# OUTSOURCING E CLOUD AI TEMPI DEL GDPR. COME IMPOSTARE I CONTRATTI SOTTO IL PROFILO DELLA SICUREZZA INFORMATICA

## Security summit

*13 marzo 2019*

**In collaborazione con:**

Clusit

Clusit Education

# PROGRAMMA P4I FOR AUSED 2019

- **16 maggio**: Indagare le componenti che caratterizzano la spesa delle Direzione IT e le implicazioni a livello di organizzazione e strategie di sourcing;
  Marco Pozzoni
- **13 giugno:** Presentare i modelli per la gestione dell'innovazione digitale e metodologie per la valorizzazione delle competenze interne;
  Marco Planzi
- **12 settembre:** Approfondire le criticità nella negoziazione di un contratto per l'acquisto di servizi in cloud, anche in relazione al GDPR (Regolamento UE 2016/679);
  Anna Italiano, Luca Bechelli
- **10 ottobre:** Presentare le modalità di gestione dei Cyber Risk e valutazione degli investimenti di prevenzione e/o protezione.
  Luca Bechelli




OSSERVATORI.NET digital innovation

# Grazie

Francesca Gatti

aused@aused.org

345 255 9509

# ALCUNI EVENTI

OSSERVATORI.NET digital innovation

L'Espresso

DISAGI

## Poste, il software è un pacco

L'hanno pagato 40 milioni di euro e dopo sei mesi si è scoperto che era bacato: ecco perché negli uffici di mezza Italia in questi giorni ci sono code chilometriche. Sul banco degli imputati Ibm e Hp, ma c'è chi ipotizza un attacco informatico

DI DAVIDE MOSCA



A mezzogiorno nell'ufficio postale di via Usodimare - Roma, quartiere Ostiense - siamo quasi alla rivolta: «Per ogni operazione ci vuole più di un'ora, io devo ritirare la pensione, è da venerdì che ci provo e non ci riesco». E poi: «Questa tecnologia ha rovinato proprio tutto, ma fare le cose a mano no?». E ancora: «Ma perché non usano la macchina da scrivere?».

Tina, Maria, Giuseppe, Carlo e molti altri, la maggior parte pensionati, che in questi giorni sono andati agli sportelli postali e, dopo attese snervanti, sono tornati a casa furiosi.

Alla base di tutto vi è un piccolissimo bug (un errore di software) che sta facendo impazzire i tecnici di Ibm e Hp.

LA STAMPA

## Poste in tilt, ora è bufera sull'Ibm

L'ad Sarmi:«Chiederemo i danni, per i consumatori danni oggettivi»

ROMA

Sembra rientrare la catastrofe informatica che ha fatto collassare i sistemi di Poste Italiane dal primo giugno, creando immensi disagi agli utenti. Disagi che - anche se ieri non sono mancate code e ritardi, e non si può dire che il problema di software causa di tutto sia stato pienamente risolto si stanno riducendo. In una nota, Poste Italiane spiega che ieri negli uffici, il cui orario di apertura è stato prolungato, sono state eseguite circa «7 milioni di operazioni postali e finanziarie eseguite oggi negli uffici postali», tra cui 250mila pensioni pagate e 1,7 milioni di bollettini di conto corrente.

# ALCUNI EVENTI

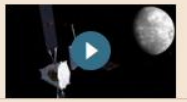
OSSERVATORI.NET digital innovation

MAXI-INTRUSIONE INFORMATICA

## UniCredit, violati i dati di 400mila clienti. «Password al sicuro»

26 giugno 2017

VIDEO



20 ottobre 2018
Partita la missione BepiColombo in viaggio verso Mercurio

I PIÙ LETTI DI TECNOLOGIA

1. IL RAPPORTO | 22 ottobre 2018
Crolla la rapidità di diffusione del web nel mondo. Qualcosa è andato storto

2. LA RECENSIONE | 22 ottobre 2018

Maxi intrusione informatica in Italia ai danni di UniCredit. La banca ha comunicato di aver subito una intrusione informatica con accesso non autorizzato a dati di clienti italiani relativi solo a prestiti personali. Tale accesso - precisa l'istituto - è avvenuto attraverso un partner commerciale esterno italiano. Secondo le risultanze della banca, una prima violazione sembra essere avvenuta nei mesi di settembre e ottobre 2016, mentre è stata appena individuata una seconda intrusione avvenuta nei mesi di giugno e luglio 2017.

REUTERS World Business Markets Politics TV

Imprisoned In Myanmar | Energy & Environment | Brexit | North Korea | Charged: The Future of Autos | Future of Money | Breakingviews

## Italy's UniCredit reveals data attack involving 400,000 clients

Paola Arosio, Gianluca Semeraro

2 MIN READ

MILAN (Reuters) - Suspected hackers have accessed client data of Italy's biggest lender, UniCredit (CRDI.MI), in two attacks in the past 10 months and affected about 400,000 Italian customers, the most serious data breach ever reported by a major Italian lender.

# TECNOLOGIE EMERGENTI, QUANTO FIDARSI?

OSSERVATORI.NET digital innovation

LA STAMPA TECNOLOGIA

SEZIONI

TEMPI MODERNI

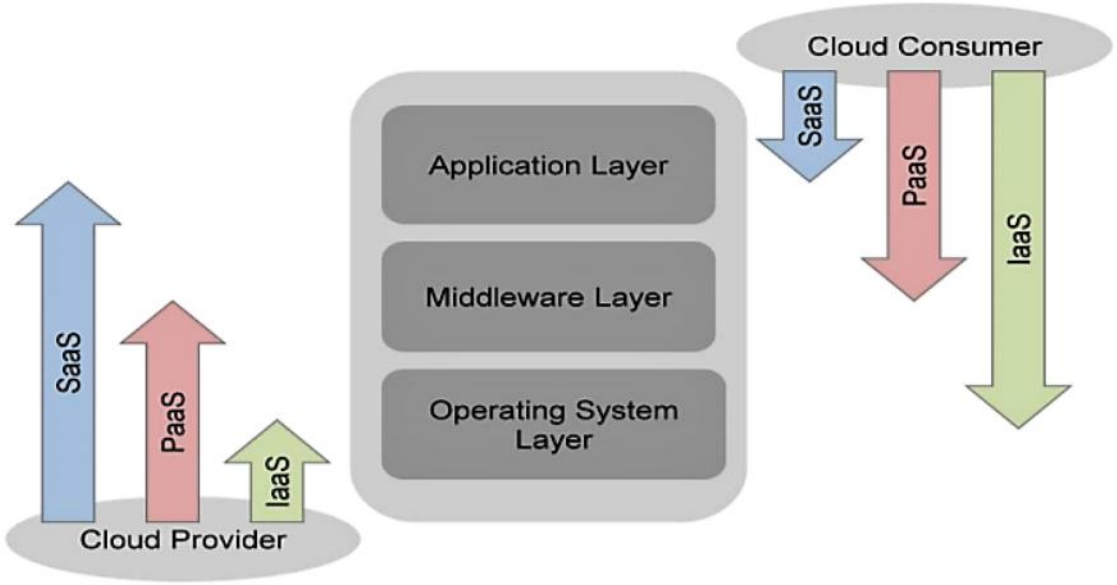
Piccoli spiritisti crescono con la tavola Ouija della Hasbro, ma è polemica sui rischi

ANDREA CIONCI

## Una vulnerabilità di Ethereum congela centinaia di milioni di dollari

La falla è stata rilevata su Multi-sig wallet, una tecnologia utilizzata per gestire le transazioni con la criptovaluta Ether

# CAMBI DI PARADIGMA




Fonte: NIST Cloud Computing Reference Architecture, September 2011
https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505

*« Through 2022, at least 95% of cloud security failures will be the customer's fault (Gartner 2020 10 top predictions) »*

# *CONTRATTI DI FORNITURA: GLI IMPATTI DEL GDPR*

# FORMALIZZAZIONE E LA REPOSANBILITA' SOLIDALE TRA CONTROLLER E PROCESSOR: COME CAMBIA IL RAPPORTO TRA CLIENTI E FORNITORI

- Accresciuta **attenzione** alle tematiche contrattuali anche sotto il profilo della normazione degli obblighi e dei ruoli privacy
- Difficoltà a **comprendere ed allocare**:
  - Le responsabilità per la **gestione della sicurezza**;
  - La **valutazione di adeguatezza** delle misure a protezione dei dati.
- Difficoltà a comprendere **cosa sia negoziabile** e cosa debba essere preteso
- Proliferazione di **clausole di manleva**
- Dubbi su come **attuare concretamente taluni requisiti** imposti dall'art. 28 (es. nell'ambito dei servizi cloud)

# I CONTENUTI CHE IL GDPR PREVEDE PER IL CONTRATTO

Il GDPR, ai sensi dell'art. 28, individua **due casi** in cui i reciproci obblighi intercorrenti tra *Data Controller* e *Data Processor*, relativamente all'esternalizzazione del trattamento dei dati personali, devono essere formalizzati:

- laddove il *Data Controller* affidi uno **specifico trattamento** di dati personali al *Data Processor*;

- laddove il *Data Processor* intenda ricorrere ad **un altro responsabile** del trattamento per l'esecuzione di **specifiche attività** di trattamento per conto del Titolare.

# I CONTENUTI CHE IL GDPR PREVEDE PER IL CONTRATTO

Il comma 3 dell'art. 28 GDPR prevede che:

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

Inoltre, la normativa (al comma 9 dell'art. 28) stabilisce le modalità con cui deve essere formalizzato l'accordo:

**Contratto o altro atto giuridico,** il quale dovrà essere stipulato in **forma scritta**, anche in **formato elettronico**

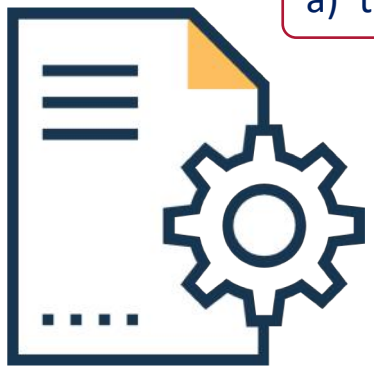
# I CONTENUTI CHE IL GDPR PREVEDE PER IL CONTRATTO

Il riferimento voluto da parte del Legislatore europeo con l'indicazione di «**altro atto giuridico**» lascia intendere che i rapporti e gli obblighi reciproci possono essere anche formalizzati con la **lettera di nomina a responsabile esterno** disciplinata, ai sensi dell'art. 29 del D.Lgs. 196/2003 ("Codice Privacy"), purché siano indicati i contenuti richiesti e previsti dal GDPR.

La lettera di **nomina** non è più facoltativa, ma **obbligatoria** per il Data Controller che decide di esternalizzare il trattamento.

# I CONTENUTI CHE IL GDPR PREVEDE PER IL CONTRATTO

L'accordo intercorrente tra *Data Controller* e *Data Processor* dovrà prevedere requisiti particolari e specifici, in particolare, l'accordo vincolante per il *Data Processor* dovrà indicare:



a) trattare i dati solo su istruzioni documentate del Titolare

b) assicurare che gli incaricati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza

c) adottare tutte le misure tecniche e organizzative ritenute adeguate per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 sulla base degli elementi indicati in cima

d) assistere il Titolare con adeguate misure per «dar seguito alle richieste per l'esercizio dei diritti dell'interessato»;

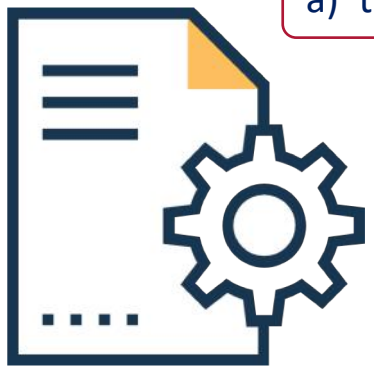
e) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile (il quale, in talune circostanze, è l'unico soggetto in grado di rilevare un *data breach*)

f) cancellare tutti i dati personali o restituire le copie esistenti alla cessazione delle funzioni di Responsabile

g) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi e collaborazione alle attività di revisione, comprese le ispezioni del Titolare (o soggetto da questi incaricato)

# I CONTENUTI CHE IL GDPR PREVEDE PER IL CONTRATTO

L'accordo intercorrente tra *Data Controller* e *Data Processor* dovrà prevedere requisiti particolari e specifici, in particolare, l'accordo vincolante per il *Data Processor* dovrà indicare:



a) trattare i dati solo su istruzioni documentate del Titolare

**b) assicurare che gli incaricati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza**

**c) adottare tutte le misure tecniche e organizzative ritenute adeguate per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 sulla base degli elementi indicati in cima**

**d) assistere il Titolare con adeguate misure per «dar seguito alle richieste per l'esercizio dei diritti dell'interessato»;**

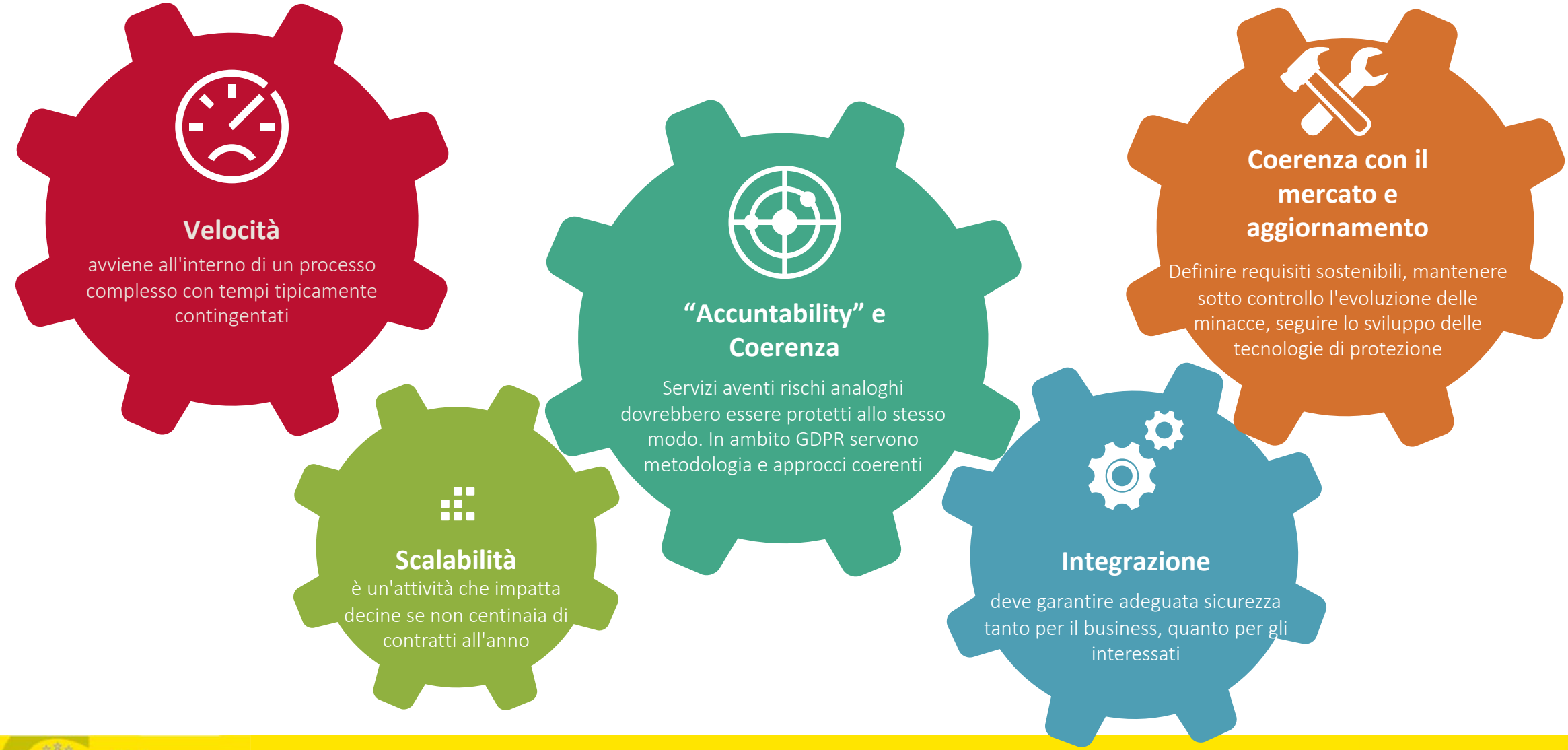
**e) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile (il quale, in talune circostanze, è l'unico soggetto in grado di rilevare un *data breach*)**

f) cancellare tutti i dati personali o restituire le copie esistenti alla cessazione delle funzioni di Responsabile

g) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi e collaborazione alle attività di revisione, comprese le ispezioni del Titolare (o soggetto da questi incaricato)

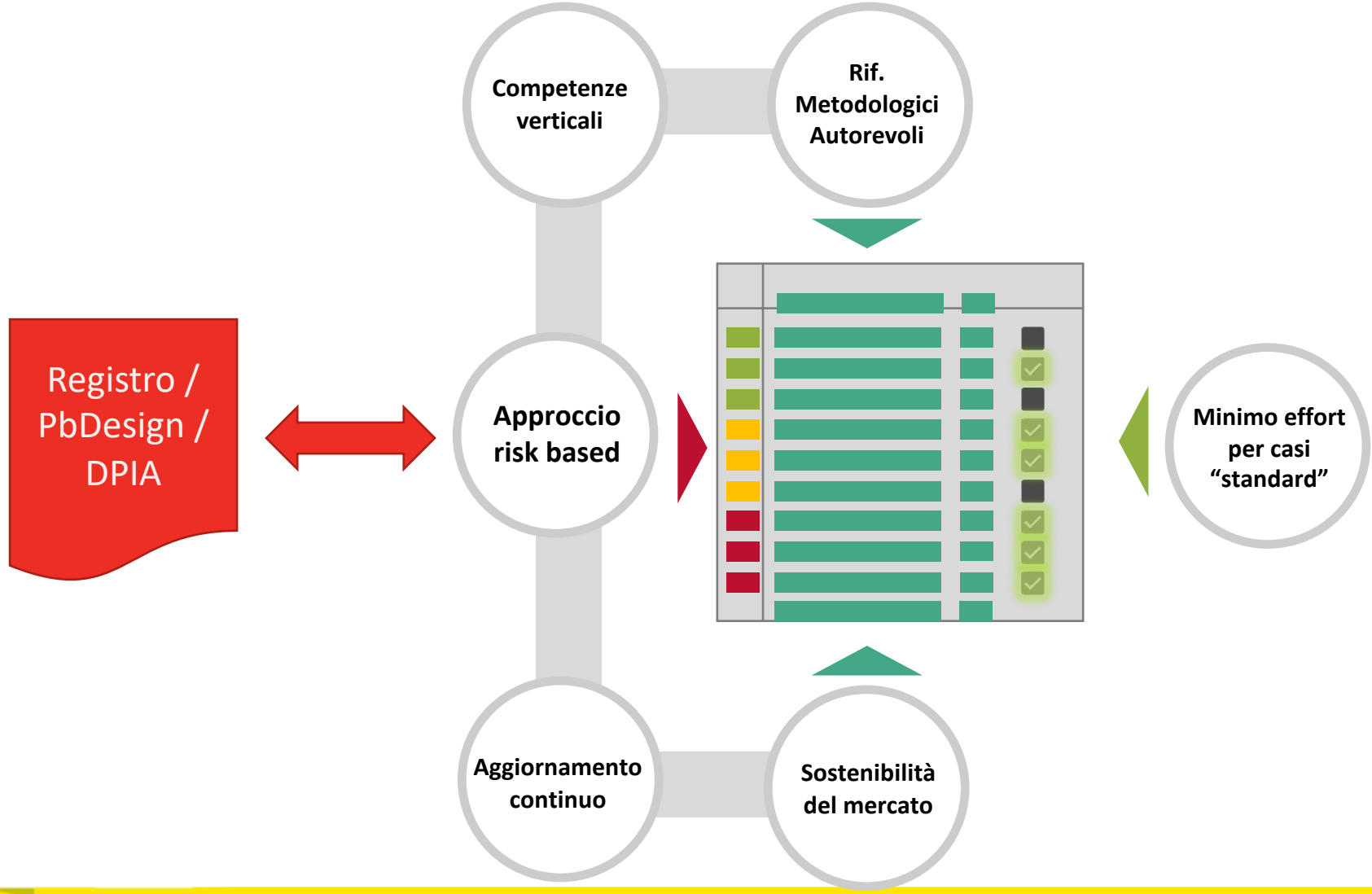
# ELEMENTI DI ATTENZIONE

- La definizione di misure e requisiti di **sicurezza** in ambito contrattuale, dovrebbe prevedere, quindi:



# ELEMENTI DI ATTENZIONE

## MODELLO DI GESTIONE DELLE CLAUSOLE DI SICUREZZA NELL'AMBITO DEI CONTRATTI



# I CONTENUTI CHE IL GDPR PREVEDE PER IL CONTRATTO

Tenendo conto della natura del trattamento e delle informazioni a sua disposizione, il *Data Processor* ha l'obbligo di assistere il *Data Controller*:

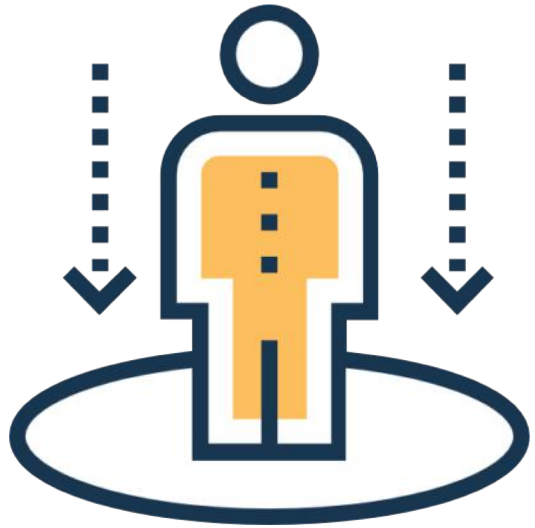
- **nell'assicurare protezione ai dati** attraverso misure tecniche ed organizzative adeguate, ai sensi dell'articolo 32 del Regolamento;
- **nel notificare all'Autorità eventuali *data breaches* occorsi, ai sensi dell'articolo 33 del Regolamento;**
- nel **comunicare agli interessati** gli eventuali *data breaches* occorsi, nei casi previsti dall'articolo 34 del Regolamento;
- **nell'effettuare la valutazione di impatto** richiesta dall'articolo 35 del Regolamento;
- nel **consultare l'Autorità**, qualora la valutazione di impatto effettuata indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
- **mettere a disposizione** del Data Controller tutte le informazioni necessarie a dimostrare il rispetto degli obblighi a cui è tenuto.

# POSSIBILITÀ DI DESIGNARE SUB-PROCESSORS (ART. 28 CO. 2 E 4)

Il Data Processor può **ricorrere ad un altro Data Processor** («*subprocessor*») previo consenso scritto, specifico o generale, del Data Controller, **imponendogli gli stessi obblighi** su cui è soggetto il primo

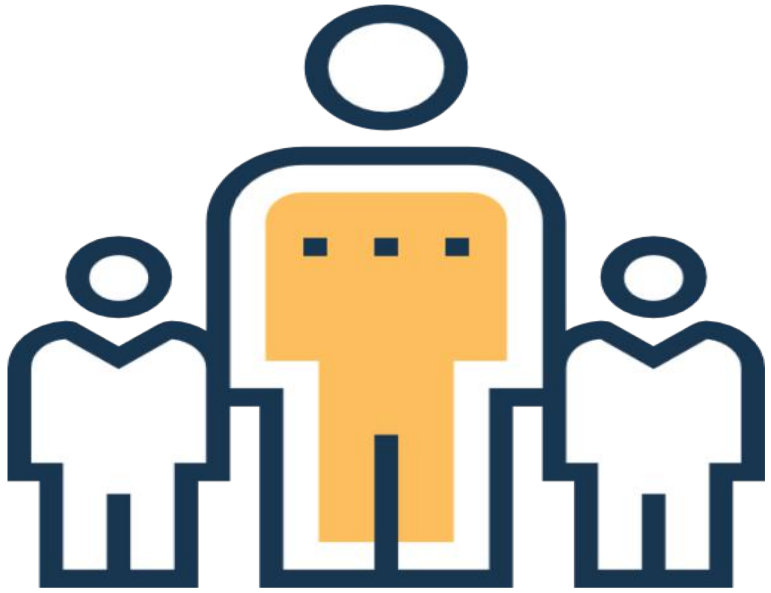
ciò significa che la designazione del secondo Data Processor debba contenere tutti gli elementi di cui all'art. 28.3 .

Novità più significativa dell'istituto in esame



Anche il subprocessor deve fornire al primo responsabile «**garanzie**» **sufficienti** per mettere in atto misure tecniche ed organizzative adeguate

# SUB-PROCESSOR

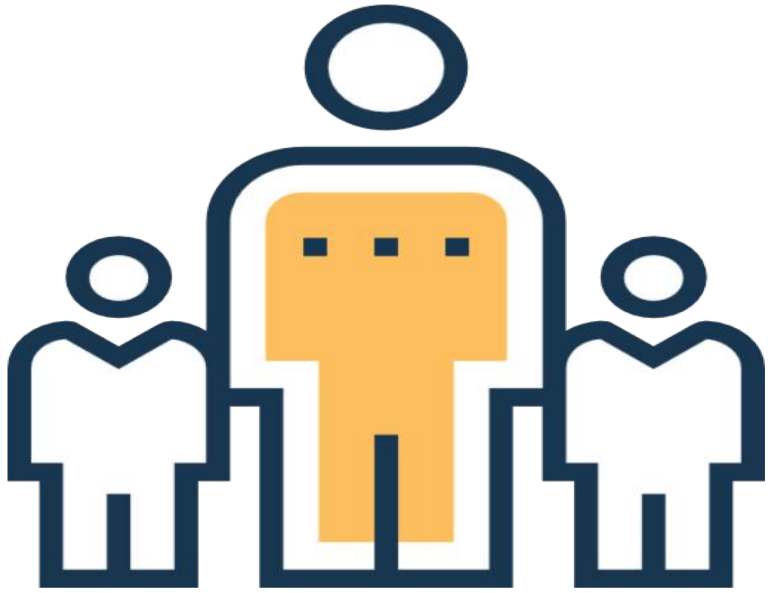


Se il **consenso** a ricorrere ad un sub-processor è **generico**, il Data Processor deve **informare** il **Data Controller** di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di sub-responsabili.

IN MODO DA

Consentire al **Data Controller** di **opporsi** a tali modifiche

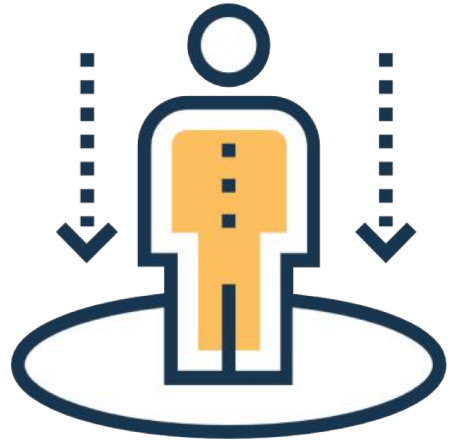
# SUB-PROCESSOR



Il Data Processor dovrà imporre al proprio subresponsabile, mediante un contratto o un altro atto scritto gli stessi obblighi di cui all'art. 28.3 del GDPR contenuti nell'accordo tra il primo ed il titolare del trattamento, in particolare sotto il profilo delle misure di sicurezza adeguate al trattamento.

# RESPONSABILIZZAZIONE DEL PRIMO DATA PROCESSOR RISPETTO ALLA PROPRIA FILIERA

Il **primo Data Processor** (e non il Data Controller) rimane comunque **pienamente responsabile,** sia per *culpa in eligendo* che per *culpa in vigilando,* in caso di **inadempimenti** da parte del sub-processors in materia di protezione dei dati.



# *LE RESPONSABILITÀ E GLI OBBLIGHI DEL DATA CONTROLLER*

# LE RESPONSABILITÀ DEL DATA CONTROLLER

In relazione alla **responsabilità** che spetta al *Data Controller*, questo dovrà assicurarsi di ricorrere ad un soggetto terzo che presenti **garanzie adeguate**.

Recita l'art. 28, co. 1, del GDPR:

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

# LE RESPONSABILITÀ DEL DATA CONTROLLER

Individuare un soggetto che, **in termini di conoscenza specialistica, affidabilità e risorse, garantisca la possibilità di mettere in atto misure di sicurezza che soddisfino le esigenze di protezione dei dati personali.**

Verificare il ricorso, da parte del responsabile, a **codici di condotta o meccanismi di certificazione** può certamente costituire un **indice di garanzia** ed **affidabilità.**

**attraverso questa verifica il *Data Controller* può dimostrare il rispetto degli obblighi relativi alla diligenza "in eligendo" dei propri Data Processor**

# LE RESPONSABILITÀ DEL DATA CONTROLLER

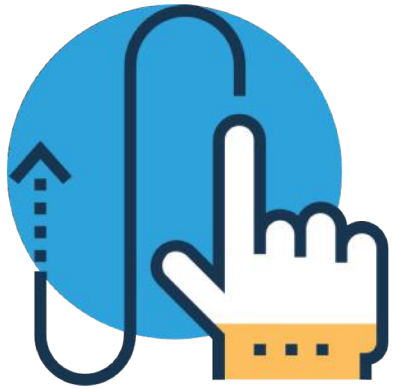
l'**obbligo** di stipulare **ACCORDI SCRITTI** con il Data Processor attraverso i quali fornire **dettagliate istruzioni** in ordine alle modalità del trattamento

Resta inteso che l'eventuale **esternalizzazione** totale o parziale del trattamento **non implica alcuna deresponsabilizzazione per il *Data Controller***, il quale risponderà direttamente, per ciò che ad egli compete, in ordine alla conformità normativa delle proprie attività di trattamento dati

# LE RESPONSABILITÀ E GLI OBBLIGHI DEL DATA PROCESSOR

# RESPONSABILITÀ PER IL DATA PROCESSOR

Di regola la responsabilità per i danni derivanti dal trattamento è allocata in capo al *Data Controller* (che decide **finalità e mezzi del trattamento**), in quanto il Responsabile svolge solo **attività strumentali** nei **limiti dell'incarico** che ha ricevuto e **deve agire secondo le istruzioni del Data Controller** (e di impartirle ai propri collaboratori).



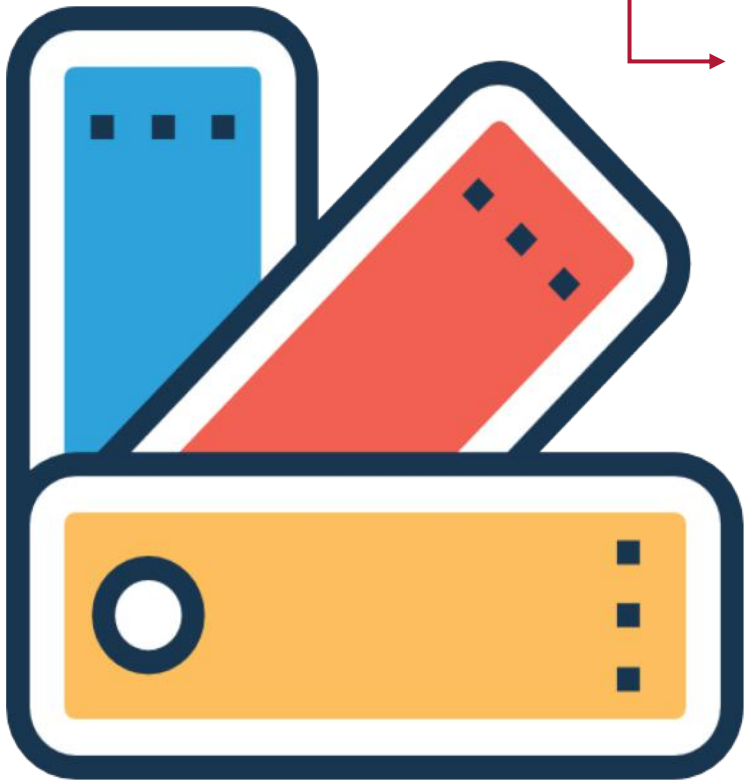
**TUTTAVIA**

Il GDPR prevede dei casi specifici, individuati dall'art. 82 co. 2, in cui il *Data Processor* è tenuto al risarcimento.

# RESPONSABILITÀ PER IL DATA PROCESSOR

Il ***Data Processor*** risponde non solo se **ha agito in modo difforme o contrario rispetto alle** legittime **istruzioni del titolare**

ma anche se **non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili**



RESPONSABILITÀ SOLIDALE

Qualora più titolari o responsabili oppure entrambi siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni **titolare** o **responsabile** è responsabile **in solido** per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato

# OBBLIGHI DIRETTI DEL DATA PROCESSOR

Tra gli adempimenti direttamente posti in capo al responsabile, la cui violazione può dar luogo a responsabilità diretta del responsabile, si segnalano in particolare:

- Gli obblighi relativi al subappalto
- Gli obblighi di cooperazione con l'Autorità di controllo
- Gli obblighi relativi alla sicurezza
- L'obbligo di istituire ed aggiornare il registro delle attività di trattamento effettuate per conto del titolare
- L'obbligo di informare senza giustificato ritardo il titolare di ogni evento di violazione della sicurezza di cui sia venuto a conoscenza
- L'obbligo di nominare un DPO laddove richiesto per legge
- L'obbligo di designare un proprio rappresentante, laddove richiesto per legge

# *CONSEGUENZE SANZIONATORIE*

# CONSEGUENZE SANZIONATORIE

Il Regolamento prevede, ai sensi dell'art. 83, la possibilità per le Autorità nazionali di irrogare **sanzioni fino a € 20.000.000** o, in caso di «*undertaking*», **al 4% del fatturato globale annuo**, a seconda di quale risulti la sanzione più elevata.

Le sanzioni più alte si applicano, *inter alia*, a:

- violazioni dei principi del trattamento, incluse le condizioni per il consenso;
- violazione dei diritti degli interessati;
- inosservanza delle norme in tema di trasferimento internazionale dei dati

**Le sanzioni più basse** (**fino a €. 10.000.000** o al **2% del fatturato globale annuo**) si applicano, fra l'altro, a

- **violazione delle obbligazioni di *controllers* e *processors*, incluso gli obblighi di sicurezza e *data breach notification*.**

Il concetto di '***undertaking***' potrebbe mettere a rischio le *revenues* di un gruppo societario, anche se non tutte le società del gruppo sono responsabili della violazione.
Le sanzioni non sono infatti imposte in riferimento alle revenues della specifica società sanzionata, ma alle revenues di un "undertaking". Ciò, in estrema sintesi, potrebbe comportare che, se la società sanzionata è parte di un "undertaking", il 4% o 2% saranno calcolati sul fatturato totale annuo dell'intera undertaking e non il fatturato totale annuo della sola specifica società sanzionata.

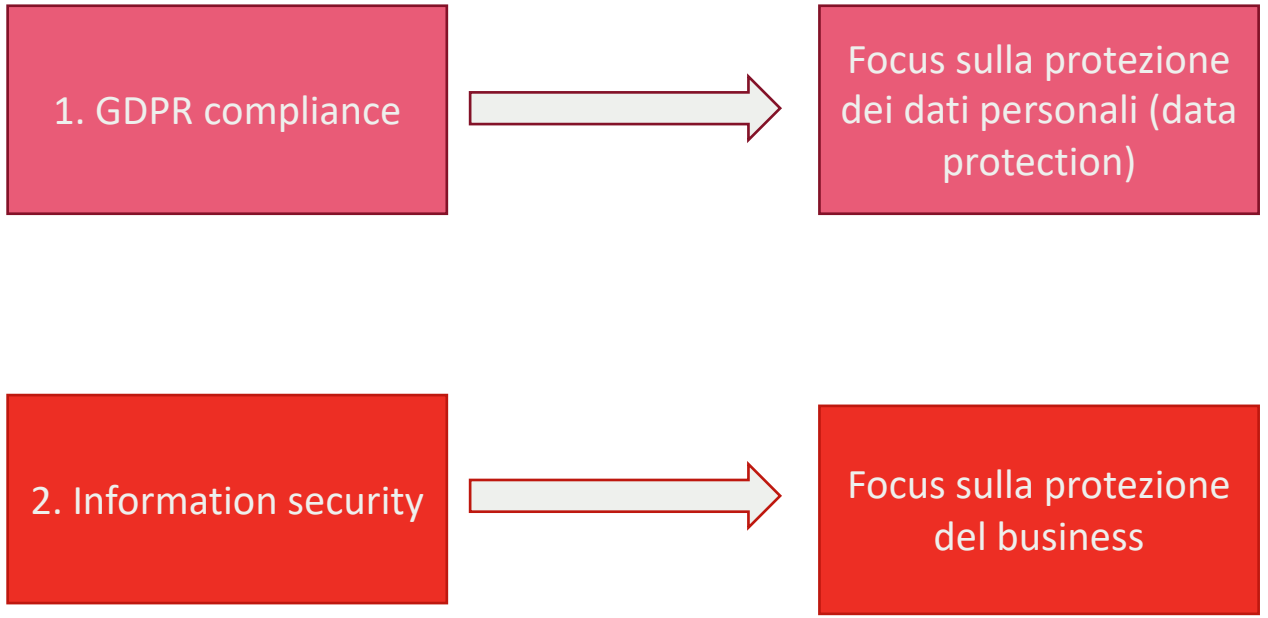
# SANZIONI AMMINISTRATIVE GDPR – FINO A 10 MLN, 2%

OSSERVATORI.NET digital innovation

| RIFERIMENTO | INADEMPIMENTO | SANZIONE |
|---|---|---|
| **Consenso dei minori (art. 8)** | Mancata verifica del consenso da parte del Titolare della responsabilità genitoriale sul minore | **Fino a 10.000.000 €, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.** |
| **Trattamento che non richiede l'identificazione (art. 11)** | Conservazione, acquisizione o trattamento di ulteriori informazioni per identificare l'interessato anche se le finalità non richiedono o non richiedono più la sua identificazione | |
| **Privacy by design/default (art. 25)** | Mancata protezione dei dati fin dalla progettazione (privacy by design) e/o mancata protezione per impostazione predefinita (privacy by default) | |
| **Contitolarità (art. 26)** | Assenza di accordo interno tra i contitolari e/o mancata determinazione, in modo trasparente, delle rispettive responsabilità in riferimento al GDPR | |
| **Rappresentanti non stabiliti in UE (art. 27)** | Mancata designazione per iscritto, da parte del titolare/responsabile, di un rappresentante nell'UE | |
| **Data Processor (art. 28)** | Mancato rispetto di quanto previsto ai sensi dell'art. 28 | |

# UNIRE I PUNTINI… DALLA COMPLIANCE ALLE OPPORTUNITÀ DI SICUREZZA

*Due differenti approcci: possono convergere?*



# 1. GDPR COMPLIANCE: PRIVACY FRAMEWORKS

OSSERVATORI.NET digital innovation

**Risk assessment**

c) implements **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk pursuant to art. 32

| | | | | |
|---|---|---|---|---|
| L | Security policy and procedures for the protection of personal data | A.1 | The organization should document its policy with regards to personal data processing as part of its information security policy. | A.5 Security policy |
| M | Security policy and procedures for the protection of personal data | A.3 | The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties | A.5 Security policy |
| H | Security policy and procedures for the protection of personal data | A.6 | The security policy should be reviewed and revised, if necessary, on a semestral basis. | A.5 Security policy |

ANSI/ISA 624

«Handbook on Security of Personal Data Processing"

43

- ISO/IEC 29100:2017
- ISO/IEC 29101:2013
- ISO/IEC 29134:2017
- ISO/IEC 29151:2017
- ISO/IEC 29190:2015
- ISO/IEC 29191:2012

Practice UNI/PdR 43:2018 «Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR) - Gestione e monitoraggio dei dati personali in ambito ICT»

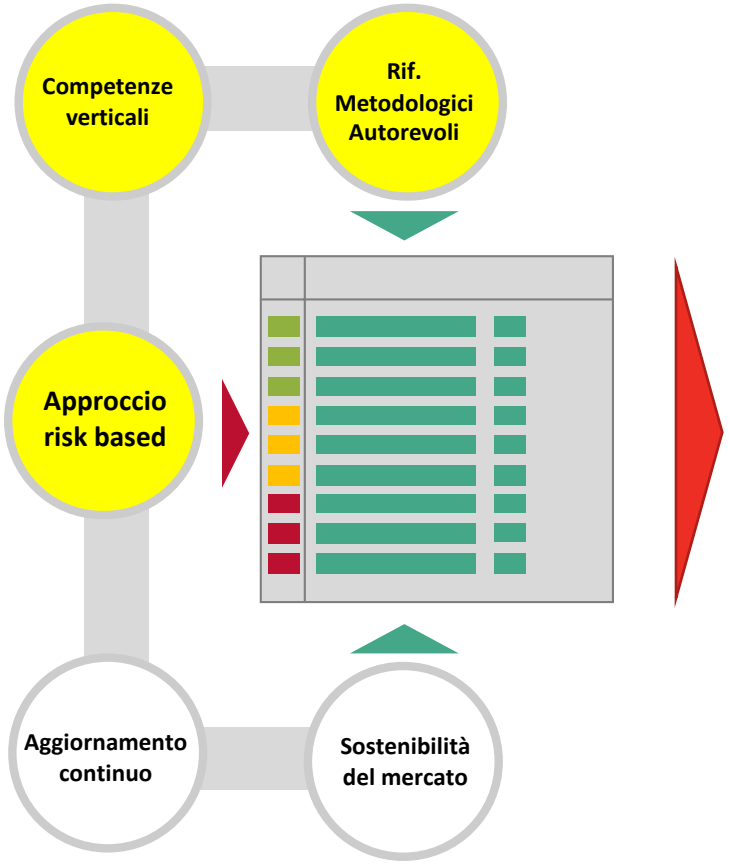
# 2. INFORMATION SECURITY: QUALE FRAMEWORK SCEGLIERE?

OSSERVATORI.NET digital innovation

| | |
|---|---|
| ISO 20000-1:2011 (Delivery of IT service) | ISO 22301:2012 (Business Continuity) |
| ISO:IEC 27000 series (Information Security Management) | NIST Cyber Security Framework |
| ANSI/ISA 62443 (Security for industrial automation and control systems) | PCI-DSS 3.2 (Electronic payments) |
| EBA / Bank of Italy Circulars | Technical Assessment (e.g. Critical Security Controls, OWASP Testing Guide, NIST 800-53A, etc.) |
| Customised models based on the Client's business | Other applicable standards (e.g. Cobit, CSA, HIPAA, etc.) |

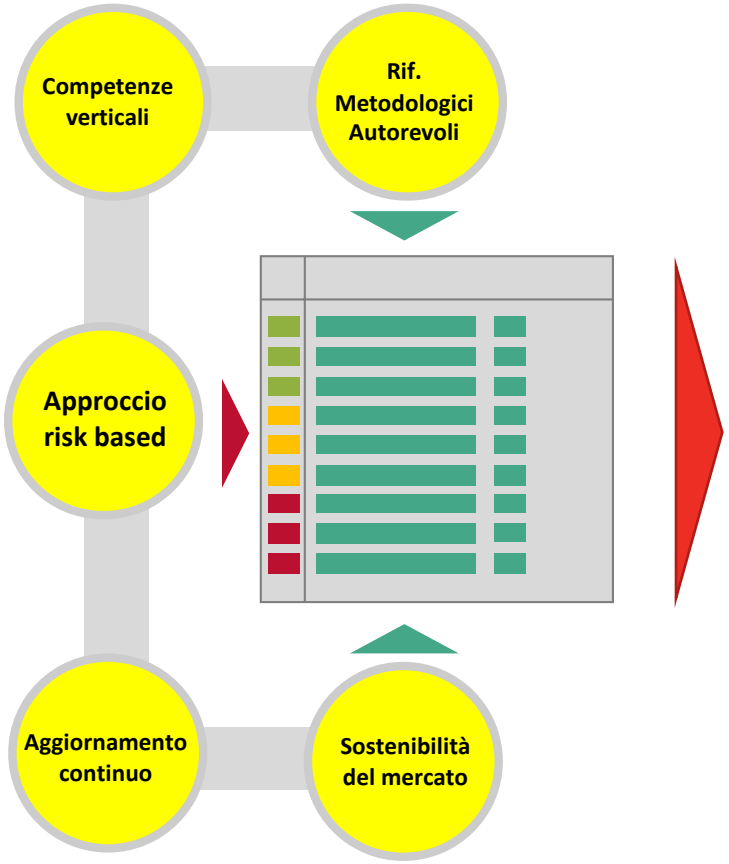
# 3. UN MODELLO INTEGRATO:

# 3.A Definizione della libreria di **minacce** e valutazione (potenziale)



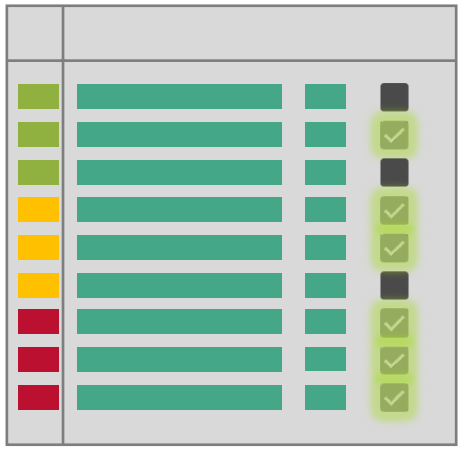

| | Data Protection | | | Information Security | | | Global Vision | | |
|---|---|---|---|---|---|---|---|---|---|
| | C | I | A | C | I | A | C | I | A |
| Threat1 | | | | | | | | | |
| Threat1 | | | | | | | | | |
| Threat1 | | | | | | | | | |

# 3.B Definizione dei **controlli** per mitigare le minacce




| | Kind | Source | C | I | A |
|---|---|---|---|---|---|
| C1 | ORG | GDPR art. 32<br>ISO 27002 A.8.3.3<br>NIST AC-2<br>CSA IAM-04 | X | | |
| C2 | TECH | | | X | X |
| C3 | TECH | | | X | |

# 3.C Calcolo del rischio residuo (inclusi i controlli)



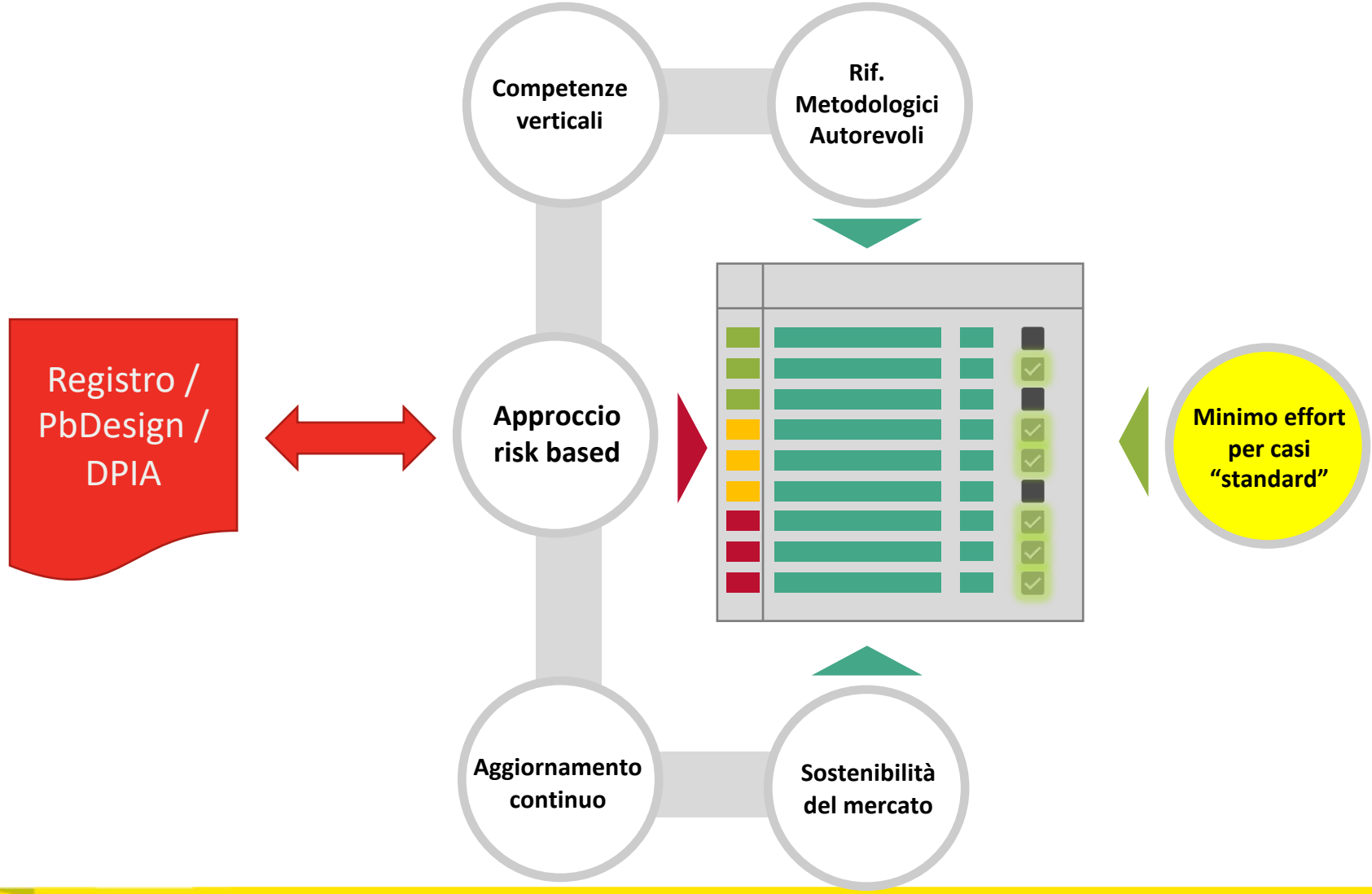
| | Data Protection | | | Information Security | | | Global Vision | | |
|---|---|---|---|---|---|---|---|---|---|
| | C | I | A | C | I | A | C | I | A |
| Threat1 | | | | | | | | | |
| Threat1 | | | | | | | | | |
| Threat1 | | | | | | | | | |

È “soddisfacente”? E’ **adeguato**?

# Risk appetite (obiettivo di rischio) e adeguatezza

- Definire il risk appetite
  - “soddisfacente” significa che siete preparati a accettare tale rischio, considerando “pros and cons”
- Come comunicare e dove migliorare la valutazione?
- E se l’obiettivo di rischio viene “superato”?
- E l’adeguatezza?

# ADEGUATEZZA: GESTIONE, EFFICIENZA, EFFICACIA



# *Grazie per l'attenzione!*

designed by {Prosymbols} from Flaticon