679/2016 conferma o rafforza gli obblighi a carico dei soggetti coinvolti nei trattamenti in outsourcing:

- Obbligo del responsabile esterno di **comunicare preventivamente al titolare i nominativi di eventuali sub-appaltatori** del trattamento
- Facoltà del titolare di **autorizzare il ricorso ai sub-appaltatori** del trattamento da parte del responsabile esterno principale
- Necessità di previa **autorizzazione (specifica o generale) scritta** al sub-appalto del trattamento dati
- Obbligo di comunicazione dei nominativi dei sub-appaltatori (incluse aggiunte/sostituzioni)
- Obbligo del titolare di impegnare il responsabile esterno al **rispetto delle misure di sicurezza** non inferiori rispetto a quelle adottate dallo stesso, e del responsabile di riversare gli **stessi obblighi di protezione** sui sub-appaltatori
- Obbligo di **vigilanza** sull'operato del responsabile esterno da parte del titolare

NB: I contenuti delle nomine devono essere adeguati al tenore del nuovo art. 28 Reg. UE.

TRATTAMENTO IN SUB-OUTSOURCING: QUALI OBBLIGHI?

Il REGOLAMENTO UE PRIVACY 679/2016 conferma o rafforza gli obblighi a carico dei soggetti coinvolti nei trattamenti in outsourcing:

Il Responsabile esterno dovrà, tra l'altro (art. 28):

- mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di legge specifici
- consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare e dai suoi delegati
- collaborare all'evasione delle richieste di esercizio dei diritti dell'interessato
- rispondere di eventuali violazioni privacy del sub-appaltatore

TRATTAMENTO IN OUTSOURCING

E’ essenziale per l’adeguatezza organizzativa operare la preliminare mappatura riclassificata di tutti i fornitori e partners che trattano «dati personali», per individuare tutti li outsourcers rilevanti (Reg. Ue 679/2016) (es. housing, hosting, gestore paghe, consulenti vari, sindaci, ecc.). Vanno inclusi anche i sub-fornitori dell’outsourcers.

Per legge prevale la situazione di fatto, sostanziale, rispetto al mero dato formale (impostazione analoga a quella «giuslavoristica» vigente in materia di deleghe)

Infatti non basta attribuire al terzo outsourcer una *qualunque* veste : gli **va attribuita la veste corrispondente** non solo al reale tipo di attività delegatagli dal titolare, quindi alle **modalità con le quale il terzo si organizza rispetto al trattamento dei dati affidatogli**

Attribuendo una veste errata all’outsourcer, si rischia di violare gli specifici obblighi che la normativa ricollega al rapporto sostanziale tra le parti.

LA FIGURA DEL NUOVO «DATA PRIVACY OFFICER» (DPO)

DATA PRIVACY OFFICER

NOMINA OBBLIGATORIA IN ALCUNI CASI DETERMINATI:

P.A. (SALVO AUTORITA' GIUDIZIARIE)

I SOGGETTI LA CUI **ATTIVITA' PRINCIPALE** CONSISTE IN TRATTAMENTI CHE – PER LA LORO NATURA, IL LORO OGGETTO E/O LE LORO FINALITA' – RICHIEDONO IL **CONTROLLO REGOLARE E SISTEMATICO** DEGLI INTERESSATI **SU LARGA SCALA**

I SOGGETTI LA CUI ATTIVITA'' PRINCIPALE CONSISTE NEL **TRATTAMENTO SU LARGA SCALA, DI CATEGORIE PARTICOLARI DI DATI EX ART. 9 (DATI SENSIBILI, SANITARI O RELATIVI ALLA VITA SESSUALE, GENETICI, BIOMETRICI, O GIUDIZIARI)** (es. sanità, sorveglianza, elaborazione buste paga, marketing con determinate profilazione degli interessati)

NEGLI ALTRI CASI:

NOMINA FACOLTATIVA

NB: IL PRINCIPIO DI ADEGUATEZZA ORGANIZZATICA puo' rendere di fatto opportuna la nomina del DPO, o comunque di una diversa figura che ne mutui almeno alcuni dei compiti

NB. E' POSSIBILE LA NOMINA DI UN UNICO DATA PRIVACY OFFICER DA PARTE DI UN GRUPPO DI IMPRESE O DI SOGGETTI PUBBLICI,

PURCHE' IL DPO SIA FACILMENTE RAGGIUNGIBILE DA CIASCUN STABILIMENTO

NB. IL DPO NON ELIMINA LA VECCHIA FIGURA DEL «RESPONSABILE DEL TRATTAMENTO» , CHE TRATTA I DATI «PER CONTO» DEL TITOLARE

- **«Attività principale o primaria» del titolare» cosa significa?**

- Da valutare in base allo statuto/oggetto sociale (visura CCIAA) e su base fattuale (cosa in concreto fa la società)

- Rileva solo l'attività di fornitura di beni e servizi che **caratterizza prevalentemente** il titolare, non il mero fatto che tale attività comporti – come prassi – lo scambio di flussi informativi tra il titolare (impresa/professionista) e i terzi (cliente/utente/consumatore): es. chi vende elettrodomestici ha come attività primaria il commercio dei medesimi anche se comunica con fornitori, clienti, PA, ecc.

- L'attività primaria deve inoltre:
  a) consistere nel monitoraggio **«su larga scala»** monitoraggio regolare e sistematico degli interessati (cui i dati personali si riferiscono) (art. 37 par. 1 lett b), o
  b) consistere nel trattamento **«su larga scala»** di determinate categorie di dati personali (espressamente indicate dagli artt. 9 e 10 Reg. UE) (art. 37 par. 1 lett. c)

- **Cosa si intende per «larga scala» del monitoraggio/trattamento?**

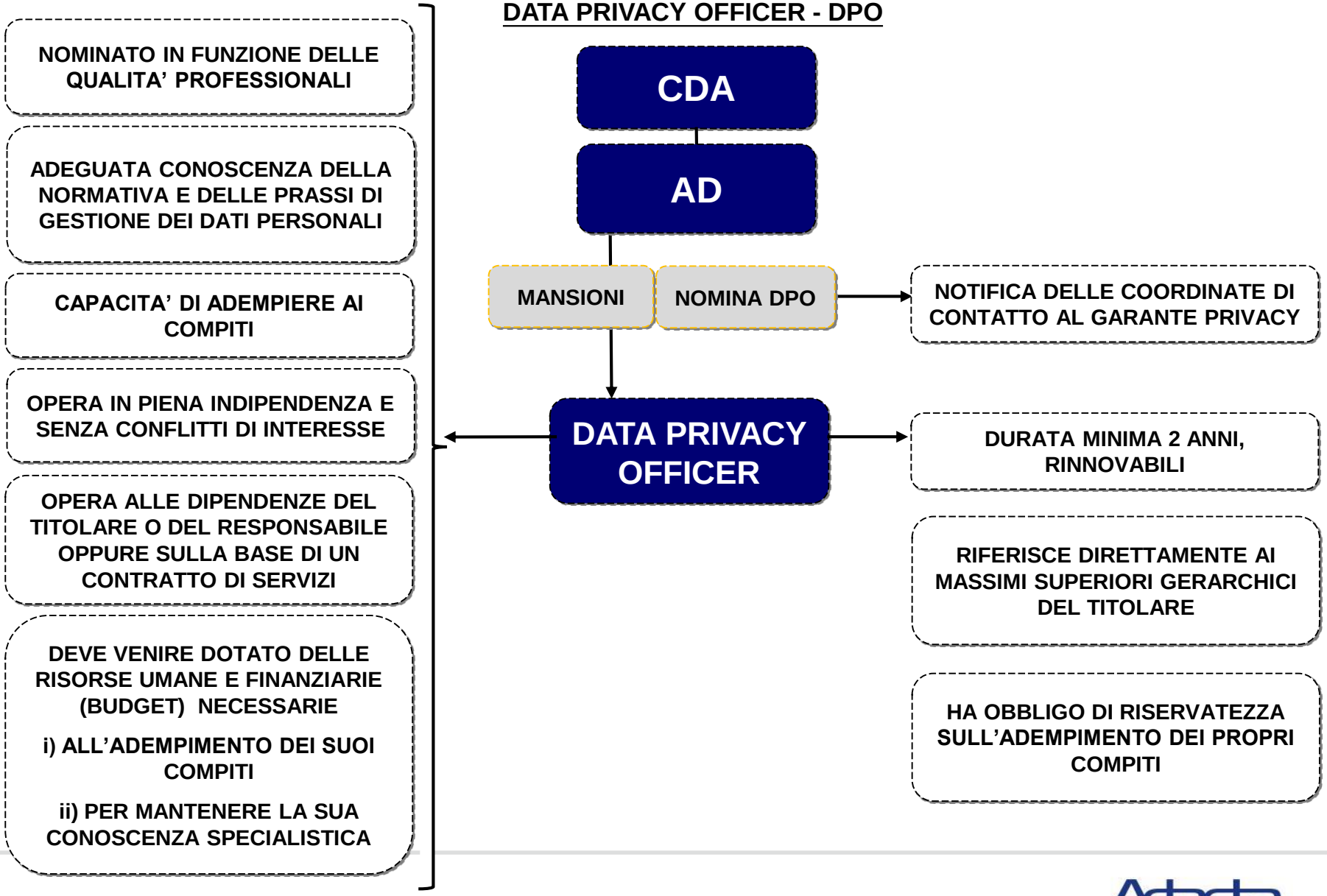
- Da valutare i) in base alla **natura**, all'ambito di **applicazione** e/o alle **finalità** dei trattamenti
- Da valutare ii) sulla base delle **Linee Guida 13.12.2106 dell'Article 29 Data Protection Working Party**, che
  ✓ menziona cinque criteri:
    - **numero degli interessati**
    - **quantità di dati** personali
    - **tipologia di dati** trattati
    - **tempo** determinato o indeterminato dell'attività di trattamento
    - **estensione geografica** del trattamento
  ✓ e propone alcune esemplificazioni estreme:
    - in positivo:
      - ospedale
      - azienda di trasporto
      - trattamento dati di geolocalizzazione
      - compagnie assicurative e istituti di credito
      - motori di ricerca
      - fornitori di servizi di telecomunicazioni
    - in negativo:
      - studio professionale medico o legale (dati pazienti/clienti)

- **Cosa si intende per «larga scala» del monitoraggio/trattamento?**

- Da valutare iii) sulla base del **Considerando 91** i trattamenti su larga scala «*mirano al trattamento di una **notevole quantità di dati** personali **a livello regionale, nazionale o sovranazionale** e che potrebbero incidere su un **vasto numero di interessati***»: quindi pare ragionevole una valutazione quantitativa
- Da valutare iv) sulla base del **Considerando 13** «*inoltre le istituzioni e gli organi dell'Unione e gli Stati membri e le loro autorità di controllo sono invitati a* **considerare esigenze specifiche delle micro, piccole e media imprese** *nell'applicare il presente regolamento* (…)»
- Da valutare altresì v) in base all'**art. 35 par. 4** «**l'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto** sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'art. 68»

→ tale elenco sarà utilizzabile anche ai fini dell'individuazione del concetto di «larga scala» ex art. 37 par. 2 lett. c) (allorchè esso rimanda alle «particolari categorie di dati» oggetto dei trattamenti

DATA PRIVACY OFFICER - DPO



DATA PRIVACY OFFICER: funzioni

INFORMA E CONSIGLIA CIRCA GLI OBBLIGHI DERIVANTI DAL REGOLAMENTO PRIVACY UE

O DA ALTRE NORME DEGLI STATI MEMBRI

ATTRIBUISCE LE RESPONSABILITA' AGLI ALTRI SOGGETTI INTERNI ALL'AZIENDA CHE TRATTANO DATI PERSONALI

VERIFICA L'ATTUAZIONE E APPLICAZIONE DEL REGOLAMENTO UE O DEGLI STATI MEMBRI SULLA PRIVACY, NONCHE' DELLE POLITICHE AZIENDALI IN MATERIA DI PRIVACY (INCLUSI: ATTRIBUZIONE DI RESPONSABILITA', FORMAZIONE DEL PERSONALE, AUDIT CONNESSI)

CONSERVA LA DOCUMENTAZIONE RELATIVA A TALI ATTIVITA' DI COMUNICAZIONE O CONSULENZA, NONCHE' LE RISPOSTE FORNITE DAI SOGGETTI

VERIFICA IL TRACCIAMENTO DELLE VIOLAZIONI DEI DATI PERSONALI E LA LORO COMUNICAZIONE AGLI INTERESSATI

VERIFICA LA PROTEZIONE DI DEFAULT DI DATI E SISTEMI E RILEVA CHE SIA GARANTITA LA SICUREZZA NEI TRATTAMENTI DEI DATI

FORNISCE PARERI SULLA VALUTAZIONE D'IMPATTO PRIVACY DELLE ATTIVITA' (SU RICHIESTA) E NE SORVEGLIA L'ATTUAZIONE

GARANTISCE LA CONSERVAZIONE DEI DOCUMENTI RELATIVI AI TRATTAMENTI

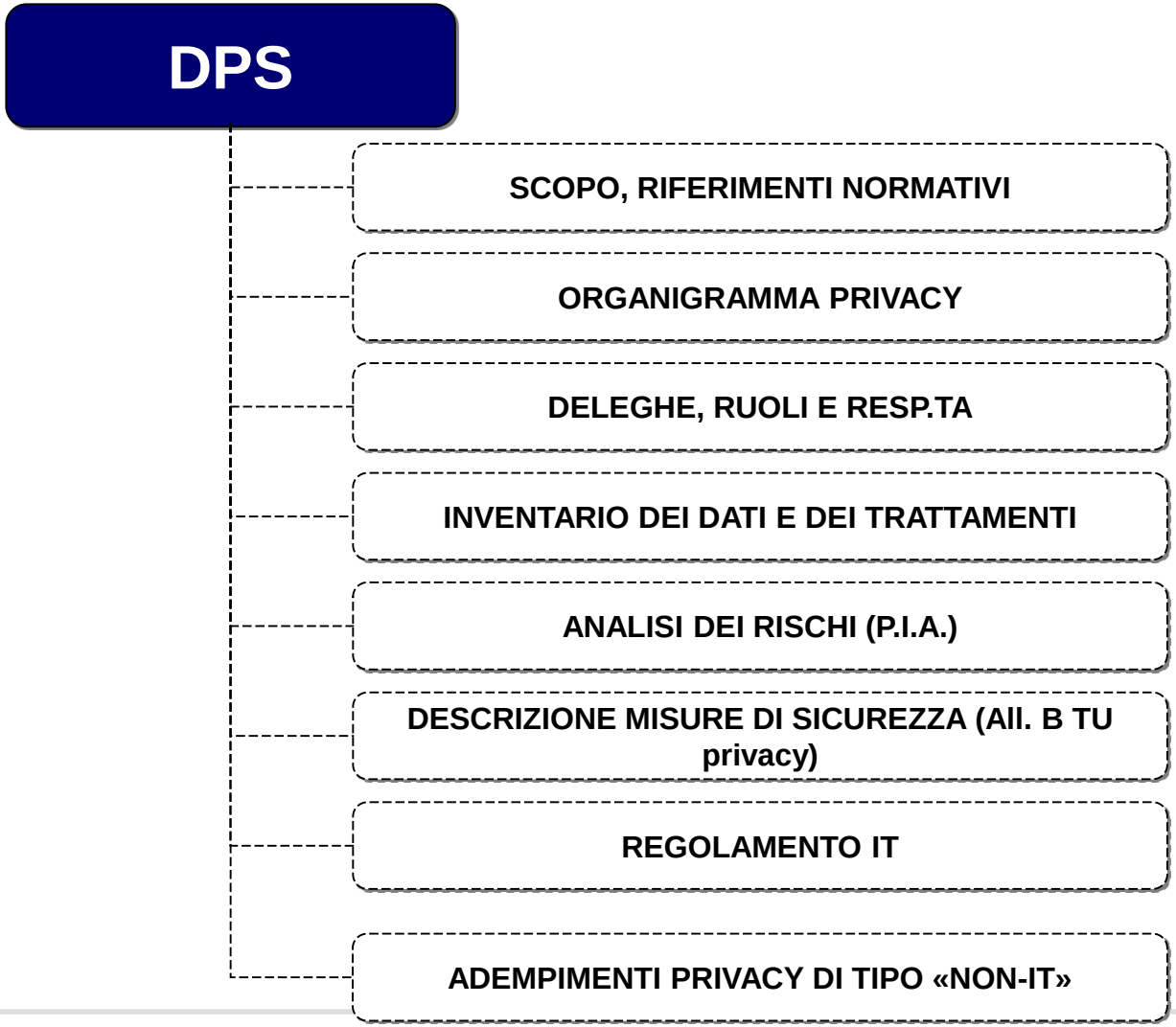
FUNGE DA PUNTO DI CONTATTO

i) PER GLI INTERESSATI IN RELAZIONE AD OGNI PROBLEMATICA CONNESSA AL TRATTAMENTO DATI O ALL'ESERCIZIO DEI DIRITTI

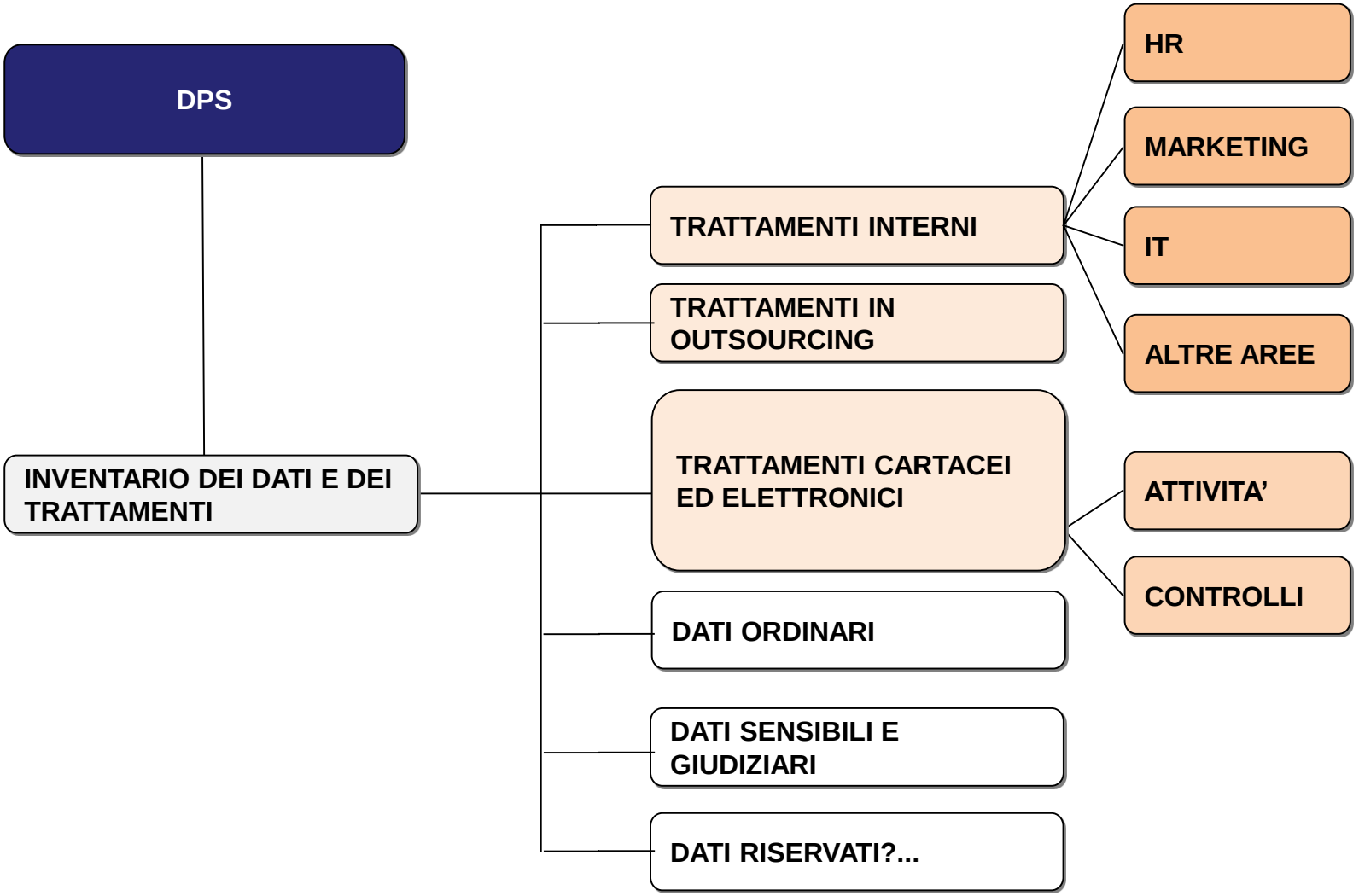
ii) CON IL GARANTE PRIVACY O DI PROPRIA INIZIATIVA LO CONSULTA

IL «NUOVO» DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS o DPIA) è il documento-guida a cui l'intera attività aziendale in materia di gestione privacy e/o sicurezza delle informazioni e IT si deve uniformare.



va complessivamente aggiornato con cadenza come minimo annuale



«Ma l'obbligo di DPS non è abrogato?..» NO!

- Nel 2012 (art. 45 D.L. 2012/5) l'obbligo - penalmente sanzionato ex art. 169 TU privacy - di adozione e aggiornamento del DPS formalmente è stato abrogato (art. 34 comma 1) in realtà la responsabilità civilistica del titolare è restata (e resterà) immutata in materia, in quanto non è mai venuto l'obbligo generale di adozione sia delle altre misure di sicurezza «minime» e soprattutto di misure di sicurezza comunque «idonee» e di aggiornamento periodico delle medesime (che presuppone un monitoraggio strutturato con idonei strumenti e cioè documenti scritti gestiti con continuità)

- **Il nuovo Regolamento UR privacy 2016/679** ribadendo l'obbligo di complessiva ***efficacia in concreto*** del «modello privacy» e di «accountability», **conferma l'ineludibilità di una adeguata documentazione** delle misure di sicurezza attuate e in genere **di tutto quanto attuato in adempimento della normativa privacy** per i trattamenti dei dati personali. Identico principio è imposto all'impresa dall'**art. 2381 co. 5 c.c.** e dal cd. **«stato dell'arte»** a cui, per espressa previsione di legge, già oggi occorre fare riferimento in tema di misure di sicurezza

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

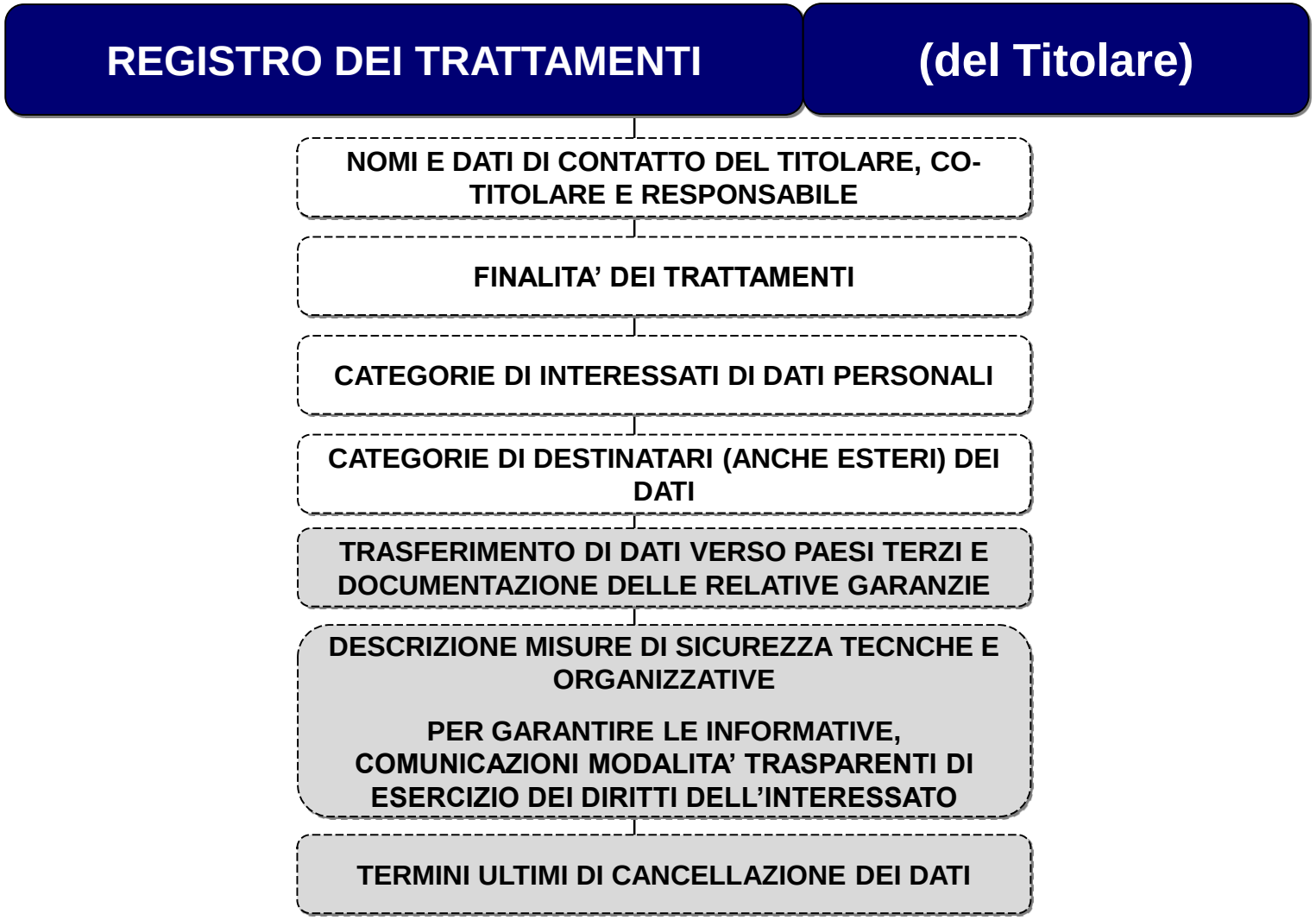
La ulteriore (ma non nuova) esigenza, in ottica di adeguatezza organizzativa, è inoltre quella di **decidere ed esplicitare gli scopi generali che il DPS/DPIA/Registro dei trattamenti intende soddisfare:**

a) il DPS va usato, solo a fini privacy, o anche per adempiere agli **obblighi adeguatezza organizzativa** di cui agli artt. 2381 co. 5 e 2403 codice civile?

b) Il DPS deve costituire lo strumento **non solo per la gestione degli aspetti informatici della privacy** (misure di sicurezza), **ma anche di ogni altro adempimento legale privacy** (es. videosorveglianza, informative, consensi, ecc.); evitando cosi rischi di dispersione delle informazioni (es. turnover del personale addetto all'aggiornamento) e di obsolescenza delle policy?

c) Il DPS è valorizzato in funzione della sola gestione a norma degli adempimenti privacy, o anche per un'adeguata gestione di tutte le principali categorie di **informazioni riservate** aziendali (dati non "personali", che però rivestono per l'azienda un valore economico e strategico, non sono destinate alla diffusione e non sono generalmente note, es. know-how)?

Il REGISTRO DEI TRATTAMENTI (RDT)) è il nuovo documento-guida minimo aziendale in area privacy. Tale nuovo REGISTRO solo per alcuni aspetti è simile al vecchio Documento Programmatico sulla Sicurezza



Il REGISTRO DEI TRATTAMENTI (RDT)) è il nuovo documento-guida minimo aziendale in area privacy.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (ART. 30 REGOLAMENTO UE)

Co. 5 Gli obblighi relativi al Registro dei trattamenti **non** si applicano alle **imprese o organizzazioni con meno di 250 dipendenti**, salvo che il trattamento effettuato:

- possa presentare un rischio per i diritti e le libertà dell'interessato;
- non sia occasionale;
- includa il trattamento di categorie particolari di dati (…);
- riguardi dati giudiziari (cioè relativi a condanne penali e reati)

Pertanto in moltissimi casi l'esenzione suddetta pare destinata a non trovare applicazione.

In ogni caso pare ben difficile, senza un Registro dei trattamenti, adempiere ad altri obblighi regolamentari (es. informative, nome degli incaricati, rapporti con gli outsourcers, ecc.)

La soluzione «adeguata» in ottica proattiva e' un DPS integrato con i contenuti del nuovo REGISTRO

DPS (INCLUDE REGISTRO DEI TRATTAMENTI)

- SCOPO, RIFERIMENTI NORMATIVI
- ORGANIGRAMMA PRIVACY
- DELEGHE, RUOLI E RESP.TA
- INVENTARIO DEI DATI E DEI TRATTAMENTI
- ANALISI DEI RISCHI (P.I.A.)
- DESCRIZIONE MISURE DI SICUREZZA (All. B TU privacy)
- REGOLAMENTO IT
- ADEMPIMENTI PRIVACY DI TIPO «NON-IT»

+

- NOMI E DATI DI CONTATTO DEL TITOLARE
- FINALITA' DEI TRATTAMENTI
- CATEGORIE DI INTERESSATI, DI DATI PERSONALI
- CATEGORIE DI DESTINATARI DEI DATI
- TRASFERIMENTO DI DATI VERSO PAESI TERZI E RELATIVE GARANZIE
- DESCRIZIONE MISURE DI SICUREZZA TECNCHE E ORGANIZZATIVE

  PER GARANTIRE LE INFORMATIVE, COMUNICAZIONI MODALITA' TRASPARENTI DI ESERCIZIO DEI DIRITTI DELL'INTERESSATO
- TERMINI ULTIMI DI CANCELLAZZIONE DEI DATI

Adacta Tax & Legal

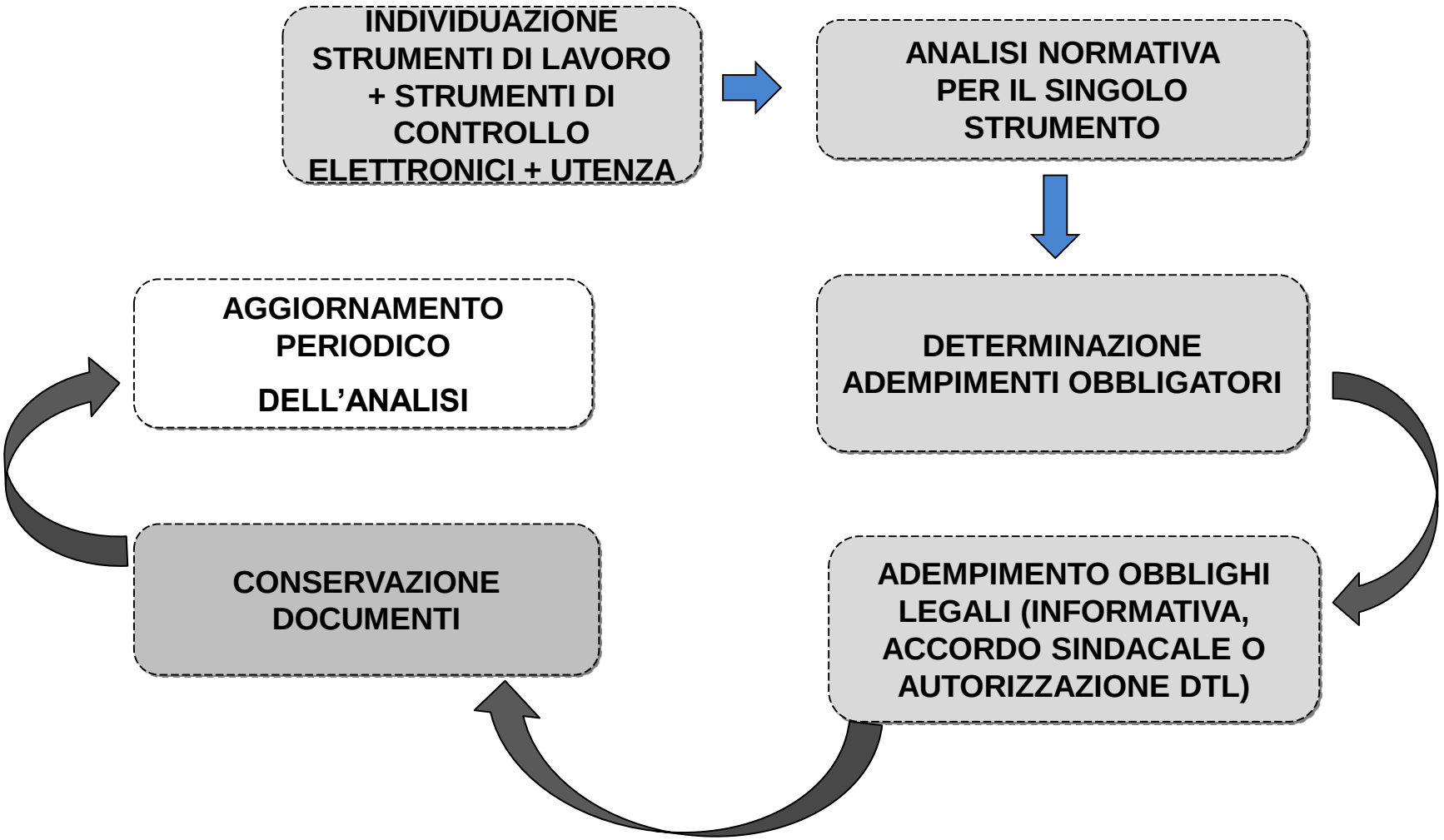
IL REGOLAMENTO IT AZIENDALE

REGOLAMENTO IT

- È un **obbligo** di legge e un **allegato** al DPS – Documento Programmatico sulla Sicurezza
- È uno dei più importanti presidi di gestione del rischio IT-privacy; si applica a tutti i **dipendenti** coinvolti nei processi ma anche ad eventuali **utenti** esterni
- È un documento tecnico+organizzativo+legale (utilizzabile **a fini disciplinari** previe formalità specifiche)
- Deve essere sempre un **tailor-made**
- Va **aggiornato** (minimo annualmente) per tenere conto dei nuovi trend tecnologici *(es. Device Mobili, Geolocalizzazione (es. black-box su veicoli), RFID, PEC, Firme Digitali, LOGS degli Amministratori di sistema, Social Media Policy, Videosorveglianza, Virtualizzazione, Cloud, VPN, SPID, IoT, Controlli elettronici e Computer Forensics, ecc.)* e delle best practices sopravvenute

- **Presuppone la previa formale mappatura integrale degli strumenti IT** di lavoro e degli strumenti di controllo elettronico presenti in azienda (v. oltre)

PROCESSO DI GESTIONE DEI CONTROLLI ELETTRONICI



Es. di MATRICE DEGLI STRUMENTI ELETTRONICI DI LAVORO E DI CONTROLLO ELETTRONICO

	Strumento di lavoro (usato dall'utente per rendere la prestazione) (art. 4 co. 2 L. 1970/300)	Fringe benfit (se previsto dal contratto con l'utente)	Controllo sistematico (continuativo, generalizzato, senza interruzioni, su base direttamente individuale)	Obbligo accordo sindacale o autorizzazione DPL (art. 4 co. 1 L. 1970/300)	Obbligo informativa all'utente (ex art. 4 commi 2-3 L. 1970/300 nonchè ex art. 13 D.Lgs. 196/2003)	Controllo usabile a ogni fine connesso al rapporto di lavoro (inclusi fini disciplinari) (art. 4 co. 3 L. 1970/300)
telefono fisso	SI	SI	NO (VIETATO)	NO (salvo per cespite fringe benefit)	SI	SI
cellulare/smartphone	SI	SI	NO (VIETATO)	NO (salvo per cespite fringe benefit)	SI	SI
tablet	SI	SI	NO (VIETATO)	NO (salvo per cespite fringe benefit)	SI	SI
internet key	SI	SI	NO (VIETATO)	NO (salvo per cespite fringe benefit)	SI	SI
SIM	SI	SI	NO (VIETATO)	NO (salvo per cespite fringe benefit)	SI	SI
badge (basato su RFID)	SI	NO	NO (VIETATO)	NO	SI	SI
carta di credito con microchip	SI	SI	NO (VIETATO)	NO	SI	SI
certificato e dispositivo di firma digitale	SI	NO	NO (VIETATO)	NO	SI	SI
posta elettronica (account), non certificata o certificata (PEC), *lato utente*	SI	NO	NO (VIETATO)	NO	SI	SI
internet (account), *lato utente*	SI	NO	NO (VIETATO)	NO	SI	SI
internet, *lato ADS*	NO	NO	NO (VIETATO)	NO	SI	SI
password, PIN, codici (sistema autenticazione/accesso)	SI	NO	NO (VIETATO)	NO	SI	SI
sistema di autorizzazione	SI	NO	NO (VIETATO)	NO	SI	SI
rete (lato utente)	SI	NO	NO (VIETATO)	NO	SI	SI
rete (lato ADS)	NO	NO	NO (VIETATO)	NO	SI	SI
software gestione delle registrazioni accessi (fisici)	NO	NO	NO (VIETATO)	NO	SI	SI
software gestione delle registrazioni accessi (elettronici), diversi dalla registrazione presenze	NO	NO	NO (VIETATO)	NO	SI	SI

Sicuri di avere compreso cosa si intende per «strumenti di controllo elettronico» soggetti agli obblighi normativi?

Rischio di interpretare erroneamente la normativa e di escludere strumenti inclusi negli obblighi di legge.

REGOLAMENTO IT AZIENDALE: CHECK LIST SU CRITICITA' PIU' FREQUENTI

REGOLAMENTO IT

NB: POLICY AZIENDALE OBBLIGATORIA, DA NON CONFONDERE CON IL REGOLAMENTO PRIVACY UE 2016!!!

MANCATO PREVIO ASSESSMENT DELLE ESIGENZE DI ADEGUATEZZA ORGANIZZATIVA

INADEGUATEZZA CONTENUTO:

- utilizzo forms standard datati e/o "tralatizi" (Confindustria)
- mancata personalizzazione in base al concreto contesto
- regole inserite nel DPS anziché nel Regolamento IT (inefficacia vs. i destinatari)
- spesso rivolto solo agli incaricati, non anche agli Amministratori di Sistema
- quindi: non usabile a fini disciplinari (Jobs Act)

MANCATA MAPPATURA/DISCIPLINA DEGLI STRUMENTI ELETTRONICI DI LAVORO E DI CONTROLLO DEI DIPENDENTI (Jobs Act)

MANCATO AGGIORNAMENTO

(es. non include nuove tecnologie come Device Mobili, USB, GPS, RFID, PEC. Firme Digitali, LOGS degli Amministratori di sistema, Social Media Policy, Videosorveglianza, ecc.)

Adacta Tax & Legal

I CONTROLLI ELETTRONICI SUI DIPENDENTI

JOBS ACT 2015 & PRIVACY

Libertà di controllo anche a distanza dei lavoratori, **per sole finalità previste dalla normativa**

- **TUTELA DEL PATRIMONIO AZIENDALE**
- **SICUREZZA DEL LAVORO**
- **ESIGENZE PRODUTTIVE**
- **ESIGENZE ORGANIZZATIVE**

OBBLIGO DI ADEGUATA INFORMATIVA AI DIPENDENTI

su:

MODALITA' DI FUNZIONAMENTO

DEGLI STRUMENTI ELETTRONICI DI LAVORO

MODALITA' DEI CONTROLLI ELETTRONICI

A) SUGLI STRUMENTI ELETTRONICI

B) SULL'ATTIVITA' (ANCHE NON ELETTRONICA) DEI LAVORATORI

JOBS ACT 2015 & PRIVACY

Libertà di controllo a distanza dei lavoratori, per le sole 4 finalità previste dalla normativa

Obbligo di ACCORDO SINDACALE o, in mancanza, AUTORIZZAZIONE D.T. DEL LAVORO

Esenti da formalita'

NON E' PREVISTO NEL CASO DI

«STRUMENTI DI LAVORO ELETTRONICI»

«STRUMENTI DI CONTROLLO ELETTRONICO A DISTANZA» DEI LAVORATORI

(SE DIVERSI DAI DISPOSITIVI DI MERA RILEVAZIONE PRESENZE)

Esempi:

- **VIDEOSORVEGLIANZA**
- **FIREWALL, PROXY SERVER, SOFTWARE MONITORAGGIO DI RETE, INTRUSION DETECTION SISTEM, ECC**
- **SISTEMI GPS**

  (es. black-box su autovetture aziendali, apps)

CONTROLLI ELETTRONICI & PRIVACY: FORMALITA'

STRUMENTI RILEVAZIONE PRESENZE

- **Nessuna formalità**

STRUMENTI DI CONTROLLO ELETTRONICO A DISTANZA DEI LAVORATORI

- **PREVENTIVO ACCORDO CON RAPPRESENTANZE SINDACALI AZIENDALI (RSA). NB: SUFFICIENTE LA MAGGIORANZA DELLE RSA**
- **IN MANCANZA DI RSA O IN DIFETTO DI ACCORDO SINDACALE: AUTORIZZAZIONE DELLA DIREZIONE TERRITORIALE DEL LAVORO COMPETENTE.**
- **NEL CASO DI PIU' STABILIMENTI, FILIALI, SEDI, UFFICI O REPARTI AUTONOMI CON + DI 15 DIPENDENTI, UBICATI NEL TERRITORIO DI DTL DIVERSE: AUTORIZZAZIONE DEL MINISTERO DEL LAVORO**

MOBILE

- Convergenza servizi su smartphone + BYOD – Bring Your Pown Device) + AGILE WORKERS (lavoro agile) con conseguente Integrazione dati privati e lavorativi (utilizzo a fini promiscui) + Ampliamento tipologie di dati raccolte e trattate + Controllo dei dati sempre più difficile & fusione tra identità digitale (codice IMEL numero cell, contatti rubrica) e identità reale + Molte apps erogate con modalità cloud con trasferimento altrove dei dati (saas) + esternalizzazione-

- SMARTPHONE SECURITY: RISK ANALISYS (ES. UTILIZZANDO STANDARD RECOMMENDATIONS ENISA DIC. 2010)

Apps: privacy by process vs. privacy by platform: nella prima la privacy è gestita tramite Tos – terms of service tra potenziale sviluppatore accreditando e il gestore del market + verifica tecnica di sicurezza dell'apps ante pubblicazione, nella seconda non vi sono verifiche tecniche da parte del gestore marketplace, la privacy è lasciata alle funzionalità del sistema operativo + informazione sui dati a cui il prodotto applicativo può accedere nell'utilizzo + ranking utenti

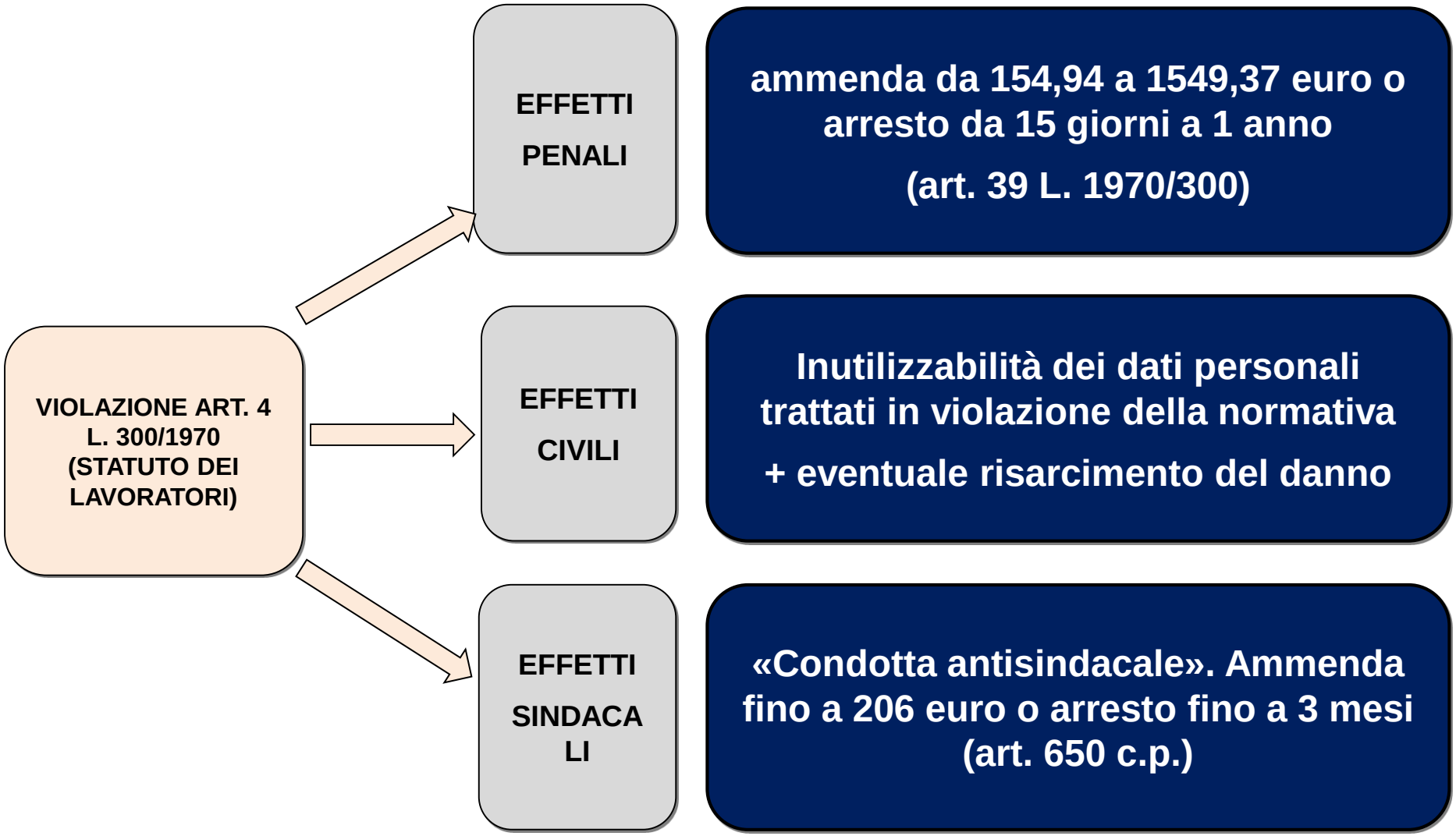
– REGOLAMENTO INFORMATICO AZIENDALE: + granulare. Obsolescenza accelerata. Esigenza di periodica revisione. Non è un costo inutile.

- PROVV. 258/2014 GARANTE SU MOBILE REMOTE PAYMENT di beni/servizi (es. su informative e consenso) rivolto a merchant, aggregatori tramite piattaforme tecnologioche e gestori servizi IT e comunicazione.

Un esempio: i metodi di gestione dei dispositivi mobili aziendali

- **BYOD** (Bring Your Own Device): L'azienda consente ai dipendenti di usare per scopi di lavoro i **dispositivi mobili da essi posseduti**.
- **CYOD** (Choose Your Own Device): L'azienda dà al dipendente la possibilità di utilizzare il proprio device personale previa autorizzazione.
- **COPE** (Corporate Owned, Personally Enabled): L'azienda fornisce al dipendente il device, ma offre **alcune importati concessioni riguardo l'abilitazione all'uso personale**, come per esempio l'utilizzo di particolari App o social network.
- **COBO** (Corporate Owned, Business Only): L'azienda fornisce il dispositivo da utilizzare esclusivamente per le attività di lavoro, e ne assicura funzionamento, manutenzione e applicativi da utilizzare.

La scelta aziendale di utilizzare luna o l'altra metodologia di gestione, h diretti riflessi sul tenore delle clausole contenute in materia nel Regolamento IT aziendale.


VIOLAZIONE ART. 4 L. 300/1970 (STATUTO DEI LAVORATORI)
EFFETTI PENALI
ammenda da 154,94 a 1549,37 euro o arresto da 15 giorni a 1 anno
(art. 39 L. 1970/300)
EFFETTI CIVILI
Inutilizzabilità dei dati personali trattati in violazione della normativa
+ eventuale risarcimento del danno
EFFETTI SINDACALI
«Condotta antisindacale». Ammenda fino a 206 euro o arresto fino a 3 mesi (art. 650 c.p.)

LA VIDEOSORVEGLIANZA E LA GEOLOCALIZZAZIONE

VIDEOSORVEGLIANZA

- I trattamenti devono rispettare tutte le linee guida (limitazioni) di cui ai **Provvedimento generali del Garante** (29.11.2000, 29.04.2004, 8.4.2010), es.:

  - ✓ L'installazione di telecamere è lecita **solo quando altre misure di sicurezza sono ritenute insufficienti o inattuabili**
  - ✓ **Divieto di controllo a distanza** (vietato installare telecamere specificamente preordinate a tale finalità, es. per controllare il rispetto dell'orario di lavoro o l'osservanza dei doveri di diligenza e la correttezza della prestazione lavorativa)
  - ✓ Facoltà di installazione per **esigenze specifiche** (organizzative, produttive, di sicurezza del lavoro e tutela del patrimonio) dalle quali derivi anche la possibilità di controllo a distanza, **accordo sindacale o autorizzazione della DTL** – Direzione Territoriale del Lavoro competente (art. 4 co. 2 L 30071970) (sanzione 38 L. 300/1970: ammenda da 150 a 1500 euro o arresto da 15 giorni a 1 anno; NB: applicabile anche se l'impianto installato non funziona ancora)

GPS – GLOBAL POSITIONING SYSTEM

- E’ un obbligo di legge la redazione di una **Procedura generale**, da aggiornare nel caso di successive variazioni sostanziali della situazione di fatto
- Implica l’**identificazione precisa delle finalità** della geolocalizzazione

- E’ reso oggetto dell’**accordo sindacale o dell’istanza di autorizzazione della DTL** – Direzione Territoriale del Lavoro competente (art. 4 L. 300/1970) (sanzione 38 L. 300/1970: ammenda da 150 a 1500 euro o arresto da 15 giorni a 1 anno)

- Presuppone la creazione di un’**informativa privacy ad hoc**, duplice (sui beni in cui è installata es. autovetture, smartphone, portatili, + interna)

GPS – GLOBAL POSITIONING SYSTEM

- Fino al 25 maggio 2018, implica l'**obbligo di notifica al Garante** privacy

- I trattamenti devono rispettare le linee guida (limitazioni) contenute nel **Provvedimento generale del Garante** in materia, e nel **Provv. Garante 8.9.2016 n. 350**

  - es. apps di geolocalizzazione per finalità di rilevazione presenze dipendenti tramite smartphone privato (cd. «geo-timbratura del cartellino) i) richiede il consenso, ii) deve essere attivata da parte del medesimo dipendente; iii) richiede informativa ad hoc sul parabrezza dell'autovettura, e iv) va limitato all'ambito lavorativo, v) deve cancellare dati (es. posizione lavoratore) diversi dalla sede di lavoro e data e orario di timbratura, ecc.)

GPS – GLOBAL POSITIONING SYSTEM

- **Circolare 7.11.2016 n. 2 Ispettorato Nazionale del lavoro – INL**

✓ **le apparecchiature di localizzazione satellitare GPS su autovetture aziendali, rappresentano un elemento «aggiunto» agli strumenti di lavoro, non venendo utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa**, ma per rispondere ad esigenze ulteriori (di carattere assicurativo, organizzativo, produttivo o di sicurezza del lavoro); **pertanto devono essere ricondotte al co. 1 dell'art. 4 L. 300/1970** (quali «altri strumenti dai quali derivi la possibilità di controllo a distanza dei lavoratori» e non già al co. 2 del medesimo articolo (che parla invece di «strumenti per rendere la prestazione di lavoro») pertanto vanno assoggettate ai relativi adempimenti (accordo sindacale, autorizzazione DTL)

✓ tali apparecchiature **finiscono per «trasformarsi» in veri e propri strumenti di lavoro,** con conseguente «liberalizzazione» ex co. 2, **solo** in casi particolari, ricorrenti quando l'installazione dei sistemi GPS sia **necessaria per consentire la concreta ed effettiva attuazione della prestazione** (non eseguibile, cioè, senza tali strumenti) **oppure sia richiesta da specifiche normative** (es. per trasporto di portavalori superiore a 1.500.000,00 euro)

GPS – GLOBAL POSITIONING SYSTEM

- **Contra: DIL di Milano – parere n. 5689/2016 (in linea con altri uffici periferici)**

  ✓ l'autovettura fornita in uso ai dipendenti per eseguire al prestazione lavorativa «**è sicuramente strumento di lavoro e lo è nella sua unicità**»,
  pertanto «***il sistema GPS (pur se montato successivamente all'originaria consegna del veicolo) non è da considerare separatamente dall'auto cui accede e per la sua installazione non è necessario il preventivo accordo sindacale o la preventiva autorizzazion***e»

SUGGERIMENTO PRATICO:

- La posizione dell'INL non è affatto convincente, tuttavia è bene che prudentemente il datore di lavoro tenga conto delle indicazioni di cui alla Circolare 7.11.2016 n. 2 Ispettorato Nazionale del lavoro.

L’INFORMATIVA PRIVACY AGLI INTERESSATI

DIRITTI DELL'INTERESSATO EX NUOVO REGOLAMENTO PRIVACY UE (ARTT. 17, 18, 19, 20)

Vengono formalizzati diritti di origine giurisprudenziale, introdotti alcuni diritti ex novo, o rafforzati diritti già previsti

- **Diritto all'informativa (e al consenso informato)**
- **Diritto al reclamo presso qualsiasi Autorità nazionale**
- **Diritto all'oblio** (se cessate finalità, o revocato consenso, o se trattamento non è conforme, ecc.)
- **Diritto alla portabilità dei dati** (ricezione in formato strutturato, di uso comune e leggibile da dispositivo automatico, trasferimento a nuovi terzi titolari)
- **Diritto alla comunicazione del Data Breach** (se colpisce i suoi diritti e le libertà fondamentali)

INFORMATIVA ALL'INTERESSATO (art. 13 D.Lgs. 196/2003)

L'INTERESSATO VIENE PREVIAMENTE INFORMATO, ORALMENTE O PER ISCRITTO, CIRCA

- **Le finalità del trattamento e le modalità del trattamento cui sono destinati i dati**
- **La natura obbligatoria o facoltativa del conferimento dei dati**
- **Le conseguenze di un eventuale rifiuto a conferire i dati**
- **I soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dai dati**
- **I diritti di cui all'art. 7**
- **Gli estremi identificativi del titolare, e se designati, dei responsabili**

NUOVO REGOLAMENTO PRIVACY UE: INFORMATIVA PRIVACY (ARTT. 13-14)

- **L'informativa si sdoppia, a seconda che la raccolta dei dati personali avvenga *presso l'interessato o in altro modo.***
- **L'informativa va resa con linguaggio semplice e chiaro e diventa ancora più articolata che in passato (indicando ad esempio:**
  - ✓ ***base giuridica*** del trattamento
  - ✓ ***legittimi interessi*** del titolare, ove esistenti
  - ✓ nel caso di trasferimento di dati a paesi terzi: esistenza o assenza di una ***decisione di adeguatezza*** della Commissione UE o indicazioni di adeguate ***garanzie*** (clausole, certificazioni)
  - ✓ periodo di ***conservazione*** o criteri per determinarlo

L'obbligo di informativa tuttavia NON SI APPLICHERA':

- ✓ ***Quando l'interessato dispone già delle informazioni***
- ✓ ***Quando l'ottenimento o la comunicazione siano già previsti dal diritto comunitario che tutela gli interessi legittimi dell'interessato mediante appropriate misure***

INFORMATIVE PRIVACY: CHECK-LIST SU CRICITA' PIU' FREQUENTI

- MAPPATURA SOLO PARZIALE DELLE TIPOLOGIE DI INFORMATIVE IN USO (IT – NON IT)
- MANCATA MAPPATURA DEI CANALI/STRUMENTI DI COMUNICAZIONE DELLE INFORMATIVE
- MANCATO COORDINAMENTO DELLE INFORMATIVE PRIVACY CON L'INVENTARIO DEI TRATTAMENTI (FINALITA', TERZI DESTINATARI COMUNICAZIONI, CATEGORIE DI DATI, TERMINE CANCELLAZIONE, , ECC.)
- INDIVIDUAZIONE SOLO PARZIALE DEI DESTINATARI (ES. ADS, OPERATORI INTERNI CALL CENTER, ECC)
- CARENTE COINVOLGIMENTO DELLA FUNZIONE IT NELLA REDAZIONE DELLE INFORMATIVE (Regolamento IT)
- INADEGUATA/INSUFFICIENTE RACCOLTA E CONSERVAZIONE DELLE PROVE DELL' INVIO AI DESTINATARI (ES. LOGS, EMAIL, ECC.)
- MANCATO AGGIORNAMENTO STRAORDINARIO NFORMATIVE AL REGOLAMENTO UE 679/2016
- MANCATA REVISIONE PERIODICA DELLE INFORMATIVE

L’INTERESSATO E I SUOI DIRITTI

Identità personale (diritto alla)	È il “bene personale”, dinamico, costituito dall’**insieme dei caratteri** (connotati e contrassegni personali, come qualità, fatti, comportamenti, informazioni, ecc) **e dal nome** (generalità o risultanze anagrafiche) **di una persona fisica**, **che consentono di identificarla e distinguerla in modo univoco**, nei confronti del potere pubblico e di terzi
Identità digitale	È l’identità personale determinata dall’**attribuzione ad un soggetto di attributi distintivi univoci**, tramite sistemi/tecniche di identificazione e autenticazione (PIN, password, token, biometria, ecc), **in funzione di un accesso a, e/o utilizzo di, sistemi informatici o telematici**
Dato personale	Definito dal TU privacy e dalla normativa europea
Privacy	Regole applicabili alle **decisioni** riferibili ai dati personali (diritto all’autoderminazione preventiva sul controllo dei dati e a reagire a determinati rischi di non integrità degli stessi)
Riservatezza	Tutela legale contro la **divulgazione non autorizzata**
Sicurezza	Regole circa la **protezione fisica, logica e organizzativa** dei dati personali e/o delle informazioni

INTERESSATO: defiinizione

1) è **la persona fisica a cui i dati personali si riferiscono, e i cui diritti devono pertanto essere tutelati ai sensi della normativa privacy**

2) in limitati casi, cioè **solo quando i dati sono trattati per finalità di marketing, sono però sostanzialmente parificate/i all'"interessato" le persone giuridiche, gli enti e le associazioni** (al fine di riconoscere loro l'esercizio dei medesimi diritti spettanti alla persona fisica, in particolar modo in tema di informativa ex art. 13 TU privacy e di consenso)

INTERESSATO: definizione

Le finalità di marketing in senso generico, sono poi ulteriormente classificabili come segue, ai fini privacy:

i) marketing diretto, ii) profilazione

iii) fidelizzazione

Le finalità di marketing diretto includono a loro volte quelle di:

- **Comunicazione commerciale**
- **Offerta di vendita di beni/servizi**
- **Ricerche di mercato**

TERMINI DI ESERCIZIO DEI DIRITTI

Art. 8 D Lgs. 196/2003

I diritti di cui all'art. 7 sono esercitati con richiesta rivolta senza formalita' al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo **riscontro senza ritardo**.

Cassazione civ. sez. I, 9 gennaio 2013 n. 349

Il titolare del trattamento dei dati deve **rispondere** alla richiesta di accesso ai dati personali ex art. 7 D.lgs. 196/2003 avanzata dall'interessato, **entro 15 giorni**. Tale termine deve intendersi come tassativo.

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALLA PORTABILITA' DEI DATI

(art. 20)

PROCEDURA

DIRITTO ALLA COMUNICAZIONE DEL DATA BREACH

(art. 34)

PROCEDURA

DIRITTO ALL'OBLIO

(art. 17)

PROCEDRA

Adacta Tax & Legal

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALLA PORTABILITA' DEI DATI

Diritto dell'interessato di:

i) **ricevere** dal titolare del trattamento, **in un formato strutturato, di uso comune e leggibile da un dispositivo automatico i dati personali** che riguardano l'interessato stesso;

ii) **trasmettere tali dati ad altro titolare senza impedimento** del precedente titolare originario ricevente;

iii) ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro (se tecnicamente fattibile)

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALLA PORTABILITA' DEI DATI

Condizioni:

- Il trattamento si basi su un **consenso** prestato per specifiche finalità dall'interessato, o
- Il trattamento si basi su un **contratto** di cui è parte l'interessato, e
- Il trattamento sia effettuato con **mezzi automatizzati**
- **Non vengano lesi i diritti e le libertà altrui**

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALLA COMUNICAZIONE DEL DATA BREACH

Obbligo dell'azienda titolare di **informare senza ingiustificato ritardo e con linguaggio semplice e chiaro** l'interessato **di ogni violazione dei dati personali** suscettibile di presentare un rischio elevato per i diritti e le libertà del medesimo

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALLA COMUNICAZIONE DEL DATA BREACH

L'informativa deve contenere, de minimis, le informazioni relative a

i) nome e dati di contatto del responsabile della protezione dei dati personali,

ii) descrizione delle probabili conseguenze della violazione,

iii) descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per rimediare alla violazione e, se del caso, attenuarne i possibili effetti negativi

NUOVI DIRITTI EX REG. UE 679/2016

ESENZIONE DALLA COMUNICAZIONE DEL DATA BREACH

Se, alternativamente:

- Il titolare aveva attua misure tecniche-organizzative di protezione adeguate dei dati personali violati (cifratura, anonimizzazione, ecc.)

- Vengono adottate misure successive idonee a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati

- Sono richiesti sforzi di comunicazione sproporzionati (in tal caso vi è obbligo di comunicazione pubblica o altra misura similare)

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALL'OBLIO

(O ALLA CANCELLAZIONE)

Diritto di **ottenere senza ingiustificato ritardo** dal Titolare del trattamento **la cancellazione** dei propri dati personali, nel casi di cui all'art. 17.

Non si applica nella misura in cui il trattamento sia necessario per le finalità di cui al comma 2 (diritto di espressione/informazione, obblighi legali del titolare, interesse pubblico sanitario, a fini di ricerca scientifica, storica o fini statistici, esercizio e difesa di diritti in sede giudiziaria,)

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALL'OBLIO

(O ALLA CANCELLAZIONE)

Presupposti:

a) Sopravvenuta **non necessità** dei dati rispetto alle finalità di originaria raccolta/trattamento

b) **Revoca del consenso** (in contestuale assenza di altra base giuridica del trattamento)

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALL'OBLIO

(O ALLA CANCELLAZIONE)

c) Opposizione al trattamento (salvo esistano dimostrati legittimi motivi cogenti prevalenti, o finalità di esercizio o difesa di un diritto in giudizio)

Opposizione al trattamento per finalità di marketing diretto (inclusa la profilazione connessa a tale marketing diretto)

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALL'OBLIO

(O ALLA CANCELLAZIONE)

d) Trattamento illecito dei dati

e) Cancellazione **necessaria per l'adempimento di un obbligo legale** del titolare del trattamento, previsto dalla normativa UE o nazionale

NUOVI DIRITTI EX REG. UE 679/2016

DIRITTO ALL'OBLIO

(O ALLA CANCELLAZIONE)

- Raccolta dei dati relativamente all'**offerta di servizi della società dell'informazione** diretti a interessati di età maggiore di 16 anni o inferiore a 16 anni – derogabile purchè superiore 13 - con consenso del relativi genitore)

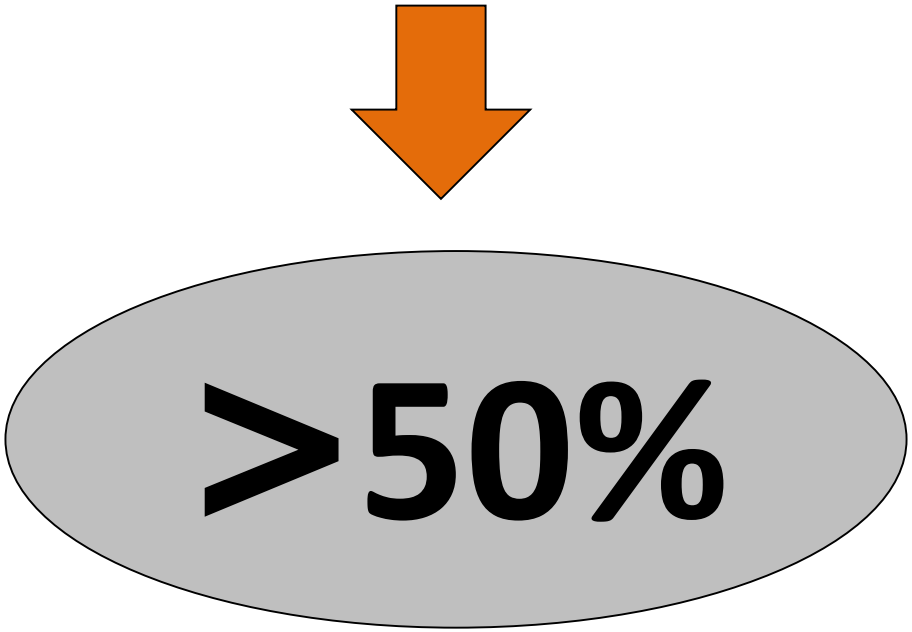
LE SANZIONI
(ATTUALI E FUTURE)

Sanzioni amministrative pecuniarie – D.lgs. 196/2003

REGIME VIGENTE (FINO AL 24.5.2018)	VIOLAZIONI AMMINISTRATIVE	SANZIONI
Omessa/inidonea informativa (art. 161)	**Violazione delle disposizioni di cui all'art. materia di informativa all'interessato**	**da 6.000 a 36.000 euro**
Omessa/incompleta notificazione (art. 163)	Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli artt. 37 e 38, ovvero indica in essa notizie incomplete	da 20.000 a 120.000 euro
Omessa informazione/esibizione al Garante (art. 164)	Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli artt. 150, co. 2, e 157	da 10.000 a 60.000 euro
Altre fattispecie (art. 162)	Cessione dei dati in violazione dell'art. 16, co. 1, lett. *b),* o di altre disposizioni in materia di disciplina del trattamento dei dati personali	da 10.000 a 60.000 euro
	Violazione della disposizione di cui all'art. 84, co. 1	**da 1.000 euro a 6.000 euro**
	Violazione delle misure minime di sicurezza *ex* art. 33 del Codice o delle disposizioni indicate nell'art. 167	**da 20.000 a 120.000 euro**
	Inosservanza dei provvedimenti del Garante di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'art. 154, co. 1, lett. *c)* e *d)*	da 30.000 a 180.000 euro
	Commissione degli illeciti amministrativi previsti dagli articoli 161, 162, 163 e 164	pubblicazione del provvedimento del Garante (facoltativa)

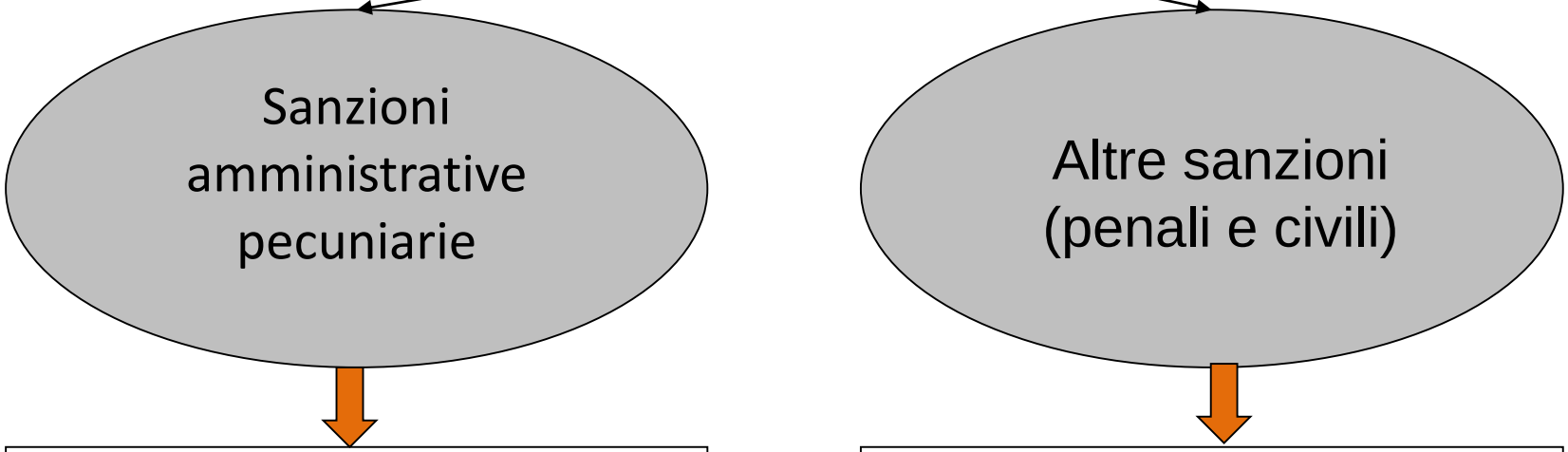
Sanzioni penali – D.lgs. 196/2003

REGIME VIGENTE (ANCHE POST 24.5.2018)	VIOLAZIONI PENALI	Sanzioni
Trattamento illecito di dati (art. 167) (es. in assenza di consenso informato)	Chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 18, 19, 23, 123, 126 e 130, o in applicazione dell'art. 129, è punito, se dal fatto deriva nocumento	**reclusione da 6 a 18 mesi o, se il fatto consiste nella comunicazione o**
	Chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli artt. 17 (trattamento che presenta rischi specifici) 20, 21, 22, co. 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento	**diffusione, reclusione da 6 a 24 mesi**
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168)	Chiunque, nella notificazione di cui all'art. 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi	**reclusione da 6 mesi a 3 anni**
Misure di sicurezza (art. 169)	**Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'art. 33**	**arresto sino a 2 anni**
Inosservanza di provvedimenti del Garante (art. 170)	Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli artt. 26, co. 2, 90, 150, co. 1 e 2, e 143, co. 1, lett. c)	**reclusione da tre mesi a due anni**
Altre fattispecie (art. 171)	**Violazione delle disposizioni di cui agli artt. 113, co. 1, (divieto di indagini sulle opinioni dei lavoratori) e 114 (controlli a distanza)**	**sanzioni previste dall'art. 38, Statuto dei lavoratori (Legge 1970 n. 300): arresto da 15gg a 1 anno**
Sanzione accessoria (art. 172)	Condanna per uno dei delitti previsti dagli articoli 167, 168, 170 e 171	**pubblicazione della sentenza di condanna (obbligatoria)**



delle norme previste dal nuovo Regolamento Privacy UE 679/2016 sono assistite da una sanzione

A partire dal 24.5.2018, le sanzioni per violazioni delle norme del Regolamento UE privacy saranno distinte, come segue::



Ignorantia legis non excusat!....

Adacta Tax & Legal

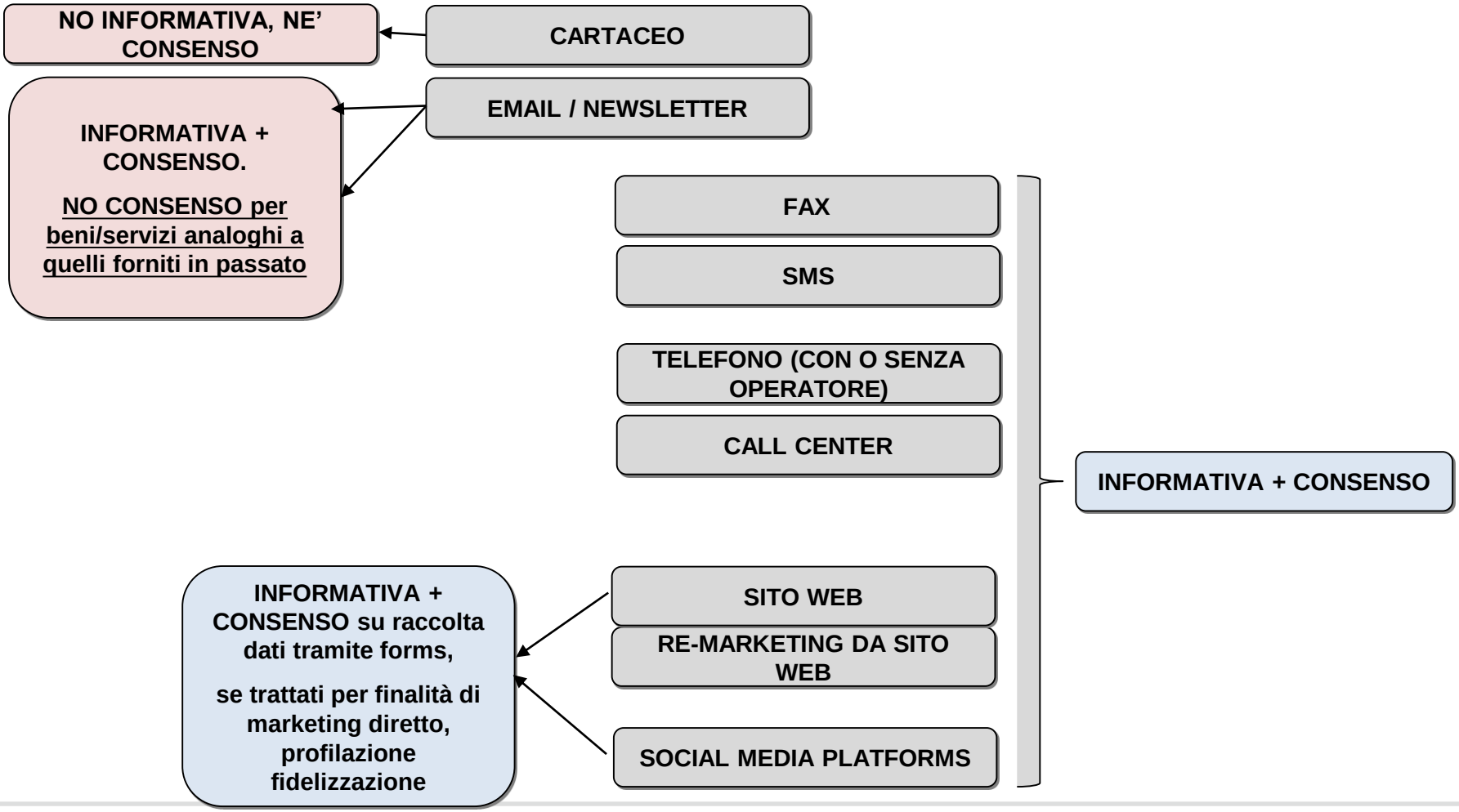
Sanzioni amministrative pecuniarie – Reg. UE 679/2016

Violazione degli artt. 8, 11, da 25 a 39 (tra cui governance, misure di sicurezza, analisi dei rischi), 42 e 43 Violazione dell'organismo di certificazione a norma degli articoli 42 e 43 Violazione dell'organismo di controllo ex art. 41 par. 4	**Fino a 10.000.00 euro, o, per le imprese, fino al 2% del fatturato annuo mondiale, se superiore**
- Violazione dei principi di base del trattamento (artt. 5 sulla proporzionalità del trattamento, 6 sul lecito e corretto trattamento, 7 relativo al consenso e 9 relativo ai dati sensibili) - Mancato rispetto dei diritti degli interessati da art. 12 a 22 (es. informative, accesso, oblio, portabilità dei dati, decisioni automatizzate, ecc.) - Violazione della norma sul trasferimento a paesi terzi - Inosservanza di ordini o divieti dell'Autorità - Violazione di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX (es. quelle relative al trattamenti dei dati nell'ambito dei rapporti di lavoro)	**Fino a 20.000.00 euro, o, per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente, se superiore**

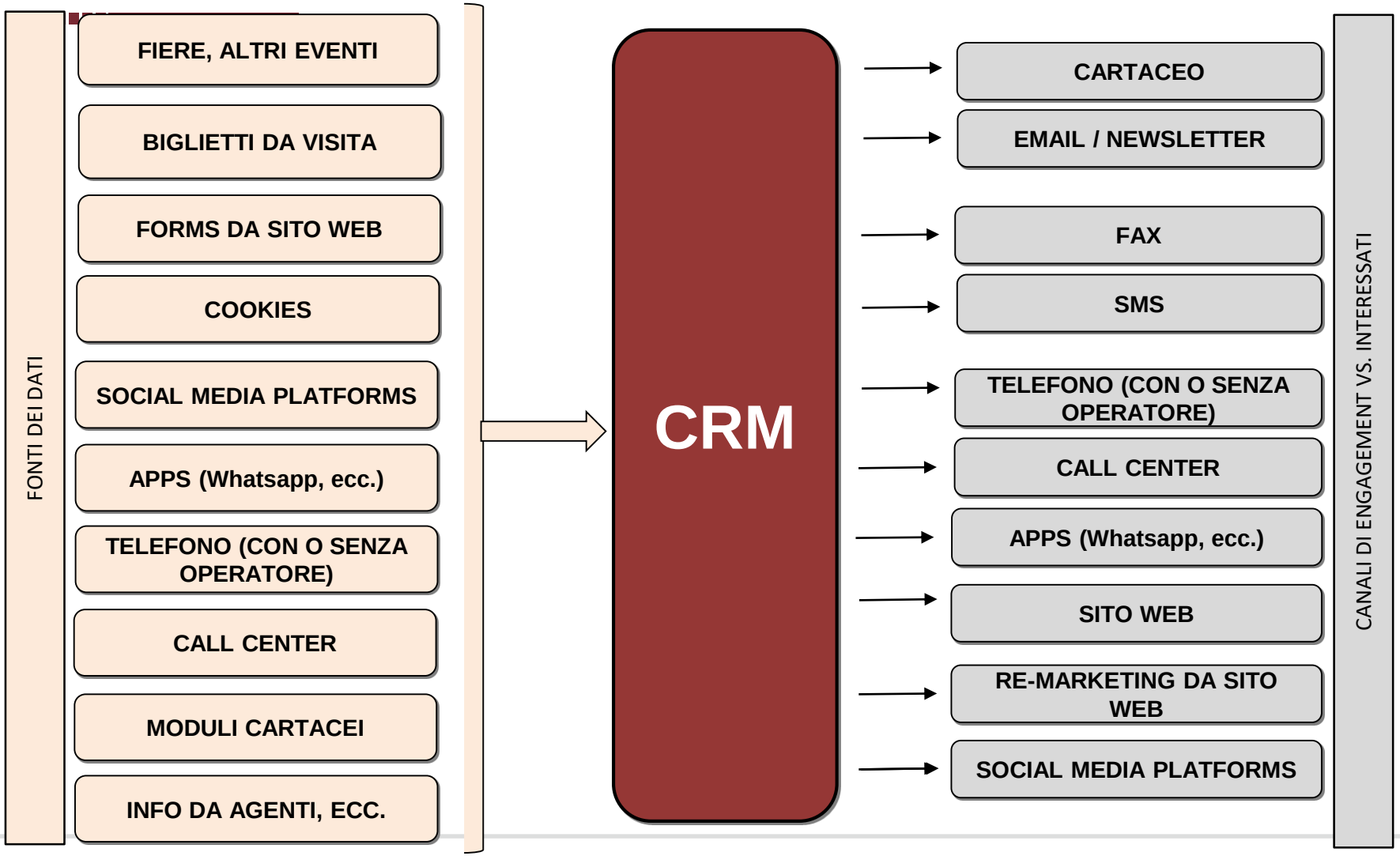
Adacta Tax & Legal

I CANALI COMMERCIALI E LA PRIVACY

GLI OBBLIGHI DI INFORMATIVA E CONSENSO PRIVACY VARIANO IN DIPENDENZA DELLA TIPOLOGIA DI STRUMENTO DI COMUNICAZIONE COMMERCIALE USATO DALL'IMPRESA

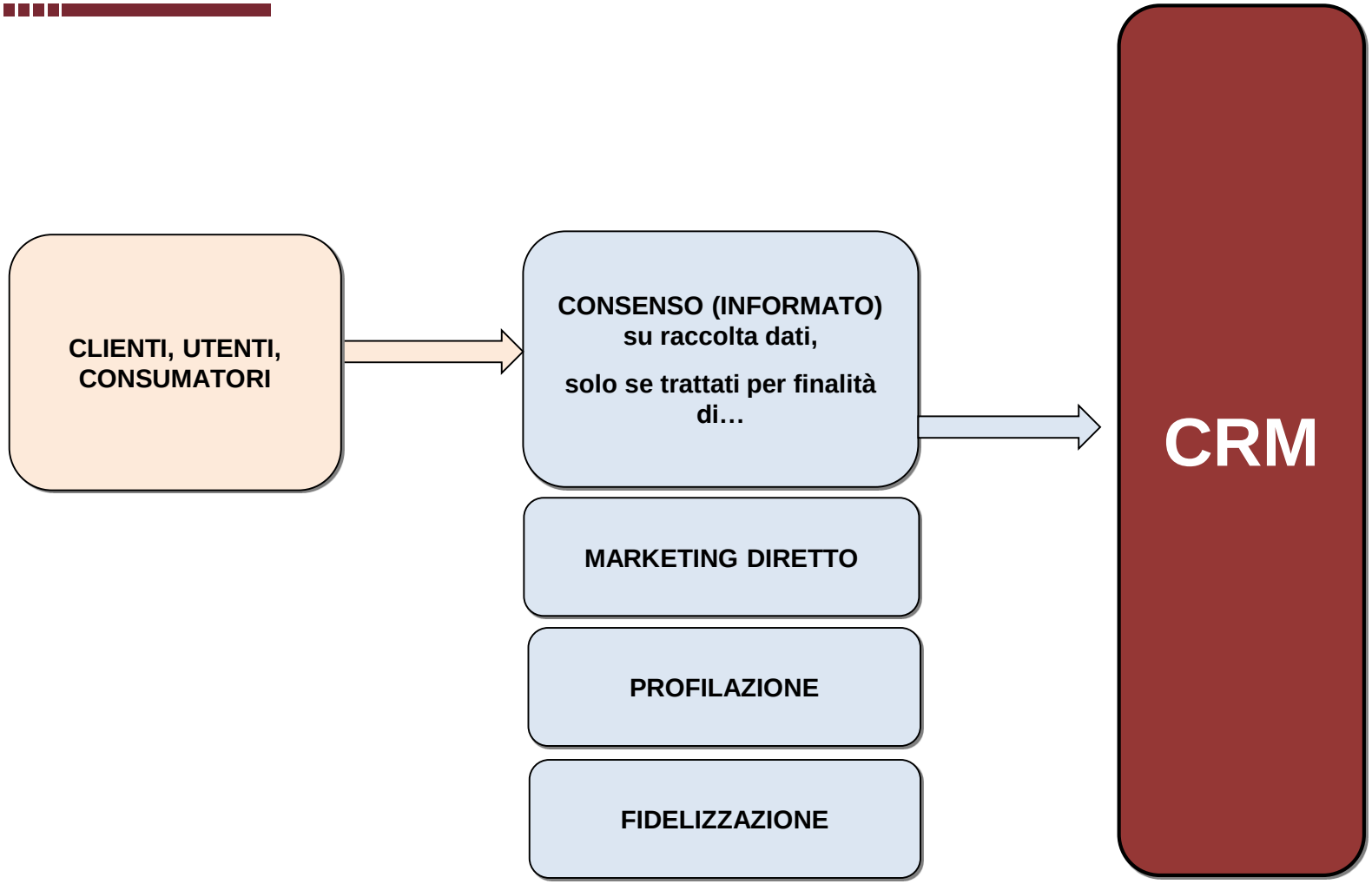


CRM – CUSTOMER RELATION MANAGEMENT



Adacta Tax & Legal

CRM – CUSTOMER RELATION MANAGEMENT



Adacta Tax & Legal

Nei casi in cui la legge richiede che il trattamento dei dati abbia luogo previo necessario <u>previo consenso</u> dell'interessato (es. trattamento per finalità di marketing, o per comunicazione dei dati di candidati a società non appartenenti al medesimo gruppo, e così via) **il consenso deve essere sempre <u>«informato»</u>,** cioè preceduto da una corretta (in particolare: completa) preliminare informativa da parte del titolare del trattamento.

Nel caso in cui l'informativa predetta sia omessa o **carente di anche solo taluno dei suoi elementi essenziali**, ogni trattamento dei dati operato dal titolare è automaticamente illecito, a norma di legge (con responsabilità addirittura penale (v. slides su Sanzioni).

I responsabili delle singole aree funzionali del trattamento (e/o il responsabile principale del trattamento, se nominato dal titolare) devono quindi accertarsi che agli interessati sia stata fornita l'informativa adeguata.

CRM – CUSTOMER RELATION MANAGEMENT

CONSENSO (INFORMATO)
su raccolta dati,

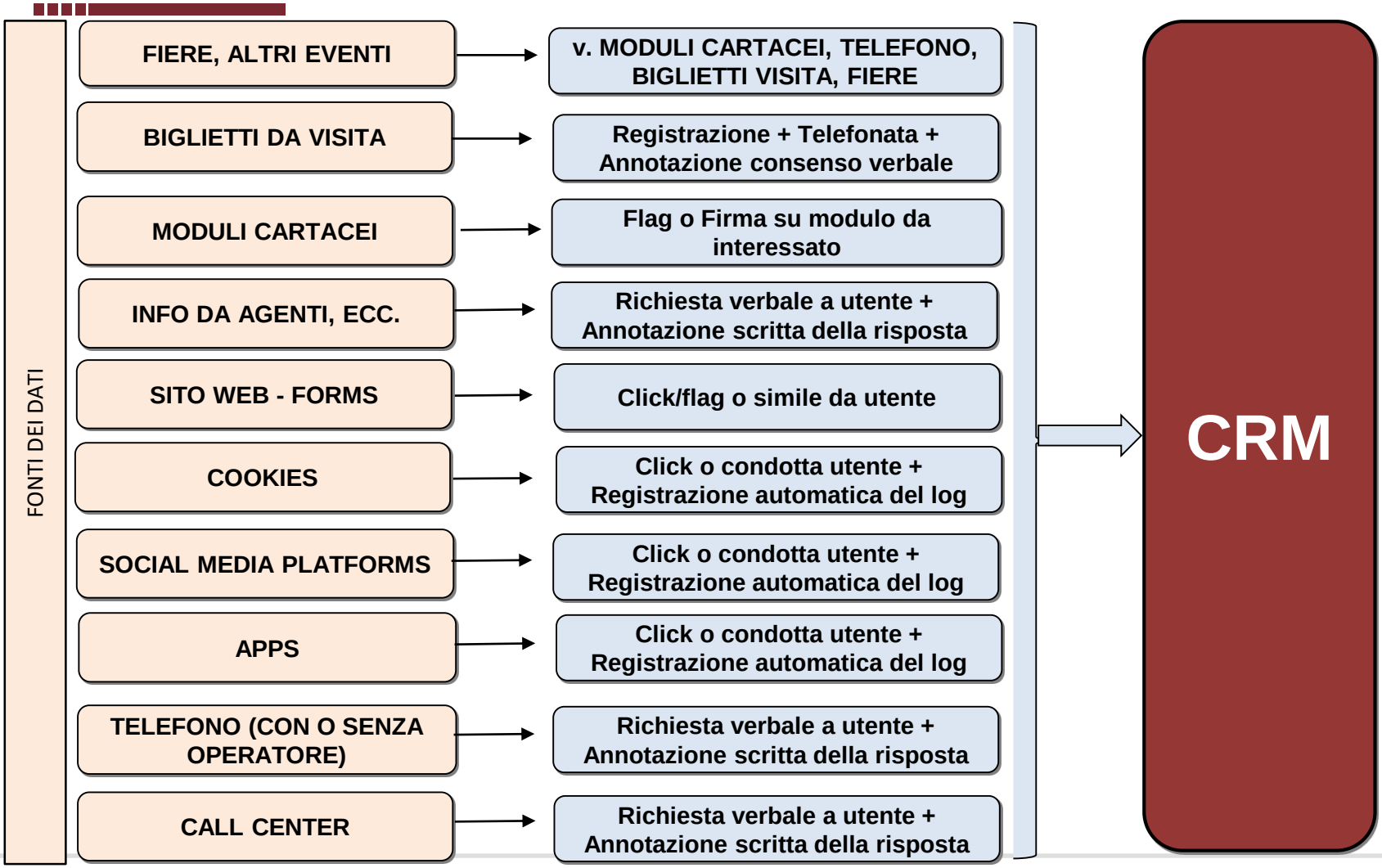
solo se trattati per finalità di…

a) MARKETING DIRETTO	**COMUNICAZIONE COMMERCIALE, OFFERTA DIRETTA DI VENDITA DI BENI E SERVIZI**
b) PROFILAZIONE	**ADOZIONE DI DECISIONI BASATE ANALIZZANDO O PREVEDENDO LE PREFERENZE, I GUSTI, LE ABITUDINI, I COMPORTAMENTI DI ACQUISTO DELL'INTERESSATO**
c) FIDELIZZAZIONE	**FIDELITY CARD, CONCORSI A PREMI, ECC**

CRM

Adacta Tax & Legal

OBBLIGO DI RACCOLTA DEL CONSENSO VS. CLIENTI/UTENTI INTERESSATI: MODALITA'

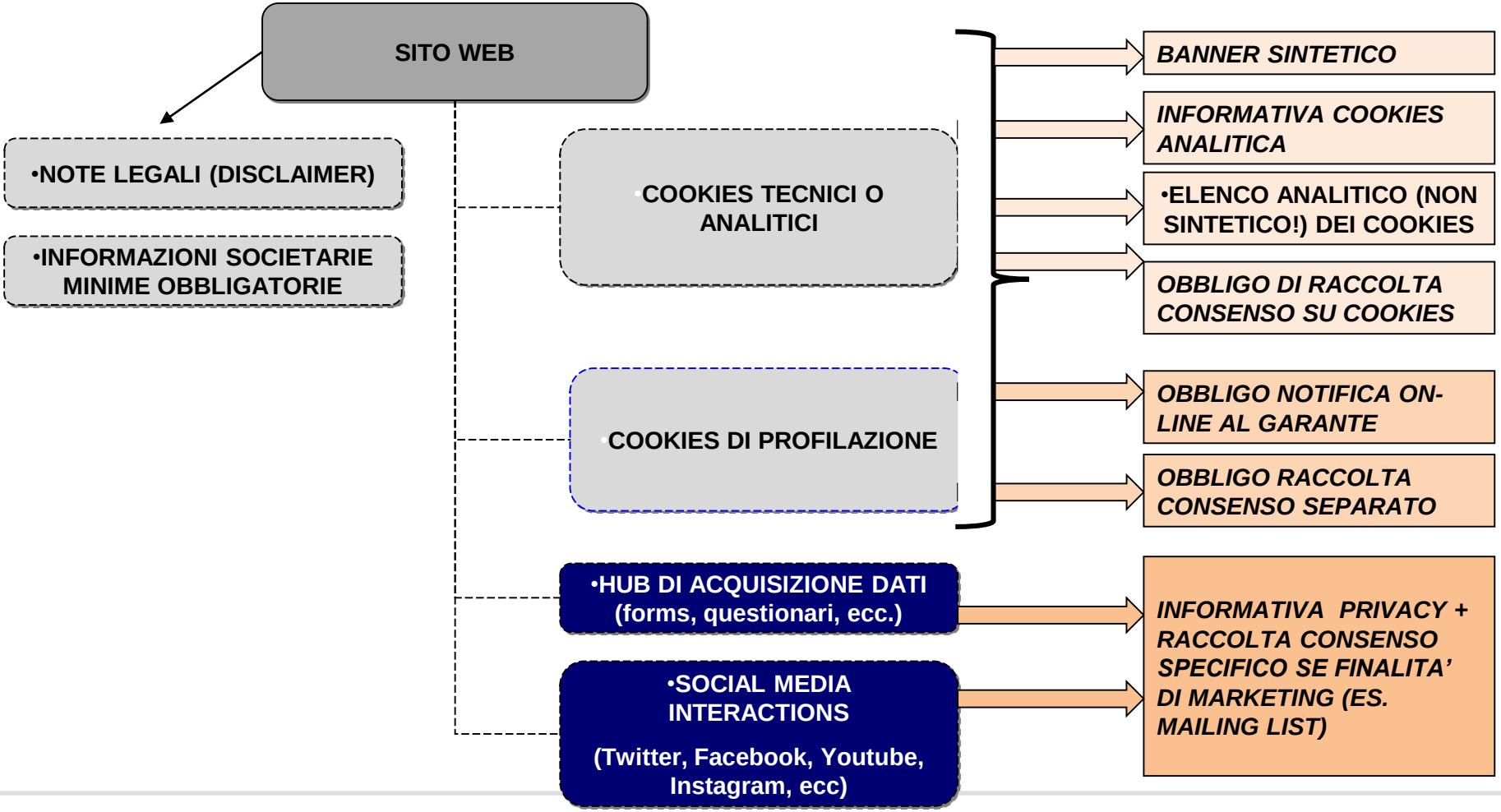


Adacta Tax & Legal

IL SITO WEB AZIENDALE E LA PRIVACY

SITI WEB, COOKIE POLICY E NOTIFICA ON-LINE AL GARANTE

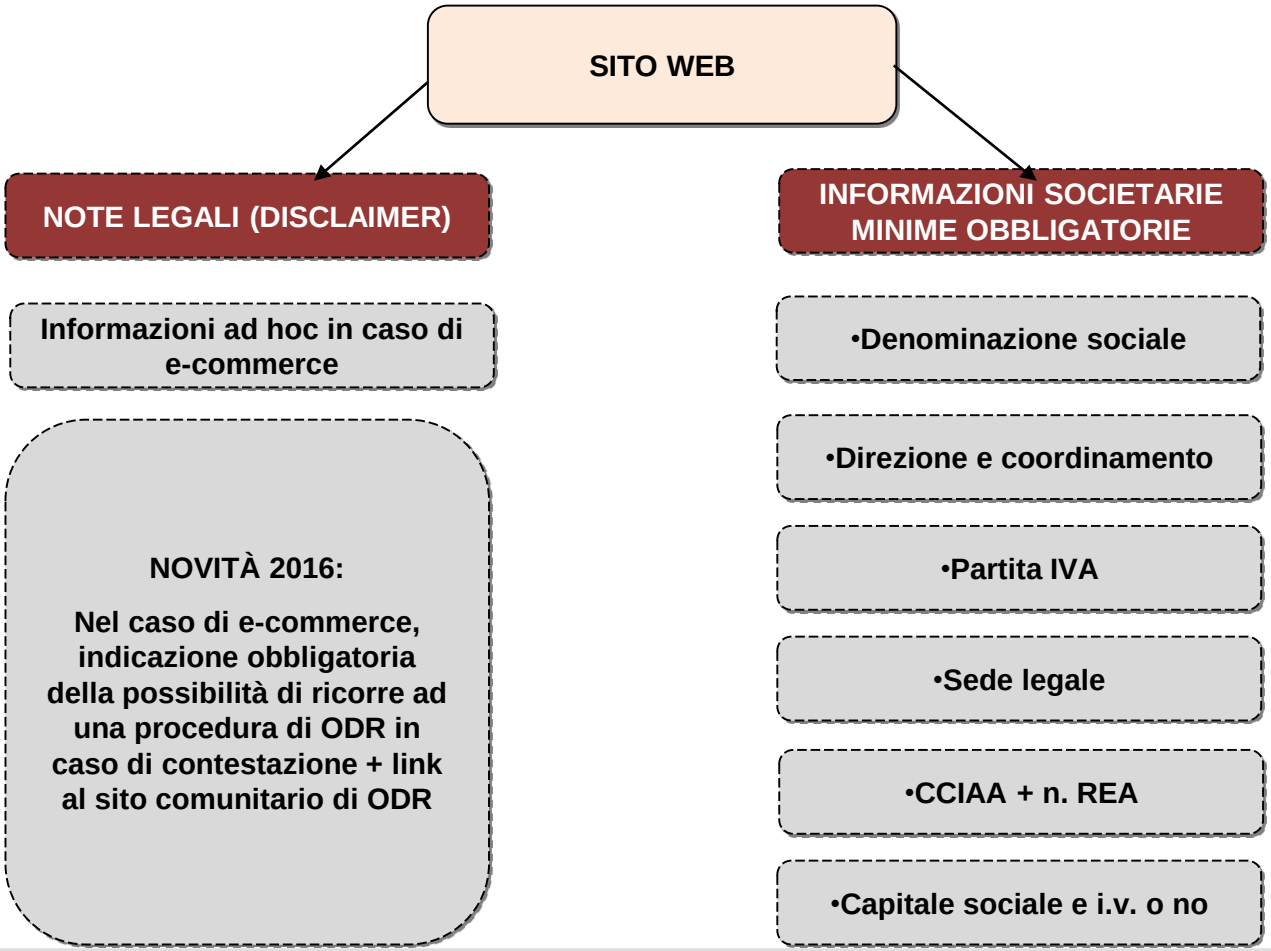
Il SITO WEB AZIENDALE OGGI HA UNA RILEVANZA OPERATIVA FONDAMENTALE, CONSENTENDO UNA INTERAZIONE INNOVATIVA CON I CLIENTI (UTENTI, CONSUMATORI, PARTNERS):



Adacta Tax & Legal

SITI WEB E CODICE CIVILE

LE NOTE LEGALI DEVONO CONFORMARSI AL CONTENUTO OBBLIGATORIO PREVISTO DALLA DIRETTIVA 2000/31/CE SUI SERVIZI DELLA SOCIETA' DELL'INFORMAZIONE E DAL CODICE DEL CONSUMO



SITI WEB: LE NOVITA' RECENTI

SI SUGGERISCE DI VERIFICARE CHE IL SITO WEB AZIENDALE SIA AGGIORNATO A DUERECENTI NOVITA' TECNICO-NORMATIVE

SITO WEB

MIGRAZIONE AL PROTOCOLLO HTTPS

A partire dal gennaio 2017, la nuova versione «56» del browser Chrome di Google, pone nella barra del browser l'etichetta NON SICURO (preceduta da triangolo rosso) sui siti web e di e-commerce che richiedono agli utenti l'inserimento di pw, dati personali o di pagamento in «HTTP» (protocollo non crittografato). Solo chi usa l'HTTPS è «SICURO» (lucchetto verde).

INFORMAZIONI OBBLIGATORIE SU ADR

Ai sensi del D.lgs. n. 130 del 6 agosto 2015 attuativo della Direttiva UE 2013/11, obbligo di avvisare il consumatore dell'esistenza della procedura di Alternative Dispute Resolution on-line per eventuali controversie su contratti di vendita e di servizi, mediante attivazione di uno specifico ipertesto / link che rinvia al sito della UE in materia.

Adacta Tax & Legal

SI SUGGERISCE DI VERIFICARE CHE IL SITO WEB AZIENDALE SIA AGGIORNATO A DUERECENTI NOVITA' TECNICO-NORMATIVE

- La policy sui cookies va quasi sempre rivista per integrarla rispetto alle interazioni «social»
- Spesso i cookies vengono elencati solo in modo generico
- Attenzione al regime provvisorio (fino al 25 maggio 2018)
- Attenzione ai «concorsi a premio on-line» specie internazionali

LA «NUOVA» PRIVACY NEI GRUPPI DI SOCIETA’

DPS NEI GRUPPI SOCIETARI

Nella prassi, un approccio che miri ad un adeguamento di procedure privacy non limitato alla sola capogruppo bensì **esteso per all'intero gruppo** implica un **budget** significativo in termini di investimento e spesso quindi ciò disincentiva l'adeguamento.

Il suggerimento è dunque quello di procedere all'**adeguamento privacy per la capogruppo operativa** e di far seguire una successiva fase l'adeguamento per le altre società.

Le metodologie e procedure utilizzate per la prima fase possono infatti essere **riutilizzate per le controllate** (da parte delle stesse e/o della capogruppo in base ad un contratto di service intercompany che includa tali specifiche attività di supporto).

Il reeingineering dell'organizzazione privacy di gruppo nella prassi quasi sempre comporta una **revisione/integrazione dei contratti di service IT** intercompany in essere.

DPS/DPIA NEI GRUPPI SOCIETARI

Spesso sono presenti importanti **flussi interfrontalieri** di dati personali (vs. società del gruppo e/o vs. terzi):

- Distinguere se verso Paesi UE o **Paesi Extra-UE**

- Se verso Paesi Extra-UE, verificare se sono in "white list" secondo la **Commissione UE** (avendo tutela legale dei dati sostanzialmente equivalente a quella UE)
  Per i Paesi UE **non "white list"**, adottare le Standard Clauses (contratti ad hoc) tra società

- Rischi territoriali specifici: trasferimento dati verso **U.S.A.** (nuovo regime 2016 US-EU Privacy Shield, in sostituzione del "Safe Harbour" abrogato nel 2015 dalla Corte di Giustizia UE)

- Rischi tecnici specifici (es. trasferimento mediante utilizzo di servizi **cloud** based)

COPYRIGHT

Il materiale didattico (ivi inclusi, ma non limitatamente, il testo, immagini, fotografie, grafica) è di proprietà esclusiva e riservata di ADACTA TAX & LEGAL, e protetto dalle leggi sul copyright nazionali e internazionali. Il materiale fornito potrà esser riprodotto solo a scopo didattico per il presente corso od evento ed ogni altra riproduzione o utilizzo in toto o in parte sono vietati, salvo esplicita autorizzazione scritta di ADACTA.

Le informazioni contenute nel presente materiale sono da ritenersi esatte esclusivamente alla data di svolgimento del corso /evento e potranno essere soggette a variazioni in base alle modifiche legislative intervenute, in relazione alle quali ADACTA non si assume l'onere di inviare l'aggiornamento salvo diversamente stabilito contrattualmente tra le parti.

Avv. Luca De Muri
l.demuri@adacta.it – cell. 349-4159526
www.adacta.it - info@adacta.it