CARONE · MINNECI & PARTNERS

STUDIO LEGALE

Il Regolamento UE 2016/679
e la gestione della privacy negli studi professionali

Milano, 10 aprile 2018

Relatore | **Avv. Vincenzo Diego Cutugno**

INDICE

1. Introduzione al GDPR
2. Disposizioni generali - Principi
3. Diritti degli interessati
4. Il Responsabile della Protezione Dati (DPO)
5. Accountability
6. Sicurezza
7. Data breach
8. Certificazioni e Codici di condotta
9. Sanzioni
10. Conclusioni
11. Q/A

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

1.

INTRODUZIONE AL GDPR

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

1.

INTRODUZIONE AL REGOLAMENTO

1. Gli Studi professionali come qualunque titolare del trattamento dei dati sono soggetti al Regolamento

2. Gli Studi professionali possono svolgere un ruolo divulgativo, di supporto e assistenza per i clienti

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

1.

INTRODUZIONE AL REGOLAMENTO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RIFERIMENTI NORMATIVI

- La direttiva 95/46/CE (c.d. «*direttiva madre*»)
- Recepita dalla Legge 675/1996, poi abrogata dal Codice della Privacy (D. lgs 2003/196)
- Il 27 aprile 2016 viene emanato il **Regolamento UE n. 2016/679** (General Data Protection Regulation «**GDPR**»)
- In Italia, sostituisce il Codice della Privacy

1.

INTRODUZIONE AL REGOLAMENTO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RATIO DELL'INTERVENTO NORMATIVO

- **Obsolescenza**:
  - ✓ Adeguamento normativo
  - ✓ Sono trascorsi oltre 20 anni (corrispondenza con fax, no e-mail, limitato internet)
  - ✓ Oggi «big data» e «internet of things»
- **Uniformità**: armonizzazione, stessa disciplina giuridica a livello comunitario: da costo burocratico superfluo a fattore di competitività
- **Libera circolazione dei dati**:
  - ✓ Non può essere limitata né vietata per motivi attinenti alla tutela non armonizzata (Cons 9)

1.

INTRODUZIONE AL REGOLAMENTO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RATIO DELL'INTERVENTO NORMATIVO

Importanza della circolazione dei dati

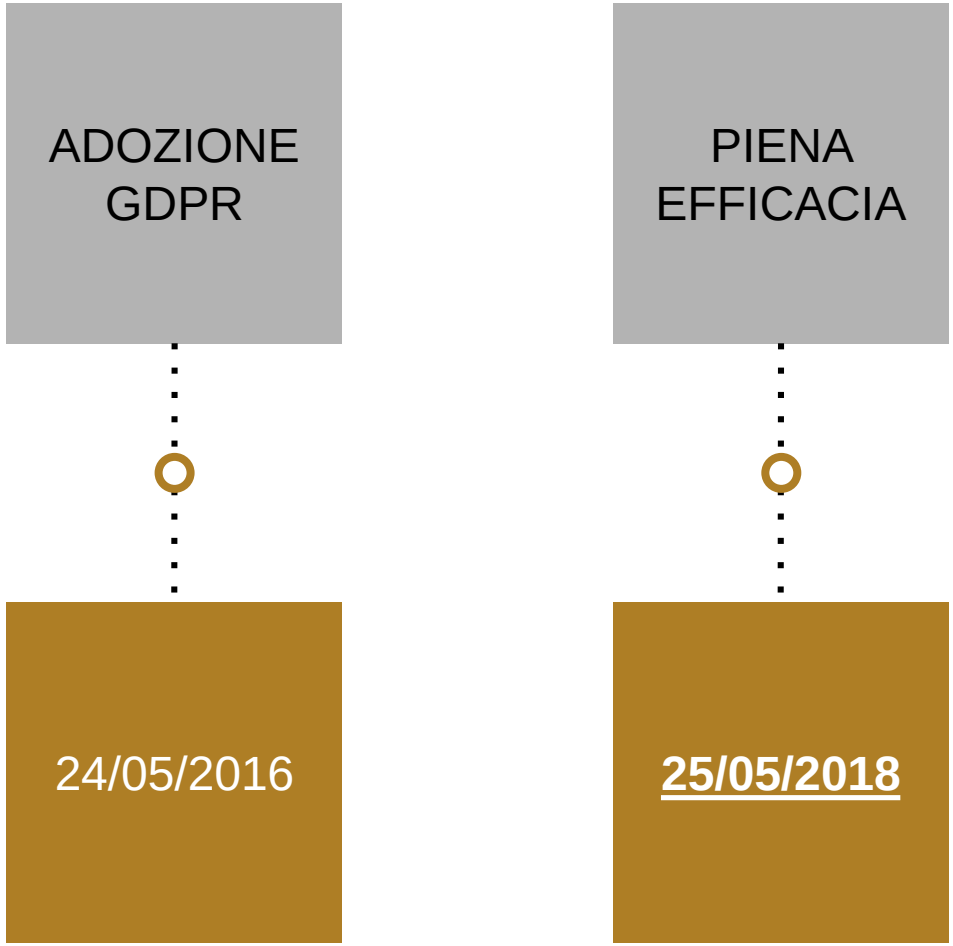
- Economica: il contributo mercato unico digitale funzionante potrebbe apportare 415 miliardi di euro all'anno all'economia europea (Commissione). Servizi digitali retribuiti con dati, importanza economica della profilazione
- Politica: il caso Cambridge Analytica (dati personali di 87 Mln di utenti), incide sullo svolgimento di elezioni e consultazioni democratiche. Oggi incontro Garanti Europei
- Sicurezza: hackers, cyber-crime, terrorismo

1.

INTRODUZIONE AL REGOLAMENTO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

AGENDA / KEY DATES



1.

INTRODUZIONE AL REGOLAMENTO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

ACCOUNTABILITY O PRINCIPIO DI RESPONSABILIZZAZIONE «Principio dei principi»

Rispetto degli altri principi e capacità di dimostrare di averli osservati

1. **Adottare** «***misure tecniche e organizzative*** *adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente»* al Regolamento
2. **dimostrare** «***la conformità*** *delle attività di trattamento*» con il GDPR
3. **dimostrare** l'«***efficacia delle misure***»

1.

INTRODUZIONE AL REGOLAMENTO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

PRINCIPALI NOVITÀ

- Nuovi diritti (portabilità, oblio, limiti alla profilazione)
- Accountability
- Privacy by design – Privacy by default
- Meno adempimenti formali: no notificazione al Garante (**Registro**)
- Valutazione dei rischi (**Risk assessment**)
- Valutazione d'impatto (**Impact assessment**)
- **Data breach**
- **Sanzioni** (pecuniarie amministrative, penali)
- DPO, registri, codici etici, certificazioni

2.

DISPOSIZIONI GENERALI - PRINCIPI

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

2.

DISPOSIZIONI GENERALI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

1. **Tutela delle persone** (fisiche) rispetto al trattamento dei loro dati personali

2. La **libera circolazione** dei dati

2.

DISPOSIZIONI GENERALI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

AMBITO DI APPLICAZIONE

- **Territorio**:
  - ✓ Se il **titolare o il RDT** è stabilito sul **territorio dell'UE**, indipendentemente se il trattamento è effettuato fuori dall'UE
  - ✓ Se il l'interessato si trova nell'UE:
    - i. **offerta di beni e servizi** anche senza corrispettivo; o
    - ii. il trattamento riguarda il **monitoraggio del comportamento** dell'interessato all'interno dell'UE (**profilazione**)

2.

DISPOSIZIONI GENERALI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

AMBITO DI APPLICAZIONE

- **Materia**:
  i. Dati **automatizzati**
  ii. **Non automatizzati,** se tenuti in **archivio**
  iii. Esclusi i trattamenti:
    a) manuali e non strutturati
    b) di persone decedute
    c) dati anonimi o anonimizzati
    d) persone fisiche per scopi personali
    e) attività che non rientrano nel diritto UE (sicurezza nazionale) o politica estera o difesa
    f) Autorità per attività di prevenzione, indagine, accertamento, perseguimento reati, esecuzione di sanzioni penali, sicurezza pubblica

2.

DISPOSIZIONI GENERALI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

FASE TRANSITORIA

- Le decisioni della Commissione e le autorizzazioni del Garante rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate
- Consenso prestato a norma della direttiva 95/46/CE, non occorre un nuovo consenso, se è **conforme** al Regolamento.

2.

PRINCIPI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

PRINCIPI

- Liceità, correttezza e trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza
- Minimizzazione della conservazione
- Integrità e sicurezza

2.

PRINCIPI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

PRINCIPI

- **Liceità e correttezza**:
  i. lecito - base giuridica
  ii. corretto – buona fede
- **Trasparente**: informazioni facilmente accessibili e comprensibili (linguaggio semplice e chiaro)
- **Limitazione delle finalità**: determinate, esplicite e legittime. Ulteriori finalità, nuovo consenso
- **Minimizzazione**: dati pertinenti, adeguati e non eccedenti rispetto alle finalità (qualitativa e quantitativa)

2.

PRINCIPI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

PRINCIPI

- **Esattezza**: dati esatti e aggiornati (diritto di rettifica)
- **Minimizzazione della conservazione**: conservati solo per il tempo necessario a conseguire le finalità (cancellazione periodica)
- **Integrità e sicurezza**: garantire adeguata sicurezza e riservatezza dei dati (pseudonimizzazione, cifratura)

2.

PRINCIPI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

TRATTAMENTO LECITO

2.

PRINCIPI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CONDIZIONI DI LICEITÀ

- **Consenso**: atto **positivo inequivocabile** con il quale l'interessato manifesta l'intenzione **libera**, **specifica**, **informata** e **inequivocabile** di accettare il trattamento dei dati personali – **preventivo e revocabile**
- **Obbligazione contrattuale o precontrattuale**: un rapporto civilistico che implica il trattamento dei dati. Il consenso al trattamento può ritenersi «assorbito» (*e.g.* preventivo)
- **Obbligo di legge**: al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri

2.

PRINCIPI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CONDIZIONI DI LICEITÀ

- **Salvaguardia di interessi vitali**: dell'interessato o di un'altra persona fisica (*e.g.* epidemie, emergenze umanitarie, catastrofi di origine naturale e umana), se il trattamento non può essere fondato su un'altra base giuridica
- **Pubblico interesse o esercizio pubblici poteri**: di cui è investito il titolare del trattamento, il diritto dell'Unione o degli Stati membri può (deve) stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile

2.

PRINCIPI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CONDIZIONI DI LICEITÀ

- **Legittimo interesse**:

1. lecito, in accordo con i principi privacy;
2. bilanciato, non prevalgono gli interessi o i diritti e le libertà fondamentali dell'interessato
3. l'interessato è stato informato del legittimo interesse

Esempi

- ✓ relazione pertinente ed appropriata (cliente o dipendente)
- ✓ l'interessato può attendersi il trattamento (prevenzioni frodi, marketing diretto → se il titolare ha adottato le misure appropriate di protezione)
- ✓ per fini organizzativi e amministrativi, se titolare è parte di un gruppo

2.

PRINCIPI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CONDIZIONE DI LICEITÀ

CATEGORIE PARTICOLARI DI DATI (SENSIBILI)

dati che rivelano l'origine razziale o etnica, opinioni politiche, convinzioni religiose, filosofiche o appartenenza sindacale, dati sanitari, attinenti alla vita e orientamento sessuale, biometrici, genetici

TRATTAMENTO VIETATO

Salvo che:

a) consenso **esplicito**
b) obblighi diritto del lavoro o sicurezza sociale
c) interesse vitale dell'interessato o di un terzo (se interessato è incapace di prestare il consenso)
d) trattamenti sanitari
e) finalità di medicina preventiva
f) se il trattamento riguarda dati resi manifestamente pubblici dall'interessato
g) etc.

2.

DISPOSIZIONI GENERALI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CONSENSO

- Estesi i requisiti del consenso

- ✓ informato: preceduto da informativa
- ✓ libero: senza condizionamenti o vincoli
- ✓ specifico: un consenso per ogni finalità
- ✓ inequivocabile: certezza che sia stato prestato
- ✓ espresso: non vale silenzio assenso, inattività o preselezione
- ✓ esplicito: dati sensibili (no comportamento concludente)
- ✓ forma scritta: non è necessaria (forma libera), ma serve prova
- ✓ comprensibile, accessibile, chiaro, semplice
- ✓ revocabile: indicato nell'informativa

2.

DISPOSIZIONI GENERALI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CONSENSO

GDPR

Novità

- dati di contatto del **DPO**
- **durata** di conservazione
- diritto di proporre **reclamo**
- diritto di **portabilità**
- diritto di **revocare** il consenso in qualunque momento
- **legittimo interesse**
- **profilazione**
- qualunque informazione necessaria a garantire la legittimità del trattamento

3.

DIRITTI DEGLI INTERESSATI

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

3.

DIRITTI DEGLI INTERESSATI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

DIRITTI CONOSCITIVI E DI CONTROLLO

- **Diritti conoscitivi**:
  1. **informativa**: ricevere informazioni sul trattamento e sui dati (artt. 13 e 14)
  2. **accesso**: richiedere/ottenere tali informazioni (art.15)
  3. **violazioni**: ricevere informazioni su gravi anomalie del trattamento (art. 34)

- **Diritti di controllo**:
  1. **consenso**: autorizzare il trattamento (artt. 6.1.a), 9.2. a)
  2. **limitazione**: modificare il trattamento (art. 18)
  3. **revoca** consenso e **opposizione**: far cessare il trattamento (artt. 7.3 e 21)

3.

DIRITTI DEGLI INTERESSATI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

DIRITTI SUI DATI

- **Diritti sui dati**:
  1. **portabilità**: spostare complessi strutturati di dati (art. 20)
  2. **rettifica e integrazione**: modificare i dati (art. 16)
  3. **cancellazione/oblio**: eliminare i dati personali

Limiti alla Profilazione

non subire decisioni unicamente basate su trattamenti automatizzati (art. 22). Diritto volto ad evitare ricomposizioni arbitrarie di profili della persona sottratti al controllo da parte di quest'ultima

4.

IL RESPONSABILE DELLA PROTEZIONI DATI (DPO)

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RESPONSABILE PROTEZIONE DEI DATI

Artt. 37 – 39 Regolamento e Linee Guida del WP29

- È uno dei pilastri del principio di *accoutability*
- Responsabile della Protezione dei Dati o (Data Protection Officer «**DPO**») nomina obbligatoria o facoltativa (sempre consigliata)

Perché il DPO

- Rientra nelle misure di Accountability
- Facilita e controlla l'osservanza della normativa

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RESPONSABILE PROTEZIONE DEI DATI

- Professionista **esperto** in materia di privacy
- DPO non risponde direttamente per la violazione del GDPR (**responsabilità**)
- Responsabile per il rispetto della normativa sono il Titolare o RDT (art. 24)
- Titolare e RDT devono mettere il DPO in condizione di svolgere l'incarico
- Attenzione a non confondere il DPO con altre figure (Responsabile Protezione Dati, Consulente Privacy)

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

NOMINA OBBLIGATORIA

Art. 37

1. Trattamento svolto da autorità o organismo pubblico
2. **Attività principali** consistono in trattamenti che richiedono **monitoraggio regolare e sistematico** di interessati su **larga scala**
3. **Attività principali** consistono nel trattamento su **larga scala** di **categorie particolari** di dati o di dati relativi a **condanne penali e reati**

La decisione se nominare un DPO deve essere il frutto di una valutazione d'impatto documentata.
Per dimostrare che l'analisi ha preso in considerazione correttamente i fattori pertinenti

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

NOMINA OBBLIGATORIA

Art. 37

1. **Attività principali**: le attività primarie. Esulano le attività accessorie
2. **Larga scala**: una notevole quantità di dati a livello regionale, nazionale o sovranazionale e che possono incidere un vasto numero di interessati. Tenere conto di:
   a) **numero** di soggetti interessati
   b) diverse **tipologie** di dati
   c) la **durata** o la **persistenza**
   d) la **portata geografica**

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

NOMINA OBBLIGATORIA

Art. 37

3. **Monitoraggio**: monitoraggio del comportamento, incluse tutte le forme di tracciamento e profilazione
4. **Regolare**: continuo, ad intervalli definiti, ricorrente o perpetuo, intervalli costanti, costante o intervalli periodici
5. **Sistematico**: per sistema, predeterminato, organizzato o metodico, nell'ambito di un progetto complessivo di raccolta dati o di una strategia
6. **Categorie particolari**: «dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

DESIGNAZIONE

Art. 37

- Unico DPO per un gruppo imprenditoriale, purché sia facilmente raggiungibile (nell'esecuzione dei suoi compiti) da ciascuno stabilimento
- Qualità professionali: **conoscenza specialistica** della **normativa** e **prassi** privacy e capacità di assolvere i compiti:

  a) il livello di conoscenza deve essere **proporzionato** alla sensibilità, complessità e quantità di dati sottoposti a trattamento

  b) Conoscenza della normativa e prassi

  c) Integrità ed elevati standard deontologici

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

DESIGNAZIONE

Art. 37

- Può essere dipendente o designato con contratto di servizi
- Se DPO è una persona giuridica, tutti i soggetti che operano come DPO devono soddisfare i requisiti
- I dati di contatto devono essere resi pubblici e devono essere comunicati al Garante (per facilitare il contatto)

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RUOLO E GARANZIE

Art. 38

1. Deve essere **coinvolto** (tempestivamente ed adeguatamente) in tutte le questioni privacy
2. Deve **partecipare** regolarmente alle **riunioni** management di alto e medio livello
3. Deve **partecipare** ogni qualvolta sono assunte **decisioni** che impattano sulla privacy
4. Devono essergli fornite tutte le **informazioni** pertinenti
5. I **pareri** del DPO devono sempre essere tenuti in grande considerazione (motivare le ragioni di disaccordo)

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RUOLO E GARANZIE

Art. 38

6. Deve essere **consultato** tempestivamente in caso di **violazione** dei dati o altro incidente
7. Deve ricevere **supporto attivo** dal management e adeguato in termini di risorse finanziarie, organizzative e di personale
8. Non deve ricevere istruzioni (**autonomia**)
9. Riferisce direttamente al **vertice gerarchico**
10. **Non** può essere **rimosso** o **penalizzato** per l'adempimento dei propri compiti
11. Deve **evitare conflitti d'interessi**
12. Deve rispettare **segretezza e confidenzialità**

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

COMPITI

Art. 39

1. **Sorvegliare l'osservanza** del GDPR:
   a) Raccolta di informazioni per individuare i trattamenti
   b) Analisi e verifica della conformità dei trattamenti
   c) Informazione, consulenza e indirizzo
2. Supporto nello **svolgimento delle DPIA**:
   a) Se condurre DPIA
   b) Quale metodologia seguire
   c) Se condurre DPIA internamente o esternalizzarla
   d) Quale misure tecniche e organizzative adottare
   e) Correttezza della DPIA e se conclusioni corrette

4.

LE FIGURE DEL REGOLAMENTO: IL DPO

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

COMPITI

Art. 39

3. Cooperare con il Garante e **fungere da punto di contatto** con il Garante e gli interessati
4. Considerare i **rischi** inerenti al trattamento, tenendo in considerazione natura, ambito applicazione, contesto e finalità
5. Supportare alla tenuta del **registro dei trattamenti**

5.

ACCOUNTABILITY

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

5.

ACCOUNTABILITY
PRIVACY-BY-DESIGN
PRIVACY-BY-DEFAULT

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

ACCOUNTABILITY

- Mettere in atto misure tecniche e organizzative in grado di **garantire**, e **dimostrare**, **conformità** al Regolamento ed **efficacia delle misure** adottate (art. 24)
- **Onere della prova** a carico del soggetto attivo del trattamento
- Misure **adeguate** che tengano conto della **natura**, **dell'ambito di applicazione**, del **contesto**, e delle **finalità** del trattamento e del **rischio** per i diritti e le libertà (Cons. 74)
- **Valutazione di adeguatezza** (*ex ante*) e verifica **dell'efficacia** (*ex post*) → tramite audit e DPIA
- Vengono meno gli obblighi consultivi del Garante, salvo il caso di rischio elevato ineliminabile
- Garante monitora i livelli di conformità (intervento *ex post*)

5.

ACCOUNTABILITY

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

PRIVACY BY-DESIGN

- in fase di **sviluppo**, **progettazione**, **selezione** e **utilizzo di applicazioni, servizi e prodotti** ridurre al minimo il trattamento dei dati mediante politiche interne, misure tecniche e organizzative (es. pseudonimizzazione)
- sia nella **determinazione dei mezzi sia all'atto del trattamento**
- investimento iniziale per migliorare il potenziale sfruttamento dei dati raccolti garantendo *compliance*
- DP DESIGNER, soggetto incaricato della progettazione conforme al GDPR di tecnologie, processi, prodotti e servizi

5.

ACCOUNTABILITY

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

PRIVACY BY-DEFAULT

adottare misure tecniche e organizzative adeguate per garantire che siano trattati, per **impostazione predefinita**, **solo i dati necessari per specifica finalità di trattamento**

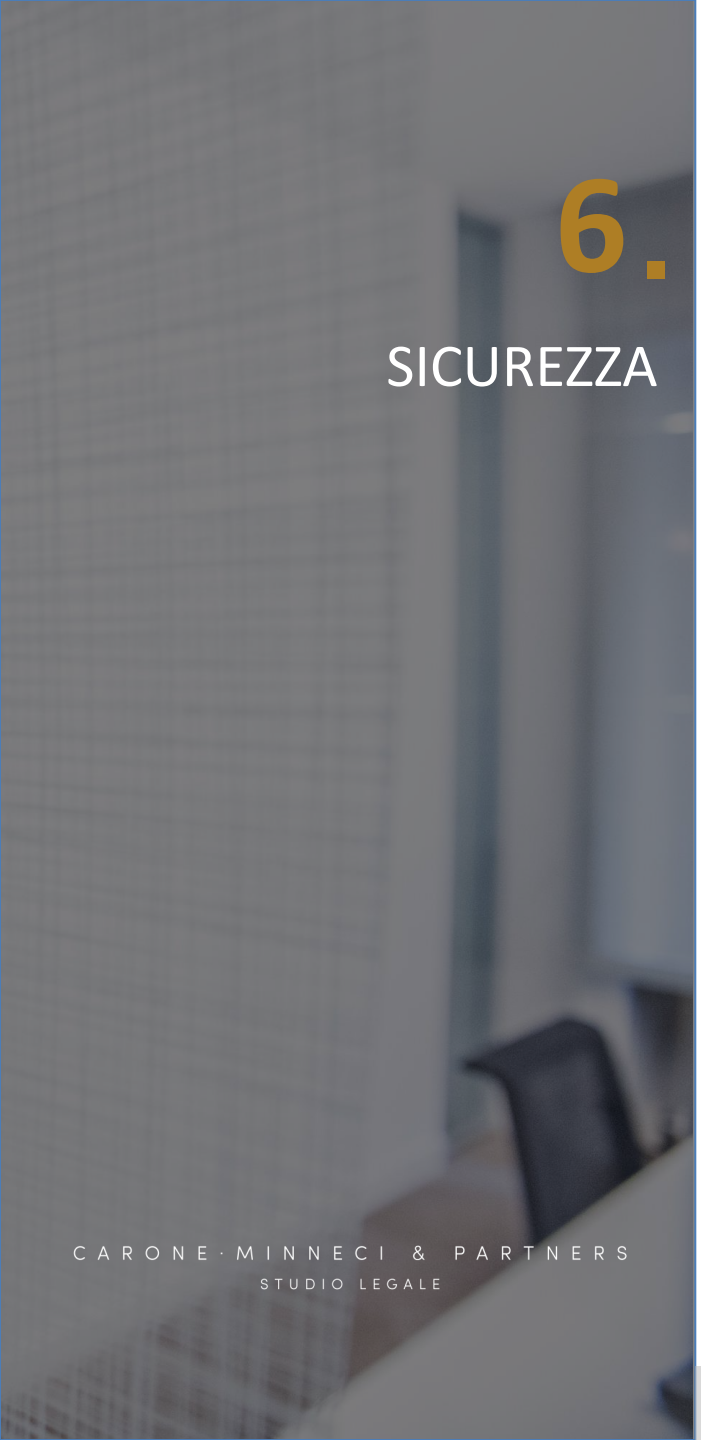
- qualità
- quantità
- portata del trattamento
- periodo di conservazione
- accessibilità

6.

SICUREZZA

CARONE · MINNECI & PARTNERS

STUDIO LEGALE



6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

MISURE TECNICHE ED ORGANIZZATIVE

- **Pseudonimizzazione e cifratura**
- Capacità di assicurare **riservatezza**, **integrità**, **disponibilità** e la **resilienza**
- Capacità di **ripristinare tempestivamente** la **disponibilità e l'accesso** in caso di incidente
- Procedura per **testare**, **verificare**, **valutare** regolarmente l'efficacia delle misure tecniche e organizzative
- Adesione a **codici di condotta e certificazioni**

6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

REGISTRO DEI TRATTAMENTI

- **CHI**: Titolari e RDT, ma lo tiene il DPO quando è designato (artt. 30.1 e 30.2)

- **QUANDO**
  i. imprese con più di **250 dipendenti**
  ii. se trattamento presenta **rischi per i diritti e le libertà** dell'interessato (a prescindere dalle dimensioni)
  iii. trattamento **non è occasionale**
  iv. categorie **particolari** di dati (sensibili e giudiziari)

- **COSA**
  i. riporta le **caratteristiche, le modalità e le finalità** dei trattamenti
  ii. sostituisce **l'obbligo di notifica** al Garante
  iii. forma **scritta e deve essere a disposizione** del Garante per ispezioni e controlli

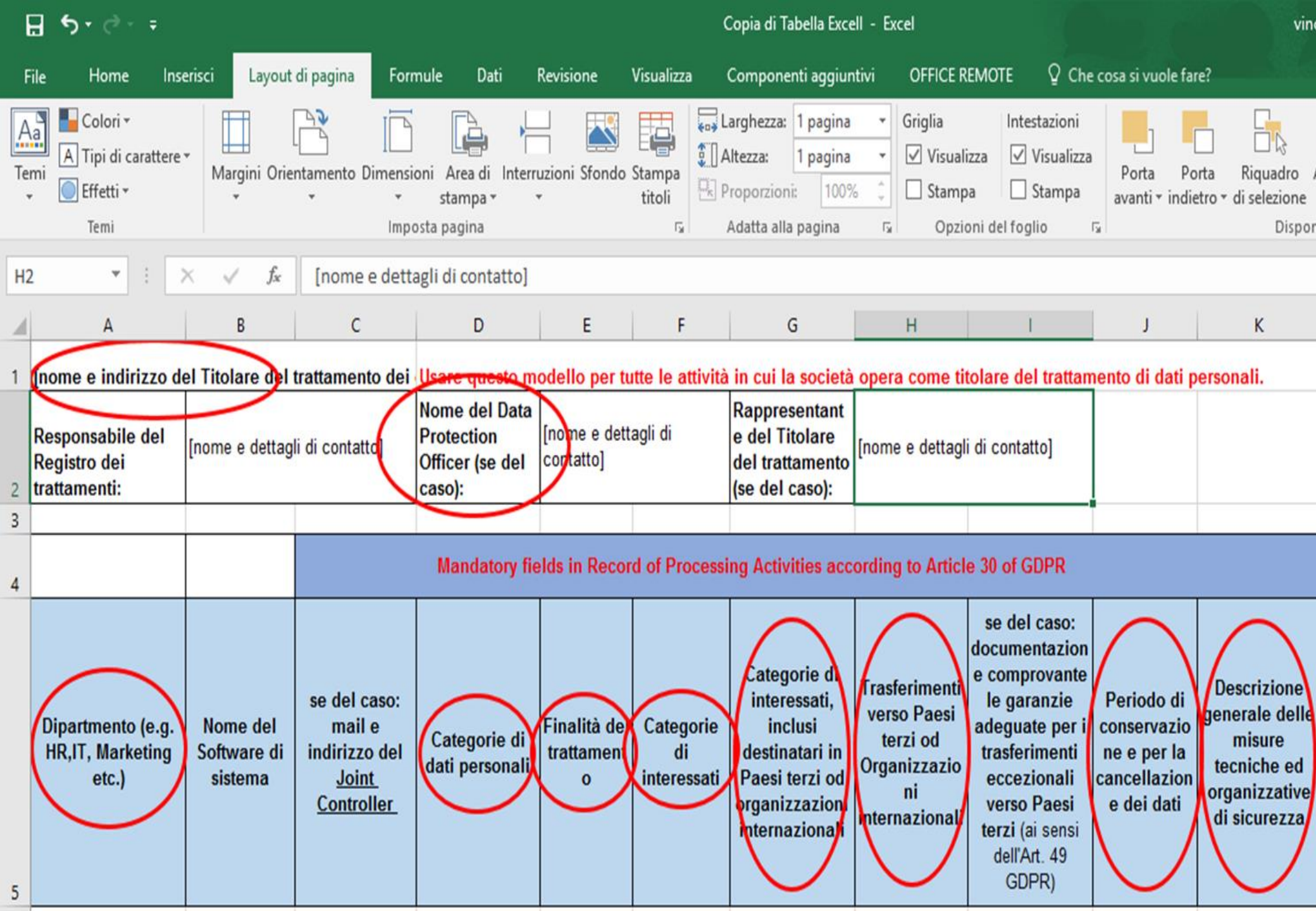
6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

REGISTRO DEI TRATTAMENTI

- **CONTENUTO**:
  - a) Dati del titolare, responsabile, contitolare, rappresentante del trattamento e del DPO
  - b) Finalità
  - c) Categorie di interessati e dei dati trattati
  - d) Destinatari a cui sono o saranno comunicati i dati
  - e) Trasferimenti verso Paesi terzi od organizzazioni internazionali
  - f) Termini ultimi previsti per la cancellazione
  - g) Descrizione generale delle misure di sicurezza tecniche e organizzative



Copia di Tabella Excell - Excel

File Home Inserisci Layout di pagina Formule Dati Revisione Visualizza Componenti aggiuntivi OFFICE REMOTE Che cosa si vuole fare?

Temi Colori Tipi di carattere Effetti — Margini Orientamento Dimensioni Area di stampa Interruzioni Sfondo Stampa titoli — Imposta pagina — Larghezza: 1 pagina Altezza: 1 pagina Proporzioni: 100% — Adatta alla pagina — Griglia Visualizza Stampa Intestazioni Visualizza Stampa — Opzioni del foglio — Porta avanti Porta indietro Riquadro di selezione

H2 [nome e dettagli di contatto]

	A	B	C	D	E	F	G	H	I	J	K
1	[nome e indirizzo del Titolare del trattamento dei			Usare questo modello per tutte le attività in cui la società opera come titolare del trattamento di dati personali.							
2	Responsabile del Registro dei trattamenti:	[nome e dettagli di contatto]		Nome del Data Protection Officer (se del caso):	[nome e dettagli di contatto]		Rappresentante del Titolare del trattamento (se del caso):	[nome e dettagli di contatto]			
3											
4			Mandatory fields in Record of Processing Activities according to Article 30 of GDPR								
5	Dipartmento (e.g. HR,IT, Marketing etc.)	Nome del Software di sistema	se del caso: mail e indirizzo del Joint Controller	Categorie di dati personali	Finalità del trattamento	Categorie di interessati	Categorie di interessati, inclusi destinatari in Paesi terzi od organizzazioni internazionali	Trasferimenti verso Paesi terzi od Organizzazioni internazionali	se del caso: documentazione comprovante le garanzie adeguate per i trasferimenti eccezionali verso Paesi terzi (ai sensi dell'Art. 49 GDPR)	Periodo di conservazione e per la cancellazione dei dati	Descrizione generale delle misure tecniche ed organizzative di sicurezza

6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RISCHI E PREGIUDIZI

- **distruzione** accidentale o illegale, **perdita**, **modifica**, **divulgazione** non autorizzata, **accesso** in modo accidentale o illegale
- danni **fisici, materiali o immateriali**
- rischi per i sistemi informatici (dal Garante):
  i. operatori: furto di credenziali, disattenzione, comportamenti sleali o fraudolenti, errore materiale
  ii. strumenti: virus informatici o malware, spam o malfunzionamento, accessi esterni, intercettazione di informazioni in rete
  iii. contesto: accessi non autorizzati a locali riservati, furto di strumenti contenenti dati, eventi distruttivi, dolosi, accidentali, dovuti ad incuria, guasto ai sistemi (impianto elettrico, climatizzazione….)

6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

RISK ASSESSMENT

- **Valutazione rischi** è **sempre necessaria** (come la sicurezza dei trattamenti)

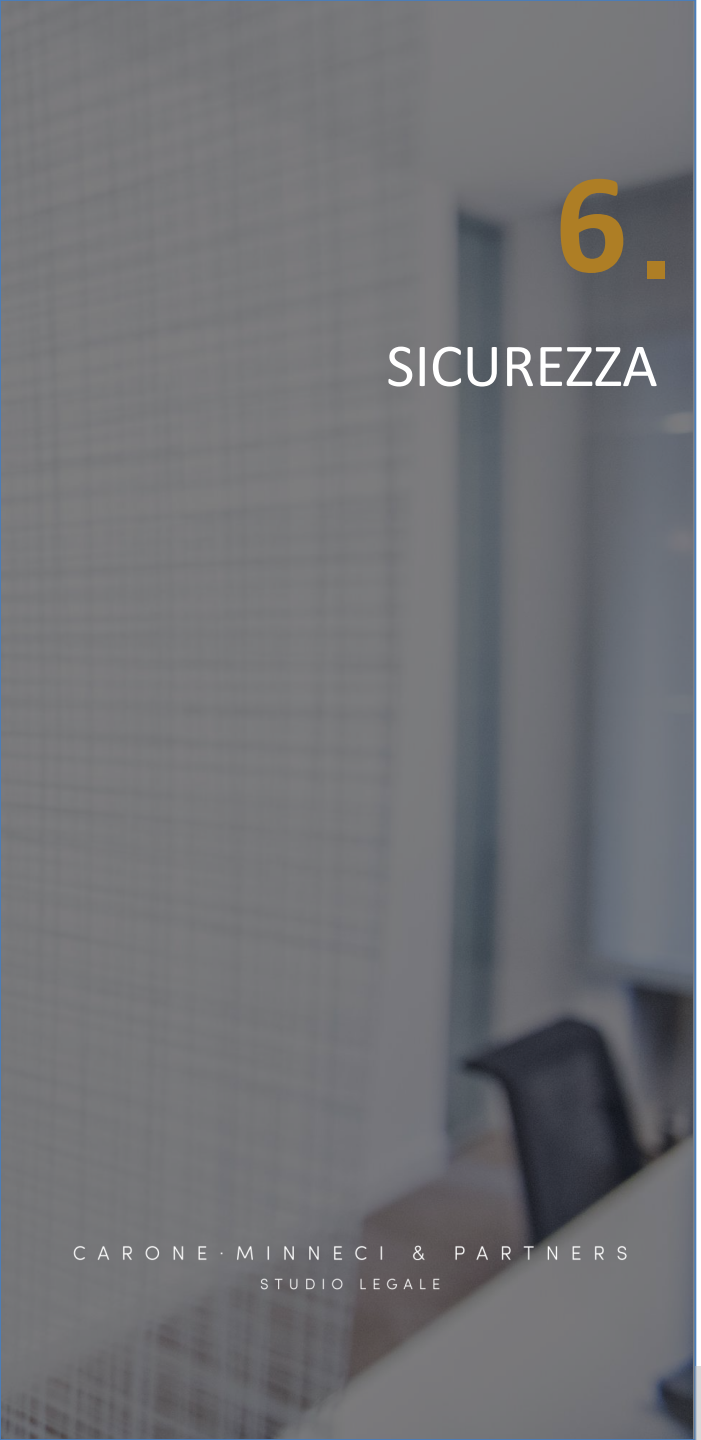
- Misure di sicurezza. I parametri per valutare sono:

  i. **stato dell'arte**

  ii. **costi** di attuazione

  iii. **natura**, **oggetto**, **contesto** e **finalità** del trattamento

  iv. rischio di varia **probabilità** e **gravità**



6.

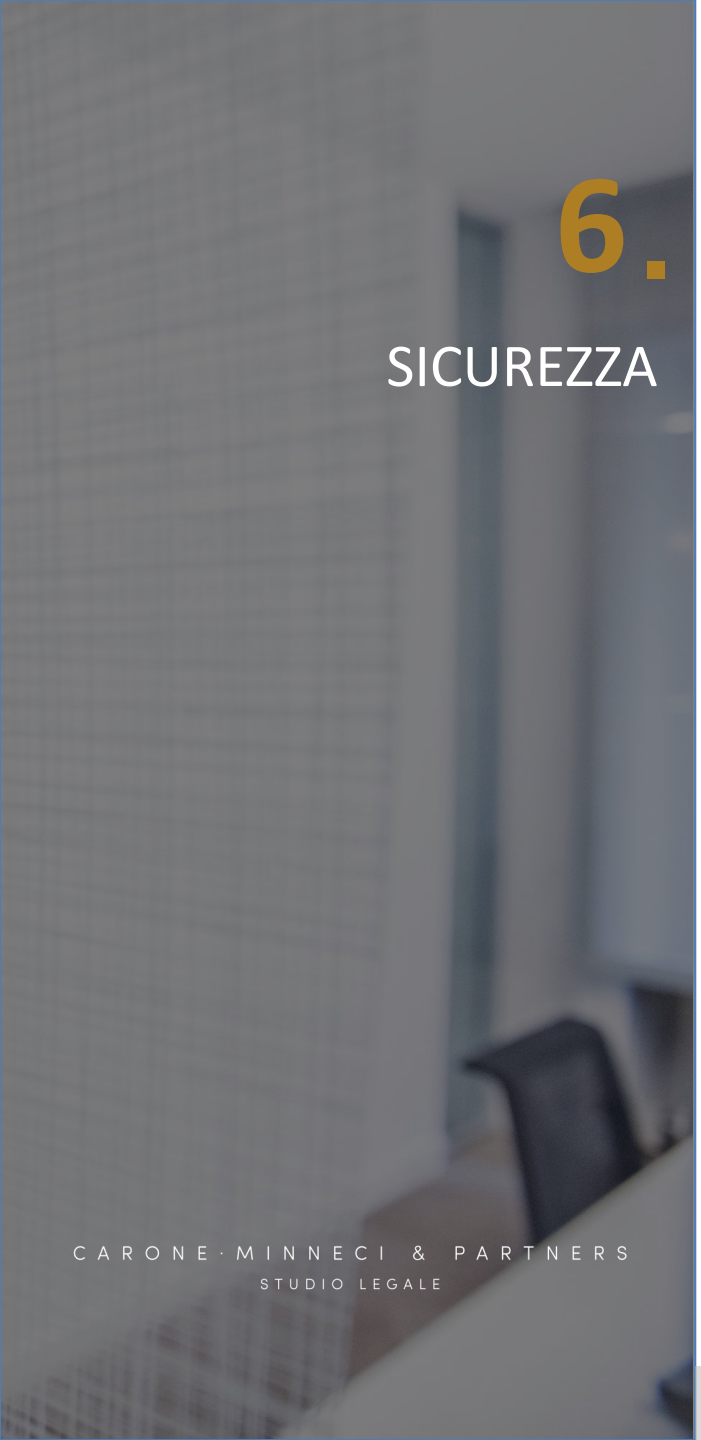
SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

IMPACT ASSESSMENT

COSA:

- È un processo inteso a **descrivere** il trattamento, valutarne la **necessità**, **proporzionalità**, nonché a contribuire a **gestire i rischi** per i diritti e le libertà delle persone, **valutandoli** e determinando le **misure** per affrontarli
- Serve a soppesare la **probabilità** e **gravità** del rischio
- Informazioni su **misure**, **garanzie** e **meccanismi** per attenuare il rischio e assicurare *compliance*
- Se non eseguita, quando è obbligatoria, è eseguita in maniera errata oppure in caso di mancata consultazione del Garante, quando necessario comporta sanzioni 10 Mln Euro – 2% fatturato annuo globale, se superiore



6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

IMPACT ASSESSMENT

QUANDO:

- Il trattamento presenta (*uso di nuove tecnologie che potrebbero presentare*) un rischio elevato per i diritti e le libertà

  i. **valutazione sistematica e globale** basata su **trattamento automatizzato** compresa **profilazione** sulla quale si fondano decisioni che producono effetti giuridici o incidono in modo analogo

  ii. **larga scala di categorie particolari di dati** o dati giudiziari

  iii. sorveglianza di zone accessibili al pubblico su larga scala

  iv. Garante deve emanare elenco dei trattamenti da sottoporre a DPIA

6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

IMPACT ASSESSMENT

COME:

- Prima del trattamento
- Deve essere consultato il DPO e il suo parere documentato nella DPIA
- Deve contenere:

1. una **descrizione dei trattamenti** (anche interesse legittimo, ove applicabile)
2. **una valutazione di necessità e proporzionalità**
3. una **valutazione dei rischi per i diritti e le libertà**
4. le **misure previste per affrontare tali rischi** e dimostrare la conformità al GDPR

6.

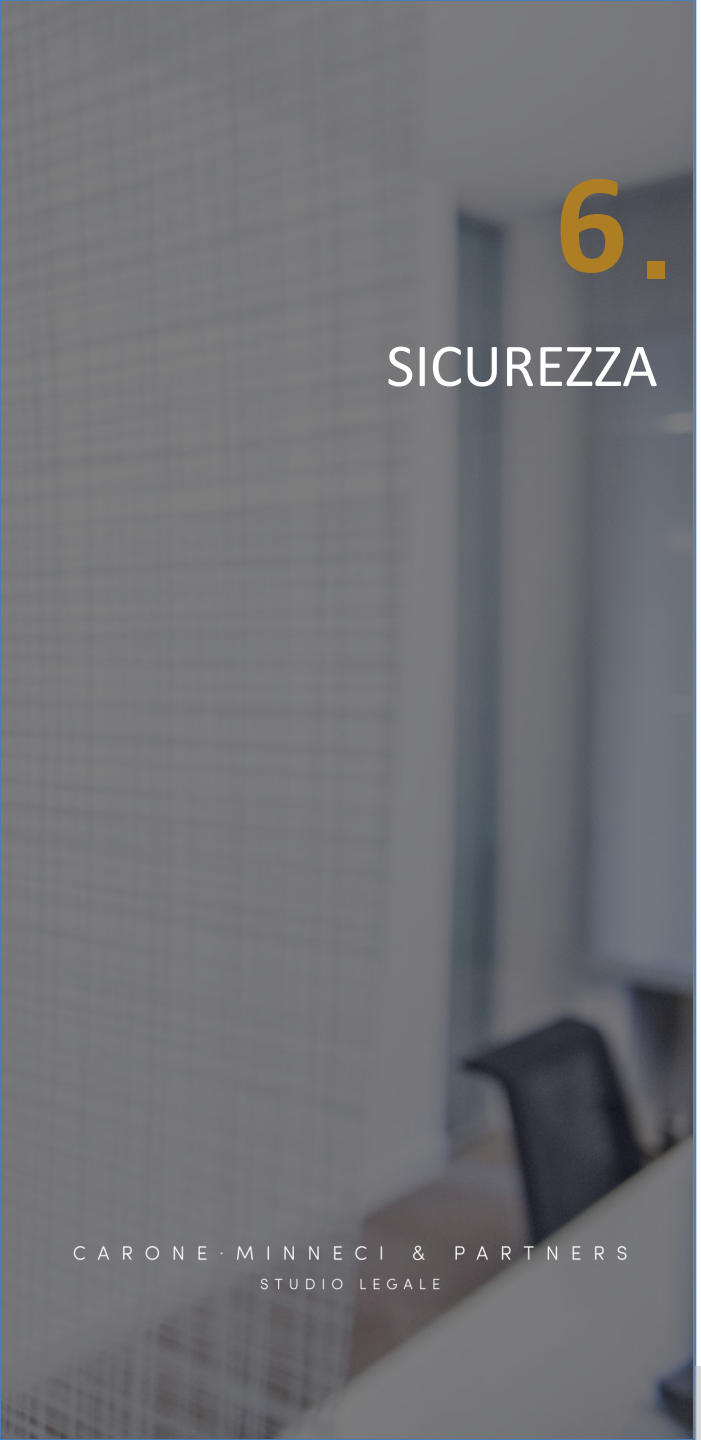
SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

IMPACT ASSESSMENT

SCOPO:

- Stabilire il contesto, tenendo conto della natura, dell'ambito d'applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio
- **Valutare i rischi** e la probabilità e gravità
- **Trattare i rischi**, attenuando tali rischi e assicurando la protezione dei dati personali
- **Dimostrare la conformità** al Regolamento
- **Consultare il Garante** se i rischi residui sono elevati
- **Conservare esiti DPIA** e aggiornamenti
- **Riesaminare** periodicamente la DPIA



6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CONSULTAZIONE PREVENTIVA

- **QUANDO**:
  1. a seguito di DPIA, rischio elevato;
  2. il rischio elevato **non può essere attenuato** mediante l'uso delle tecnologie o i costi sono elevati
- l'Autorità deve pronunciarsi entro 8 settimane con **parere scritto e può dare prescrizioni**
- **LA RICHIESTA CONTIENE**
  i. **rispettive responsabilità** (titolare, contitolari, responsabili)
  ii. **finalità** e **mezzi** del trattamento
  iii. le **misure** e le **garanzie** previste
  iv. i **dati di contatto del DPO** (se del caso)
  v. la **valutazione d'impatto**
  vi. **altre informazioni richieste** dall'Autorità

6.

SICUREZZA

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

POLICIES – MISURE - PROCEDURE

MISURE DA ADOTTARE

- Obblighi di informativa (forma intellegibile, elettronicamente, icone standardizzate
- Risks Analysis, DPIA, Privacy by-Design, Privacy by-Default
- Registro dei trattamenti
- Trasferimenti con misure di sicurezza adeguate
- Training e formazione continua
- Codici di condotta e certificazioni
- Notifiche di data breach

7.

DATA BREACH

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

7.

DATA BREACH

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

OBBLIGHI DI NOTIFICA

AL GARANTE

- Notificare senza ingiustificato ritardo (e comunque **entro 72 ore**) le violazioni dei dati personali: obbligo di documentare le violazioni.
- **Quando**: in caso di **distruzione, perdita, modifica, rivelazione non autorizzata o accesso**
- **A chi**: all'Autorità di controllo e, in casi circoscritti, agli interessati
- **Indica:** natura della violazione, le categorie e il numero delle registrazioni, dati di contatto del DPO, conseguenze della violazione, misure adottate
- **Non è necessario se**: il titolare può dimostrare che la violazione dei dati non comporta un rischio per i diritti e le libertà

7.

DATA BREACH

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

OBBLIGHI DI NOTIFICA

ALL'INTERESSATO

- **Quando**: senza indebito ritardo in caso di **rischio elevato**
- **Come:** indicando natura e formulando raccomandazioni
- **Non è necessario se il titolare**:
  i. ha adottato preventivamente tutte le misure tecniche e organizzative adeguate (e.g. cifratura)
  ii. ha adottato successivamente misure atte a scongiurare rischio elevato
  iii. comunicazione richiederebbe sforzi sproporzionati

8.

CERTIFICAZIONI E CODICI DI CONDOTTA

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

8.

CODICI DI CONDOTTA E CERTIFICAZIONE

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CODICI DI CONDOTTA E CERTIFICAZIONE

CODICI DI CONDOTTA

- Contribuiscono alla corretta applicazione GDPR
- Devono definire:
  i. trattamento corretto
  ii. legittimi interessi perseguiti
  iii. raccolta dei dati personali
  iv. informazione del pubblico e interessati
  v. misure e procedure by-design by-default
  vi. procedure di notifica e stragiudiziali

CERTIFICAZIONE

- Rilasciata dagli organismi di certificazione o dal Garante
- Durata 3 anni e può essere rinnovata
- Può essere revocata
- Non incide sulla responsabilità del titolare
- Lascia intatti i poteri e i compiti del Garante

9.

SANZIONI

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

9.

SANZIONI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

QUALI SONO

Art. 83

- fino a **10.000.000 EUR**, o per le imprese, fino al **2 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore

- fino a **20.000.000 EUR**, o per le imprese, fino al **4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore

9.

SANZIONI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

COME SONO DEFINITE

- **Effettive, proporzionate e dissuasive**
- Elementi da valutare:

i. **natura**, **gravità** e **durata** della violazione

ii. carattere **doloso** o **colposo**

iii. **misure adottate** per attenuare il danno

iv. il grado di **responsabilità**

v. eventuali **precedenti violazioni**

vi. il grado di **cooperazione** con l'Autorità

vii. le **categorie di dati** interessati

viii. come l'Autorità ha appreso della violazione

ix. provvedimenti, adesione a **codici** o **certificazioni**, altre aggravanti o attenuanti

9.

SANZIONI

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

POTERI CORRETTIVI

- Possibilità di limitare o vietare un trattamento (sospensione del servizio ai clienti)
- Altri poteri:
  i. rivolgere **avvertimenti**
  ii. rivolgere **ammonimenti**
  iii. ingiungere di **soddisfare le richieste dell'interessato**
  iv. ingiungere di **conformare** il trattamento al **GDPR** in determinata maniera o tempo
  v. ingiungere di **comunicare all'interessato**
  vi. ordinare **rettifica** o **cancellazione** di dati
  vii. revocare la certificazione
  viii. sospendere flussi di dati

10.

CONCLUSIONI

CARONE · MINNECI & PARTNERS

STUDIO LEGALE

5.

ACCOUNTABILITY
PRIVACY-BY-DESIGN
PRIVACY-BY-DEFAULT

CARONE · MINNECI & PARTNERS
STUDIO LEGALE

CONCLUSIONI

- Alla luce di quanto sin qui detto, si potrebbero adottare le seguenti misure:

1. Chiara ripartizione delle responsabilità
2. Esecuzione DPIA
3. Privacy-by-design e by-default
4. Nomina DPO
5. Registro dei trattamenti
6. Misura tecniche e organizzative (cifratura, Pseudonimizzazione)
7. Adozione di BCR (corporate binding rules) o *model clauses* (per trasferimenti verso Paesi terzi)
8. Codici di condotta e certificazioni
9. Procedura di *Data Breach*


Q/A
CARONE · MINNECI & PARTNERS
STUDIO LEGALE