LA DATA GOVERNANCE NEL GDPR. PAROLA CHIAVE: ACCOUNTABILITY

Dalla data protection alla data governance: il Regolamento UE 679/2016

30 novembre 2017
Università degli Studi di Milano
Aula 2018 - – via Festa del Perdono, 7 – Milano

JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

(Cons. 9) «Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE **non ha impedito la frammentazione** dell'applicazione della protezione dei dati personali nel territorio dell'Unione, **né ha eliminato l'incertezza giuridica** o la **percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche**. (…). Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE».

- **il 72%** degli internauti europei nutre preoccupazione per la quantità di dati richiesti online
- **sette persone su dieci** sono preoccupate del fatto che i loro dati vengano usati per finalità diverse da quelle per cui erano stati raccolti
- **una persona su sette** sottolinea che in tutti i casi dovrebbe essere richiesta l'esplicita autorizzazione dell'interessato prima della raccolta e del trattamento dei dati (*dati Eurobarometro riportati dal Garante Europeo)*
- **il 25%** degli internauti europei si è trovato nel corso del 2015 ad affrontare problemi di sicurezza informatica comuni, quali virus, violazioni dei propri dati personali, perdite economiche (*Fonte Eurostat)*
- **entro il 2020** saranno collegati a Internet **6 miliardi di elettrodomestici** (*Fonte: IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, studio per la Commissione europea)*

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com
JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

DIGITAL SINGLE MARKET: LE DIMENSIONI E LE PROSPETTIVE

European Commission

Digital Single Market

Commission strengthens trust and gives a boost to the data economy

Building the European Data Economy

The digital revolution is built on data

Data is a new type of economic asset, which is rapidly becoming vital in the global economy. Most economic ac will depend on data within a few years → This provides great opportunities for all sectors, including:

health · food security · resource efficiency · energy management · intelligent transport · smart cities · smart agriculture · civil protecti

Access to large and diverse datasets is a prerequisite for innovation.

Agriculture weather or soil data used by farmers

Energy data from smart meters for the development of infrastructure: patterns of consumption show where energy demand is likely to grow/fall

Manufacturing sensor data used to predict maintenance needs

Geo-spatial data data from satellites, e.g. earth observation and meteorological data

The EU wants to make data available to businesses and citizens.

The datasets resulting from technologies such as the Internet of Things are large and complex → It is currently too difficult to process such data with the traditional data management tools and methods → New technological advances on data analytics, processing and storage will make this possible.

The potential of the data-driven economy

- Big data is an essential resource for economic growth, job creation and societal progress.
- The value of the EU data economy was €272 billion in 2015, close to 1.9% of GDP.
- With adapted policy and legal solutions, its value could more than double by 2020.

The way forward

The Commission is entering an intense dialogue with Member States and other stakeholders to develop the most appropriate actions to reap the full potential of the European data economy. It also proposes to interested Member States to explore data related issues in a real-life cross-border situation, building on several ongoing connected cars projects.

Public consultation on building European data Economy: https://ec.europa.eu/digital-single-market/news-redirect/52039
Public consultation on Liability for Defective Products: http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=9048

Why we need a Digital Single Market

315 million Europeans use the Internet every day

A Digital Single Market can create up to **€415 billion** in additional growth, **hundreds of thousands** of new jobs, and a **vibrant knowledge-based society**

But obstacles remain to unlock this potential...

The Digital Market today is made up

by **national** online services (42%)
and **US-based** online services (54%)
EU cross-border online services represent only 4%

3 Creating a European Digital Economy and society with growth potential

Big data and cloud

Digital data stored in cloud:
2013: 20% - 2020: 40%

The use of big data by the top 100 EU manufacturers could lead to **savings worth €425 billion**

Studies estimate that, by 2020, big data analytics could boost EU economic growth by an additional **1.9%**, equalling a **GDP increase of €206 billion**

An inclusive e-society

Almost half the EU population (**47%**) is not properly digitally skilled, yet in the near future, **90% of jobs** will require some level of digital skills

A strategy of 'digital by default' in the public sector could result in around **€10 billion of annual savings**

Addressing current barriers

- **Unjustified restrictions**: Increasing number of barriers to the movement of data around the EU.
- **Legal uncertainties**: Limited access to data generated by new technologies because there are no clear rules for sharing this data.

1. Free Flow of Data

Due to digitisation, more and more goods and services depend on the availability and innovative use of data.

PROBLEM	EXAMPLE:	SOLUTION:
Legal or administrative restrictions on data location may prevent the private and public sectors from having a good choice of data services.	It is difficult for a small provider of digital invoicing and accountancy services to offer competitive prices in several markets within the EU, because it would have to arrange data storage or processing capacity in every Member State.	Removing data localisation restrictions except if they are required for national security and similar objectives. Data does not have to be stored in one specific Member State. Free flow of data is enshrined in the General Data Protection Regulation. All existing rights and obligations on data protection and privacy will be applied.

2. Data access and transfer

PROBLEM	EXAMPLE:	SOLUTION:
Companies tend to analyse data only in-house, data sharing with other stakeholders remains uncommon. There are no comprehensive policy frameworks for the economic utilisation, re-use and tradability of non-personal and anonymised data generated by machines and sensors.	Farming machines need 90 minutes to map yields from one hectare. A specialized provider, who operates drones and uses data from farms, can do the same in 10 minutes.	Improve access to non-personal/ anonymous machine-generated data. Facilitate and incentivise data sharing and re-use. Protect investments and assets. Minimise lock-in efects.

3. Legal responsibility for data based products

PROBLEM	EXAMPLE:	SOLUTION:
Due to many market players providing different elements for very complex systems like the Internet of Things, it is difficult to identify who is responsible. This legal uncertainty affects innovation and uptake of data-driven products and services.	In the case of a fire, a smart home security system should contact the fire service and the owner, unlock doors and switch on security lights. But if it fails, it can be difficult to establish the part of the system which did not work and who may be liable for any damage.	Defining responsibilities according to how a risk is generated or how it is managed (a so-called risk-generating or risk-management approach); considering voluntary or mandatory insurance schemes.

4. Data portability, interoperability and standards

PROBLEM	EXAMPLE:	SOLUTION:
Personal data portability is a right. Non-personal data portability can be complicated or costly in practice, including for data stored in cloud services.	A business using cloud services cannot easily extract or port their data (e.g. to switch providers) because it might be too expensive or technically complicated.	Reducing switching costs to stimulate an innovation-friendly environment; developing rights to data portability; improving technical interoperability and data standards.

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com
JACOBACCI AVVOCATI · AVOCATS A LA COUR · ABOGADOS

NECESSARIA LA CREAZIONE DI UN CLIMA DI FIDUCIA PER CONSENTIRE LO SVILUPPO DELL'ECONOMIA DIGITALE IN TUTTO IL MERCATO INTERNO
(Parlamento Europeo)

SUPERAMENTO EFFETTIVO DELLA FRAMMENTAZIONE NORMATIVA

+

CAPACITA DI ADATTAMENTO DELLE NORME AI MUTAMENTI TECNOLOGICI E STRATEGICI DEL MERCATO

=

AGGIORNAMENTO NORMATIVO

«Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, **data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno**. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche» *(cons. 7).*

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

UNO SVILUPPO SOSTENIBILE PER L'ECONOMIA DIGITALE:
IL CONTESTO E LE DINAMICHE DI RIFERIMENTO

GARANZIA DI CONTROLLO DEI PROPRI DATI ⟷ **SVILUPPO ECONOMICO**

«Il trattamento dei dati personali dovrebbe essere **al servizio dell'uomo**. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va **considerato alla luce della sua funzione sociale** e va **contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità**. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.» *(Cons. 4)*

PROTEZIONE DEI DIRITTI FONDAMENTALI DELL'INDIVIDUO	SVILUPPO ECONOMICO
AUTODETERMINAZIONE	LIBERTA D'ESPRESSIONE
PROTEZIONE DEI DATI PERSONALI	LIBERTA D'INFORMAZIONE
DIRITTO ALL'IDENTITÀ PERSONALE	LIBERTA DI INIZIATIVA EPROPAGANDA POLITICA
UGUAGLIANZA E NON DISCRIMINAZIONE…	LIBERTA D'INIZIATIVA ECONOMICA E COMMERCIALE…

CRITERIO DI PROPORZIONALITA

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com
JACOBACCI
AVVOCATI · AVOCATS A LA COUR · ABOGADOS

UNO SVILUPPO SOSTENIBILE PER L'ECONOMIA DIGITALE: IL SISTEMA GDPR

JAdp - DATA PROTECTION

Obbligo di **DIMOSTRARE** la conformità del trattamento al GDPR e l'efficacia delle misure attuate

RAFFORZAMENTO DELL'ASSUNZIONE DI RESPONSABILITÀ ATTIVA DEL TITOLARE ED ESTENSIONE A TUTTI I SOGGETTI ATTIVI DEL TRATTAMENTO:

ACCOUNTABILITY

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

Organismi comunitari, Stati membri, Autorità di controllo nazionali collaborano per la progressiva definizione **di regole di dettaglio**

GDPR = NORME UNIFORMI IN UNA GRIGLIA DINAMICA

Il potere riconosciuto all'interessato: non solo PROTEZIONE ma GESTIONE dei propri dati

CONTROLLO EX ANTE = CONSENSO INFORMATO

CONTROLLO EX POST = RIMEDI ESERCITABILI PRESSO IL TITOLARE

Privacy by design
e by default
Semplificazione
Effettività

INTERAZIONE tra DIRITTI FONDAMENTALI in un continuo **BILANCIAMENTO** regolato dal CRITERIO DI PROPORZIONALITÀ

Finalità
Necessità
Pertinenza

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

ACCOUNTABILITY: ARCHITETTURA

JAdp - DATA PROTECTION

Obbligo di **ATTUARE** **misure** tecnologiche ed organizzative **adeguate ed efficaci** di prevenzione del **rischio di violazione dei diritti e libertà fondamentali degli individui**

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

Valutazione del rischio

Rischio attenuabile

Rischio non attenuabile

Individuazione di strumenti per attenuare il rischio

Adozione codici condotta approvati

certificazione

Nomina DPO

Adozione eventuali misure minime per speciali categorie di trattamenti

Pratiche improntate a privacy by design e by default

Obbligo di consultare l'Autorità di controllo

Procedimentalizzazione della valutazione del rischio e delle azioni conseguenti

Obbligo di **DIMOSTRARE** la **conformità** del trattamento al Regolamento e **l'efficacia** delle misure

Formalizzazione delle regole e dei processi che governano le azioni di prevenzione

Art. 24 GDPR

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento («ACCOUNTABILITY»)

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com
JACOBACCI AVVOCATI • AVOCATS A LA COUR • ABOGADOS

ACCOUNTABILITY: RESPONSABILITÀ GENERALE BASATA SULLA PREVENZIONE DEL RISCHIO

➢ RESPONSABILITÀ DELLA PROGETTAZIONE, ATTUAZIONE E CONTROLLO DEL TRATTAMENTO:

prevenzione adeguata ed efficace del rischio

RAFFORZAMENTO DELL'ASSUNZIONE DI RESPONSABILITÀ ATTIVA DEL TITOLARE ED ESTENSIONE – ANCHE IN TERMINI DI RISARCIMENTO E DI SANZIONI – A TUTTI I SOGGETTI ATTIVI DEL TRATTAMENTO:

ACCOUNTABILITY come *compliance* dinamica, costruita «su misura»

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

misure concrete ed efficaci per

- "attuare i principi di protezione dei dati" *(art. 25 – Privacy by design e by default)*
- "garantire un livello di sicurezza adeguato al rischio" *(art. 32 - Sicurezza del trattamento)*

da individuare **autonomamente** in rapporto alle **peculiarità del caso specifico (valutazione del rischio)**

➢ RESPONSABILITÀ DELLA VIOLAZIONE DEL GDPR

Responsabilità risarcitoria: imputazione individuale

Rafforzamento del sistema sanzionatorio (sanzioni «*effettive, proporzionate e dissuasive*»)

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

L'ALTRA FACCIA DELL'»ACCOUNTABILITY»: LA RESPONSABILITÀ PER LA NON CONFORMITÀ DEL TRATTAMENTO AL GDPR

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

L'ALTRA FACCIA DELL'«ACCOUNTABILITY» LE SANZIONI AMMINISTRATIVE PECUNIARIE: gli importi

Sanzioni amministrative pecuniarie fino a € **10.000.000** o – per le imprese – fino al **2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore

ARTICOLI **8** (consenso dei minori), **11, 25** (privacy by design e by default), **26, 27, 28, 29** (norme su titolari e responsabili), **30** (registri attività trattamento), da **31 a 34** (sicurezza e disclosure di data breach)**, 35 e 36** (valutazione d'impatto e consultazione preventiva), **da 37 a 39** (norme sul DPO)**, 42 e 43 (certificazioni)**

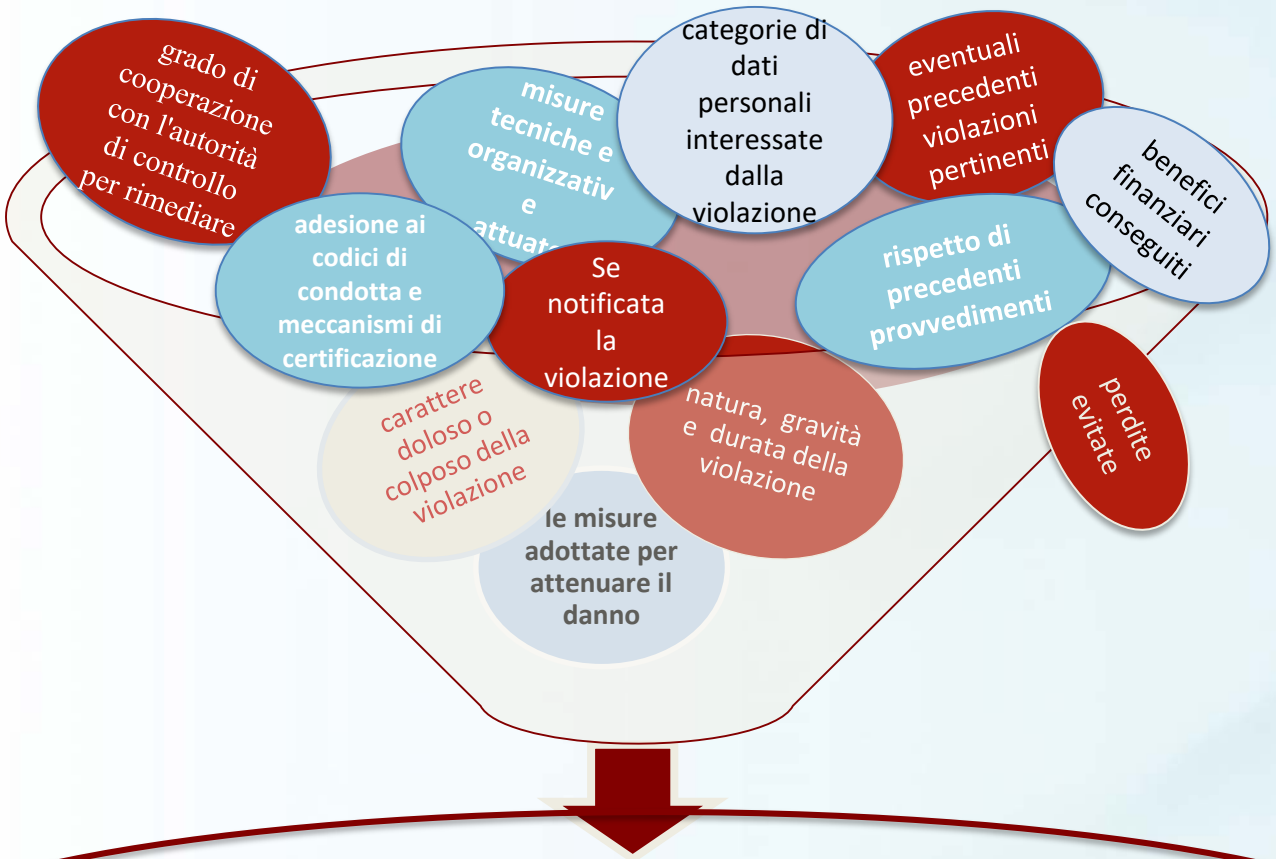
Sanzioni amministrative pecuniarie fino a € **20.000.000** o – per le imprese – fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore

ARTICOLI **5, 6, 7, 9** (principi di base e consenso), da **12 a 22** (informativa e diritti degli interessati), da **44 a 49** (trasferimenti transfrontalieri), inosservanza di ordini dell'Autorità

Articolo 84 GDPR - Sanzioni
1. Gli Stati membri stabiliscono le norme relative ***alle altre sanzioni per le violazioni del presente regolamento*** *(…)*

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

L'ALTRA FACCIA DELL'«ACCOUNTABILITY» LE SANZIONI AMMINISTRATIVE PECUNIARIE: i criteri (Art. 83, comma 2)



Art. 83, comma 1 GDPR: «Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso **effettive, proporzionate e dissuasive.**»

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

LA RESPONSABILITA RISARCITORIA NEL GDPR: introduzione del criterio soggettivo

Art. 15 Codice Privacy: «***Chiunque cagiona danno*** *ad altri per effetto del trattamento di dati personali* ***è tenuto al risarcimento*** *ai sensi dell'articolo 2050 del codice civile.*»

Art. 82, comma 1 GDPR:

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

- IMPUTAZIONE **GENERALE:**

l'assenza di richiamo a una richiesta nei confronti di **specifici** soggetti di condotte **predeterminate** rende difficoltosa la concreta riconduzione della responsabilità

- responsabilità **oggettiva:**

non è esclusa dalla prova dell'adempimento puntuale delle norme ma solo dalla «*prova di avere adottato tutte le misure idonee a evitare il danno*» (art. 2050 Cod. Civ.)

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

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

MA QUAL È IL PERIMETRO DELLA VIOLAZIONE RILEVANTE AI SENSI DEL GDPR?

JAdp - DATA PROTECTION

«2. Il presente regolamento protegge **i diritti e le libertà fondamentali delle persone fisiche, in particolare** il diritto alla protezione dei dati personali» (art. 1.2 GDPR)

«Quando un tipo di trattamento, (…) può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, …» (art. 35.1 GDPR)

(*Cons. 75*) **I rischi per i diritti e le libertà delle persone fisiche**, aventi probabilità e gravità diverse, **possono derivare da trattamenti di dati personali SUSCETTIBILI DI CAGIONARE un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo**; (…).

«In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente (…), **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**.» (Art. 33.1 GDPR)

«Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo» (Art. 34.1 GDPR)

"8/ In the context referred to above (*la valutazione del rischio, ndr*), the scope of "the rights and freedoms" of the data subjects **primarily concerns the right to privacy** but **may also involve other fundamental rights** such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion" *(op. WP218).*

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com
JACOBACCI AVVOCATI • AVOCATS A LA COUR • ABOGADOS

LA RESPONSABILITA RISARCITORIA NEL GDPR: conseguenze pratiche

DIFESA IN GIUDIZIO

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

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

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

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

Art. 32 - Sicurezza del trattamento

Tenendo conto **DELLO STATO DELL'ARTE E DEI COSTI DI ATTUAZIONE**, (…) il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio»

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

PREVENIRE IL RISCHIO DI VIOLAZIONE: esempi di azioni e processi

INDIVIDUARE
- i rischi

VALUTARE
- le probabilità di accadimento
- i danni che ne possono derivare

DESCRIVERE
- le possibili soluzioni
- i costi
- gli impatti organizzativi
- le motivazioni delle scelte
- i rischi residui

PROCESSI

- definizione degli obiettivi secondo principi di liceità, trasparenza, pertinenza e non eccedenza del trattamento, esattezza dei dati trattati, trasparenza e semplificazione dell'informativa, effettività della tutela, privacy by design e by default
- individuazione nei trattamenti progettati dell'esistenza di rischi di violazione dei diritti degli interessati e conseguente valutazione della relativa natura, probabilità e gravità nonché degli eventuali correttivi o della opportunità di consultazione preventiva dell'Autorità di controllo nel caso di rischio non attenuabile
- adeguata selezione dei fornitori (prestatori di servizi/list broker)
- selezione dati e relative fonti e valutazione della conformità ai trattamenti progettati
- Individuazione della base giuridica dei trattamenti e sviluppo di proprie informative e consensi
- individuazione di ruoli e responsabilità nel trattamento, all'interno e all'esterno dell'azienda del titolare
- **formalizzazione dei ruoli e responsabilità nel trattamento (es. contratti con responsabili / contitolari del trattamento**

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

LA RESPONSABILITA GENERALE: formalizzazione dei ruoli

GLI ATTORI DEL TRATTAMENTO

Un titolare assume responsabilità per qualsiasi trattamento che effettua direttamente, con altri o che altri effettuino per suo conto, ma a ciascuno degli attori è riconosciuta anche responsabilità autonoma

TITOLARE ⟷ accordo interno ⟷ **CONTITOLARE**

CONTRATTO O ALTRO ATTO GIURIDICAMENTE VINCOLANTE, SCRITTO, CONTENENTE OBBLIGHI E GARANZIE DI CONFORMITÀ AL REGOLAMENTO: CONTRATTO INDIVIDUALE O BASATO SU CLAUSOLE CONTRATTUALI TIPO

RESPONSABILE

SUB - RESPONSABILE

SUB - RESPONSABILE

RESPONSABILE

SUB - RESPONSABILE

RESPONSABILE

SUB - RESPONSABILE

SUB - RESPONSABILE

- Autorizzazione scritta del titolare
- Atto giuridicamente vincolante contenente gli stessi obblighi e garanzie di conformità al GDPR contenuti nella nomina rilasciata dal titolare

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

L'AUTONOMIA DEL RESPONSABILE PER LA VIOLAZIONE DEL GDPR: gli obblighi dedotti nel contratto

NOMINA DEL RESPONSABILE
Atto giuridicamente vincolante

→ indicazione dettagliata:
- ✓ delle circostanze del trattamento affidato
- ✓ degli obblighi e garanzie indicati dal Regolamento

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

Art. 28 c. 3 GDPR:

(…) **Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento**:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento (…);
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate (…) al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti (…);
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

L'AUTONOMIA DEL RESPONSABILE PER LA VIOLAZIONE DEL GDPR: gli obblighi di legge

JAdp - DATA PROTECTION

NOMINA DEL RESPONSABILE
Atto giuridicamente vincolante

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

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

ALCUNI OBBLIGHI DIRETTI DEL RESPONSABILE

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

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

Il responsabile ha contemporaneamente

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

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

JACOBACCI AVVOCATI • AVOCATS A LA COUR • ABOGADOS

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

GARANZIE

CARATTERISTICHE DI PROCESSO

Accordo quadro

MANLEVE

CLAUSOLE CONTRATTUALI TIPO

FUNZIONI E RUOLI DELLE PARTI

Rapporti con l'interessato

PIA

Dimostrazione della conformità

Strumenti per la conformità del trattamento

ACCOUNTABILITY

DEFINIZIONE FORMALE DI CRITERI PER LA CONFORMITA

TRADUZIONE IN BEST PRACTICE E PROCEDURE DOCUMENTALMENTE FORMALIZZATE

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com

Grazie dell'attenzione

Maria Roberta Perugini

Partner

Studio Legale Jacobacci e Associati

CONTEMPORARY IP

Via Senato 8, 20121 Milano ITALY
Phone: +39 02 76022513
Fax : +39 02 781958

JACOBACCI
AVVOCATI • AVOCATS A LA COUR • ABOGADOS

Avv Maria Roberta Perugini
mrperugini@jacobacci-law.com