Avv. Carlo Gonella
GRODER

Ordine degli Avvocati di Ivrea

Le novità del GDPR Europeo in materia di trattamento dei dati personali

7 maggio 2018

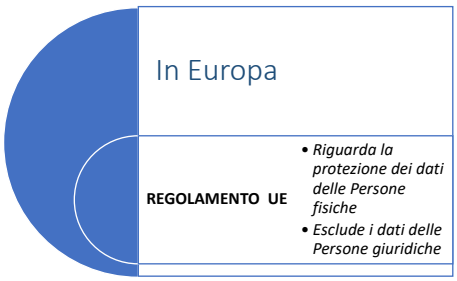
Regolamento UE sulla privacy- n° 2016/679

- disciplina la privacy delle persone fisiche
- e la libera circolazione dei dati

✓entrata in vigore: **25 maggio 2016**

✓applicabilità in tutti i Paesi della UE:

25 maggio 2018



Principi generali del Codice Privacy contenuti anche nel Regolamento UE

- **NECESSITA' / MINIMIZZAZIONE**: (ex art 3 cdp)
- **TRASPARENZA:** informativa (ex art 13 cdp)
- **LICEITÀ'**: Legge, Consenso, Legittimo interesse (ex art 23 cdp)
- **PROPORZIONALITÀ'**: finalità vs mezzi utilizzati (ex art 11 cdp)
- **PERTINENZA E NON ECCEDENZA** (ex art 11 cdp)
- **CONSERVAZIONE:** cancellazione esaurito lo scopo (ex art 11 cdp)
- **SICUREZZA/INTEGRITÀ'**(ex art 31 segg cdp)

Norme del Codice Privacy modificati dal Regolamento UE

- **INFORMATIVA** (art 12 segg.)
  CONSENSO (art 7)
- **DIRITTI DI ACCESSO DELL'INTERESSATO**
- **RESPONSABILITÀ TITOLARE | RESPONSABILE OUTSOURCING** (art 28)
- **ANALISI RISCHI E MISURE DI SICUREZZA** (art 32)
- **SANZIONI** (art 82 segg.)

Norme nuove del Regolamento UE

- **RAFFORZAMENTO DIRITTO ALL'OBLIO** (art 17)
  - Diritto a ottenere la cancellazione dei dati esaurito lo scopo
- **DIRITTO ALLA PORTABILITÀ DEI DATI** (art 20)
  ✓Diritto a ottenere il trasferimento dei dati da un fornitore all'altro
- **ACCOUNTABILITY** (art 24)
  ✓Responsabilizzazione e obbligo di prova
- **PRIVACY BY DESIGN E BY DEFAULT** (art 25)
  ✓ Obbligo di proteggere i dati fin dalla progettazione e garantire la privacy con impostazioni predefinite

Norme nuove del Regolamento UE

- **REGISTRO DEI TRATTAMENTI** (art 30)
  - ✓Obbligo di tenere un registro dei trattamenti svolti
- **DATABREACHES** (art 33)
  - ✓Obbligo di notifica delle violazioni all'interessato e al Garante
- **DPIA - VALUTAZIONE DI IMPATTO** (art 35)
  - ✓Obbligo di valutare preliminarmente l'impatto dei trattamenti sulla privacy

Norme nuove del Regolamento UE

- **DATA PROTECTION OFFICER** (art 37)
  - ✓ Nuova figura di Garanzia all'interno delle organizzazioni
- **CERTIFICAZIONE /MARCHI** (art 42)
  - ✓ Riconoscimento di conformità al Regolamento
- **RAFFORZAMENTO DELLE SANZIONI PECUNIARIE** (art 83 segg)
  - ✓Aumento dell'importo delle sanzioni fino al 4% fatturato

Definizioni

Dato personale

«QUALSIASI INFORMAZIONE RIGUARDANTE UNA PERSONA FISICA IDENTIFICATA O IDENTIFICABILE ...» (Art. 4,1)

- Nome, dati anagrafici
- Dati relativi all'ubicazione
- Numero di identificazione
- Identificativo on line
- Stato di salute, abitudini
- Immagine, voce
- Dati oggettivi e di origine soggettiva

Categorie di dati personali

- **| DATI PARTICOLARI | ex dati sensibili**

✓Origine razziale o etnica | Opinioni politiche | Convinzioni religiose - filosofiche | Appartenenza sindacale | Dati Relativi alla salute Relativi alla vita sessuale o all'orientamento sessuale

- **Dati Genetici**
- **Dati Biometrici**
- **DATI PENALI art 10**

✓Condanne penali | Reati Connessi a misure di sicurezza

Categorie di dati personali

- **DATI CHE PRESENTANO RISCHI ART. 35**
  - ✓per libertà/dignità della persona e sono assoggettati ad accorgimenti specifici, su base "Valutazione di Impatto" (prior checking).
- **DATI COMUNI**
  - ✓Tutti gli altri dati riconducibili ad una persona
  - ✓Es: Anagrafici, indirizzi postali, indirizzi IP, codici identificativi, conto corrente, carta di credito, valutazioni....
- **DATI ANONIMI [non si applica il Regolamento UE]**
  - Informazioni che non possono essere associate ad un interessato identificato o identificabile.

Trattamento - art 4.2

"QUALSIASI OPERAZIONE concernente la RACCOLTA, REGISTRAZIONE, ORGANIZZAZIONE, STRUTTURAZIONE, CONSERVAZIONE, ADATTAMENTO, MODIFICA, ESTRAZIONE, CONSULTAZIONE, USO, COMUNICAZIONE, MESSA A DISPOSIZIONE, RAFFRONTO, INTERCONNESSIONE, LIMITAZIONE, CANCELLAZIONE E DISTRUZIONE di dati»

Profilazione art 4.4

" Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti

il rendimento professionale | la situazione economica | la salute | | le preferenze personali | gli interessi |l'affidabilità | il comportamento | l'ubicazione o gli spostamenti di detta persona fisica

Soggetti

Titolare - art 4.7

- E' il soggetto (persona fisica, giuridica, ente...) che determina le finalità e i mezzi del trattamento
- Non richiede nomine
- Gli sono attribuiti tutti gli obblighi di adeguamento alla legge
- Deve condurre verifiche periodiche- culpa in vigilando
- • SE AZIENDA PERSONA GIURIDICA è L'azienda nel suo complesso
- SE DITTA INDIVIDUALE è la persona fisica del Titolare dell'Azienda

Responsabile Interno

Coadiuva il Titolare negli obblighi privacy

- Nomina opzionale ma di fatto obbligatoria se l'organizzazione è complessa

Deve presentare adeguate garanzie di competenza

Ha assegnato compiti scritti assegnati e riceve istruzioni

Può designare gli incaricati

Responsabile Esterno

CHI E'ALL'ESTERNO DELL'AZIENDA [*OUTSOURCER]*

Soggetto che tratta dati per conto del Titolare

- ✓nuovo ruolo obbligatorio in caso di esternalizzazione di attività (e predisposizione cedolini, gestione sistema informativo, cali center, agenti...)
- ✓Può essere persona fisica o giuridica
- ✓Deve presentare adeguate garanzie di rispetto del Regolamento

I trattamenti esternalizzati devono essere disciplinati da un contratto scritto

- ✓Il contratto deve prevedere una serie di vincoli prestabiliti (art 28)

Incaricati art 29

TUTTI I LAVORATORI (dipendenti, stagisti, consulenti)

Le persone che hanno accesso ai dati personali e agiscono sotto l'autorità del Titolare o del Responsabile

- ✓solo persone fisiche
- ✓devono essere individuati
- ✓devono ricevere istruzioni privacy
- ✓ogni Incaricato deve poter accedere solo ai dati necessari per la mansione

Data Protection Officer - art 37

DIPENDENTE DI ALTO PROFILO oppure ESTERNO CON CONTRATTO DI SERVIZIO

figura di garanzia del rispetto della legge in azienda

- ✓Nomina Obbligatoria in determinati casi (P.A., Monitoraggio...)
- ✓Nominato dal Titolare o dal Responsabile (artt. 37-39)
- ✓Deve essere in possesso di competenza e professionalità
- ✓Deve essere dotato di risorse umane e finanziarie
- ✓Riferisce al vertice gerarchico
- ✓Opera in autonomia
- ✓Punto di contatto per Interessati e Garante Privacy

Interessati

Art 4.1 Le persone fisiche a cui si riferiscono i dati personali

TUTTI COLORO DI CUI IL TITOLARE DETIENE DATI PERSONALI (Clienti, Fornitori, Dipendenti, Collaboratori, Candidati, Visitatori web etc.)

Particolari tipologie di dati

Trattamento dei «Dati Particolari»

- *(Origine razziale, opinioni politiche...dati genetici, biometrici)*
- E' *vietato | Salvo eccezioni prestabilite*

ECCEZIONI | IL TRATTAMENTO E' CONSENTITO

Se l'Interessato ha manifestato il proprio Consenso - salvo ulteriori disposizioni di legge /Autorizzazione del Garante,

E' necessario per assolvere obblighi o esercitare diritti in materia di lavoro o della sicurezza sociale e protezione sociale, medicina del lavoro, capacità lavorativa del dipendente

Per finalità di tutela della vita, della salute, di interesse pubblico, o esercizio di un diritto in sede giudiziaria

Dati resi manifestamente pubblici dall'Interessato (art.9)

Dati penali

E' vietato il trattamento | Salvo eccezioni prestabilite

ECCEZIONI | IL TRATTAMENTO E' CONSENTITO se autorizzato dalla Legge o dal Garante:

AUTORIZZAZIONE GENERALE GARANTE | n.7 Dati giudiziari

AUTORIZZAZIONE GARANTE specifica| per casi eccezionali

Diritti dell'interessato ed obblighi del Titolare

Diritti dell'Interessato

- alla manifestazione del consenso art. 7
- di controllo sui propri dati artt. 15-22
- ad ottenere risposta dal Titolare art. 12

Informativa Art. 13

- Dichiarazione del Titolare all'Interessato per:
  - metterlo in grado di conoscere le intenzioni del Titolare in ordine ai dati personali conferiti
  - consentirgli di valutare le conseguenze
  - poter accettare o rifiutare il trattamento
  - effettuare il controllo sui dati conferiti
- **SEMPRE NECESSARIA** anche se non deve essere richiesto il consenso

Outsourcing Art 2

Chi svolge attività "per conto di...» è obbligatoriamente un Responsabile privacy esterno

OBBLIGHI CONTRATTUALI

art. 28 Reg. UE

IL CONTRATTO DI SERVIZIO

- **Deve disciplinare**
  - ✓la materia esternalizzata, la durata, la natura e finalità del trattamento, il tipo di dati, le categorie di interessati, gli obblighi e i diritti del Titolare
- **Deve includere i seguenti obblighi per il Responsabile esterno:**
  - ✓Trattare i dati soltanto su istruzioni documentate del Titolare, anche in caso di trasferimento extra Ue
  - ✓Garantire che gli incaricati siano obbligati al rispetto della privacy
  - ✓Adottare misure di sicurezza adeguate
  - ✓Assistere il Titolare nelle risposte da fornire all'interessato in caso di esercizio del diritto di "controllo dei dati"
  - ✓ Assistere il Titolare nel garantire il rispetto degli obblighi di Sicurezza, Data Breach, Valutazione preventiva dì impatto, Prior checking col Garante
  - ✓Vietare il sub-appalto senza accordo preventivo del Titolare
  - ✓Cancellare i dati o restituirli al titolare alla fine del servizio
  - ✓Consentire attività di verifica, controllo, e ispezione del Titolare
  - ✓Informare il Titolare dei casi di violazione della privacy

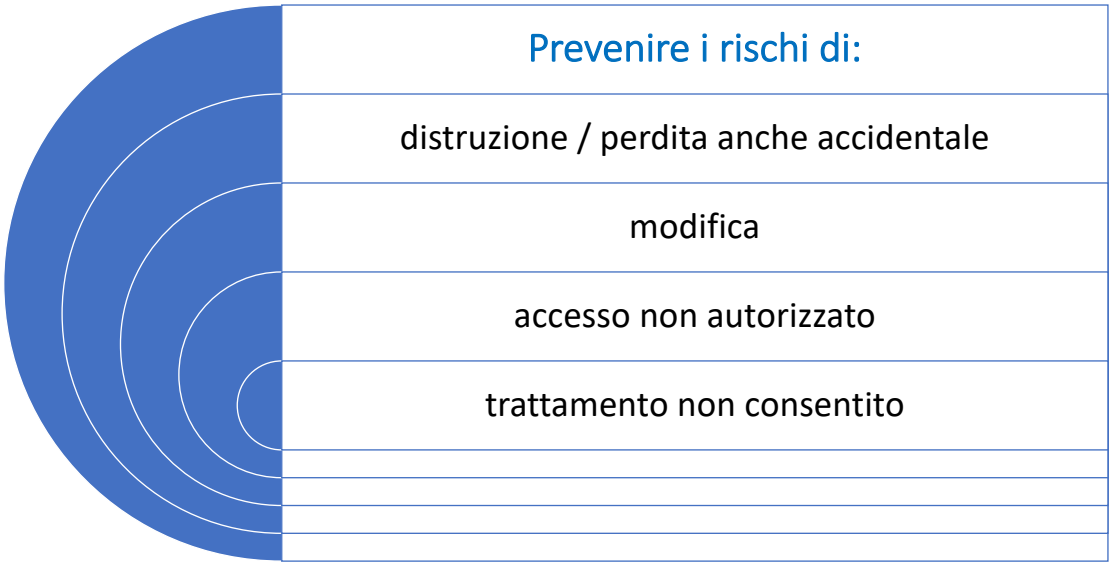
OCCORRE RIVEDERE ED INTEGRARE TUTTI I CONTRATTI DI OUTSOURCING IN CORSO

Amministratore di Sistema

Provv. Gen. Garante Italiano del 27/11/2008

il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione e figure equivalenti

Misure di sicurezza



Le misure di sicurezza devono essere

- ✓ adeguate INDIVIDUATE DAL TITOLARE
- ✓ specifiche INDIVIDUATE DAL GARANTE
  - minime [NON PIU' ESISTENTI già nell'allegato B del codice Privacy]
- ❑ ora principio di **ACCOUNTABILITY**

Misure tecniche preventive

- proteggere i file con password di cifratura
- memorizzare i dati su hard disk/supporti magnetici con sistemi di
- cifrare automaticamente al momento della scrittura

Misure fisiche ed organizzative

- Impedire accessi non autorizzati
- Proteggere i luoghi ove si svolge il trattamento da indebite intrusioni
- Procedere alla comunicazione dei dati con modalità tali da escludere una indebita conoscenza da parte di terzi non designati Incaricati
- Impartire istruzioni agli incaricati in ordine all'osservanza del segreto d'ufficio anche con riguardo a dipendenti del medesimo datore di lavoro che non abbiano titolo per venire a conoscenza di particolari informazioni

Misure fisiche ed organizzative

- Prevenire l'acquisizione e la riproduzione dei dati trattati elettonicamente, in assenza di adeguati sistemi di autenticazione o autorizzazione
- Prevenire l'acquisizione o la riproduzione di documenti contenenti informazioni personali da parte di soggetti non autorizzati.
- Prevenire l'involontaria acquisizione di informazioni da parte di terzi o di altri dipendenti in particolari situazioni ambientali

Misure fisiche ed organizzative

Comportamento dei Dipendenti

- **PREVENIRE ILLECITA DIVULGAZIONE** *A Terzi, a Colleghi (principio del need to Know)*
- **PROTEGGERE DATI vs STRUMENTI**
  - ✓*Segretezza e robustezza Psw, utilizzo PIN, Screen saver*
  - ✓*Controllo e custodia degli strumenti*
  - ✓*Clean Desk Policy*
- **PROTEGGERE DATI vs LUOGHI/ACQUISIZIONI INVOLONTARIE**
  - ✓*Distanze di cortesia/ Open Space/Aree chiuse*
  - ✓*Presidio Stampanti, Copiatrici, Fax...*
  - ✓*Separazione dati sensibili da dati comuni*
  - ✓*Armadi chiusi a chiave*
  - ✓*Distruggi documenti*
- **AZIONI PREVENTIVE**
  - ✓*Codifica voci su cedolino.*
  - ✓ *Consegna diretta dei documenti/invio plichi chiusi*

Rottamazione

- **MISURE TECNICHE DI CANCELLAZIONE SICURA**
  - ✓usare programmi di riscrittura che provvedono una volta eliminati i file (es: nel cestino) a scrivere ripetutamente nelle aree vuote
  - ✓usare sistemi di formattazione a basso livello o di demagnetizzazione
- **SMALTIMENTO RIFIUTI**
  - ✓per hard disk e supporti non riscrivibili, utilizzare punzonatura, deformazione meccanica o distruzione fisica

Risk assesment

Relativo a:
|strumenti|
|contesto|
|comportamento|

- **MISURE DI CONTRASTO DEI RISCHI**
  - ✓Adottare misure di sicurezza che comprendano:
  - ✓uso di pseudonimi e cifratura dei dati
  - ✓garanzia di disponibilità dei dati
  - ✓integrità dei dati
  - ✓riservatezza dei dati
  - ✓resilienza dei sistemi e dei servizi
- **Ripristino tempestivo in caso di incidente**
- **Effettuazione di Test di efficacia risk analysis**

Obblighi di verifica e scadenze

- Controlli periodici di efficacia e adeguatezza (art 29 Cdp/ Accountability GDPR)
- Verifica periodica dei profili di autorizzazione su base almeno annuale
- Verifica periodica dell'attività degli Amministratore di Sistema su base almeno annuale
- Verifica periodo conservazione dati
- Verifica periodica del Registro dei trattamenti e delle istruzioni

Privacy by design

Privacy by default

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

Privacy by design

- **Qualsiasi NUOVO progetto va realizzato considerando dalla progettazione (by design):**
- il rispetto dei Principi di Protezione dei dati
- la presenza di misure di sicurezza dei dati (non solo tecnologiche ma anche organizzative, procedurali) adeguate ai rischi dei trattamenti applicato non solo nello sviluppo di nuovi processi di trattamento di dati personali, ma anche nel caso di cambiamenti ai processi esistenti, o a fronte di incidenti.
- **Occorre:**
- adottare processi e strumenti di Project Management e Change Management
- coinvolgere il DPO/ Delegato Privacy sin dall'origine

Privacy by default

i requisiti di privacy ed il trattamento devono essere sempre applicati in modo predefinito

- **Il Titolare deve assicurare e controllare che le soluzioni tecnico-organizzative definite in fase di progettazione e per impostazione predefinita siano:**
  - correttamente implementate in fase di realizzazione e correttamente "collaudate" prima della loro adozione;
  - oggetto di "rivalidazione", in caso di cambiamenti tecnico-organizzativi *(re-design)* nei processi di trattamento di dati personali;
  - migliorabili nel tempo in relazione alla evoluzione delle tecnologie

Data Protection Impact Assessment

[DPIA]

Articolo 35

Valutazione d'impatto sulla protezione dei dati

["Data Protection Impact Assessment" DPIA]

- **Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.**
- La valutazione contiene almeno:
- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Articolo 36

Valutazione di impatto- Consultazione preventiva

- Il titolare del trattamento, **prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati**.... indichi che il trattamento presenterebbe un **rischio elevato in assenza di misure adottate** dal titolare del trattamento per attenuare il rischio.
- **Se ritiene che il trattamento previsto** di cui al paragrafo 1 **violi il presente regolamento,** in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, **l'autorità di controllo fornisce,** entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un **parere scritto** al titolare del trattamento e, ove applicabile, al responsabile del trattamento
- Al momento di consultare l'autorità di controllo ...., il titolare del trattamento comunica all'autorità di controllo:
  - ✓le **rispettive responsabilità del titolare** del trattamento, dei **contitolari** del trattamento e **dei responsabili** del trattamento, ,
  - ✓le **finalità e i mezzi** del trattamento previsto;
  - ✓le **misure e le garanzie previste** per proteggere i diritti e le libertà degli interessati
  - ✓la valutazione d'impatto sulla protezione dei dati

MISURE DI SICUREZZA conformi a standard di riferimento

ISO 27001

Possibile utilizzo di standard internazionali relativi alla sicurezza delle informazioni e alla privacy

- ***Standard di riferimento***
  - ✓**ISO 29100 - 29101** (Privacy Frameworks)
  - ✓**ISO 29151** (Code of Practice for Personally Identified Information protection)
  - ✓**ISO 27001/2** (Information Security Management System)

Notifica delle violazioni dei dati personali
[Data Breach]

Art. 33 - Notifica di una violazione dei dati personali all'Autorità di Controllo

- **Obbligo di notifica al Garante,** senza ingiustificato ritardo, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che non sia in grado di dimostrare, in conformità con il principio di responsabilità, che la violazione non comporti un rischio per i diritti e le libertà degli interessati:
  - ✓ Natura della violazione, categorie e numero di interessati
  - ✓ Riferimenti del Responsabile Protezione Dati o altra figura
  - ✓ Probabili conseguenze della violazione dei dati personali
  - ✓ Misure adottate per porre rimedio alla violazione e per attenuarne i possibili effetti negativi

Art. 34 - Comunicazione della violazione dei dati personali all'Interessato

- **Obbligo di comunicazione anche agli Interessati,** senza ritardo
  - ✓ In caso di **rischio elevato** (es. discriminazione, furto di identità, perdite finanziarie etc.) per i diritti e le libertà delle persone fisiche
  - ✓ Per disposizione del Garante
- **Non è richiesta** la comunicazione all'interessato se:
  - ✓ il titolare del trattamento ha attuato misure tecniche e organizzative adeguate di protezione tali da rendere i dati incomprensibili (Cifratura)
  - ✓ la comunicazione richiederebbe sforzi sproporzionati (può' essere sostituita da una comunicazione pubblica)

Conseguenze per il Titolare

- Sanzioni penali e amministrative
- Risarcimento danni agli interessati (danni patrimoniali, non patrimoniali)
- Interventi del Garante
- Costi per gestire e porre rimedio alla violazione
- Costi per la comunicazione agli interessati (se numerosi)

Danni per il business e l'immagine aziendale

Sanzioni

Tutte le sanzioni

- Sanzione amministrativa
  - ✓fino al 4% del fatturato annuo mondiale
- Risarcimento del danno
- Sanzione penale
  - ✓disposta da singoli stati
- Danno di immagine
  - ✓notifica Data Breach

In dettaglio.

Sanzioni di carattere economico

art. 83

Sanzione amministrativa pecuniaria **fino ad un massimo di € 10.000.000 oppure, per le imprese, fino al 2% del fatturato mondiale totale annuo riferito all'esercizio precedente** in caso di

- ✓inosservanza dei principi base del trattamento
- ✓ inosservanza dei diritti degli Interessati
- ✓inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali
- ✓inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo

Sanzioni di carattere economico

art. 83

Sanzione amministrativa pecuniaria **fino ad un massimo di € 20.000.000 oppure, per le imprese, fino al 4% del fatturato mondiale totale annuo riferito all'esercizio precedente** (se si tratta di un importo superiore a 20 milioni di euro) in caso di:

- ✓inosservanza di un ordine correttivo dell'autorità di controllo

Sanzioni correttive

Emesse dal Garante nei confronti del Titolare e/o del Responsabile del Trattamento

- ✓**Rivolgere avvertimenti** sul fatto che i trattamenti previsti possono violare il GDPR
- ✓**Rivolgere ammonimenti** ove i trattamenti abbiano violato le disposizioni del GDPR
- ✓**Ingiungere** di soddisfare le richieste dell'Interessato
- ✓**Ingiungere** di conformare i trattamenti alle disposizioni del GDPR
- ✓**Ingiungere** di comunicare all'interessato una violazione dei dati personali
- ✓**Imporre una limitazione** provvisoria o definitiva al trattamento, incluso il divieto di trattamento
- ✓**Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento** e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali
- ✓**Revocare la certificazione** o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti
- ✓**Infliggere una sanzione amministrativa pecuniaria** in aggiunta alle presenti misure
- ✓**Ordinare la sospensione dei flussi** di dati verso un destinatario in un paese terzo o un'organizzazione internazionale

Sanzioni

Criteri di valutazione

- devono avere carattere di effettività, proporzionalità e dissuasività.
- possono essere **integrative**, oppure **completamente sostitutive** delle sanzioni correttive
- La decisione sull'applicazione delle sanzioni spetta al l Garante per la Protezione dei Dati Personali
- nella valutazione, tiene conto delle circostanze del singolo caso, ossia:
  – della natura, gravità e durata della violazione
  – del carattere doloso o colposo della violazione
  – delle misure adottate per attenuare il danno subito dagli interessati
  – delle eventuali precedenti violazioni commesse dal titolare del trattamento
  – del grado di cooperazione con l'autorità di controllo
  – degli eventuali altri fattori aggravanti

E gli Studi Legali ?

Il ruolo di Titolare all'interno dello studio legale

- Quando l'attività è svolta individualmente, titolare del trattamento è lo stesso avvocato
- Se due professionisti operano congiuntamente gli avvocati saranno contitolari
- Se l'attività è svolta in forma societaria o associata il titolare è l'entità nel suo complesso

Nomine di Responsabili ed Incaricati nello Studio Legale

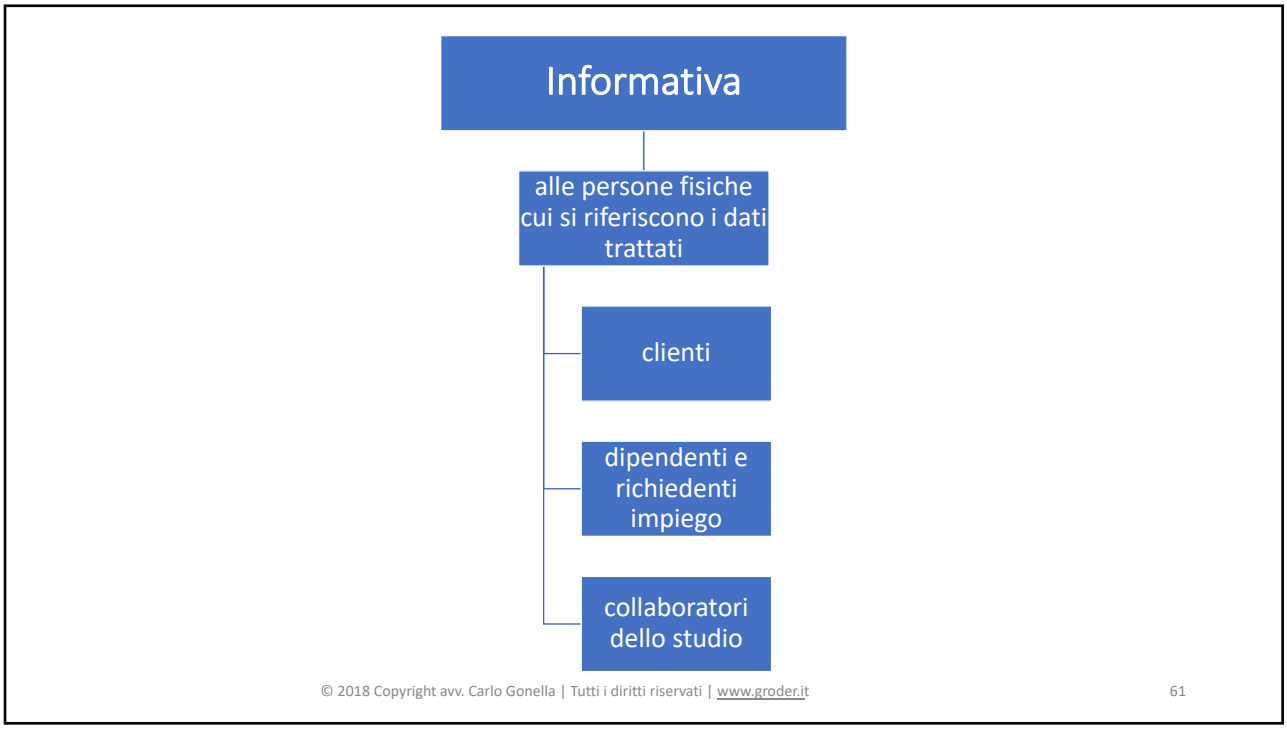
Responsabili del trattamento

- soggetti interni
- soggetti esterni **(nomina obbligatoria)**

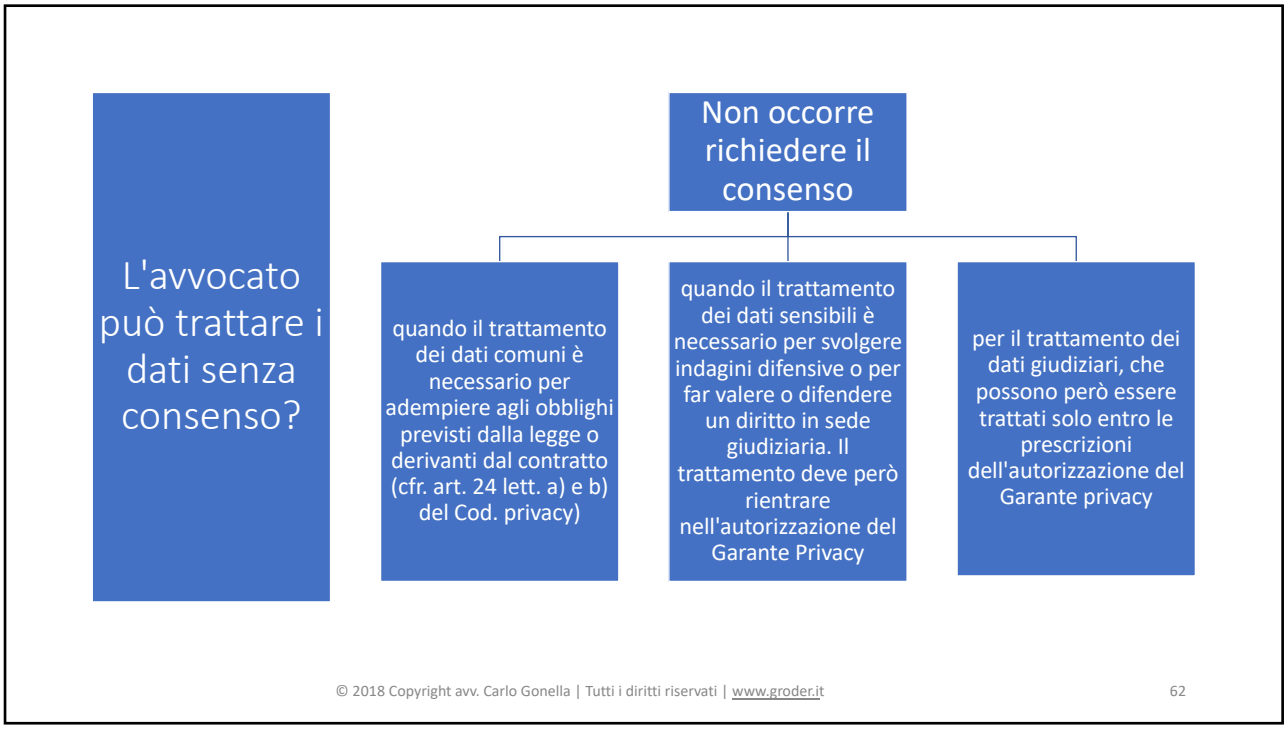
Incaricati del Trattamento

chiunque ha accesso ai dati

(praticanti, personale amministrativo ecc.)



 61



 62

Le autorizzazioni generali del Garante Privacy

Autorizzazione n. 4/2016 - Autorizzazione al trattamento dei dati sensibili da parte dei liberi professionisti (doc. web 5797347)

Autorizzazione n. 7/2016 - Autorizzazione al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici (doc. web 5803630)

DPO [*responsabili della protezione dei dati (RPD)*] negli studi legali?

Nomina obbligatoria se:

il trattamento di dati personali è effettuato da un'**autorità pubblica** o da un **organismo pubblico,**

quando le **attività principali** dell'organizzazione consistono in trattamenti che, richiedono il "**monitoraggio regolare e sistematico"** degli interessati **"su larga scala";**

quando le attività principali dell'organizzazione consistono nel trattamento "**su larga scala**" di dati "**sensibili**" (rectius, "categorie particolari di dati") o "giudiziari" (rectius, "dati personali relativi a condanne penali e reati").

Linee Guida del Gruppo di lavoro art. 29 (WP29) sui responsabili della protezione dei dati (RPD) del 13/12/16

Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento.

trattamento sia su "larga scala»:

numero di soggetti interessati dal trattamento

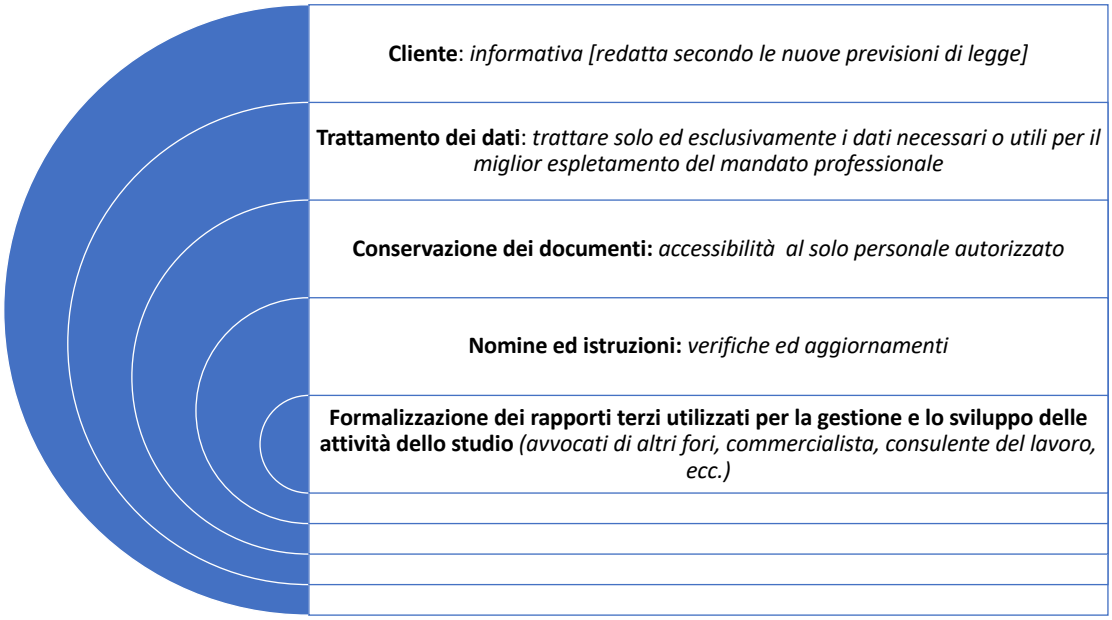
volume dei dati e/o loro diversa tipologia

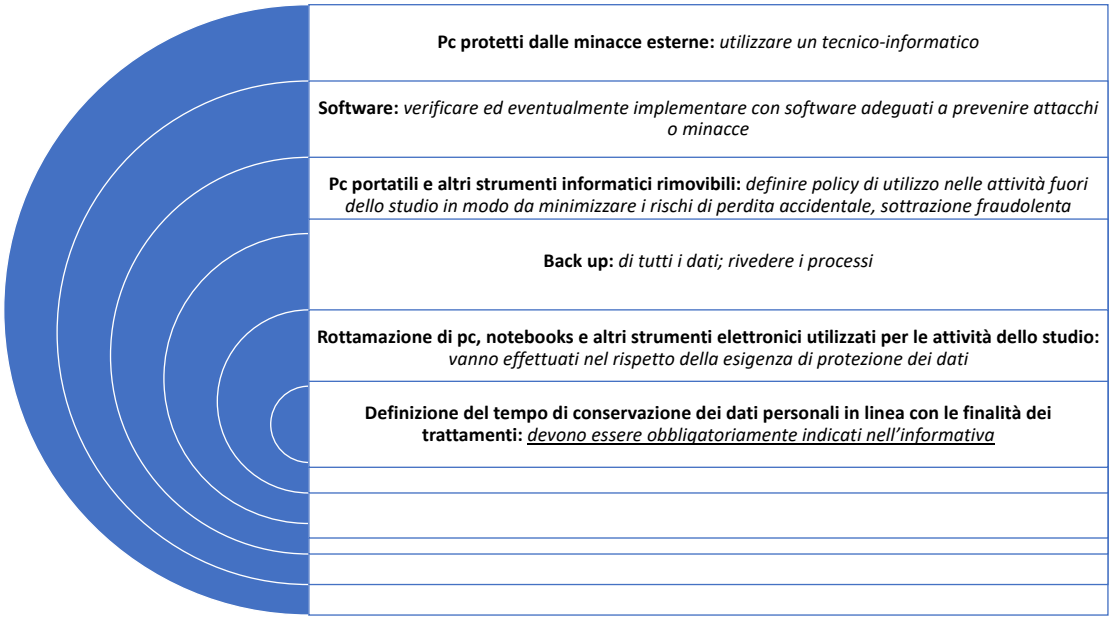
durata o persistenza dell'attività di trattamento

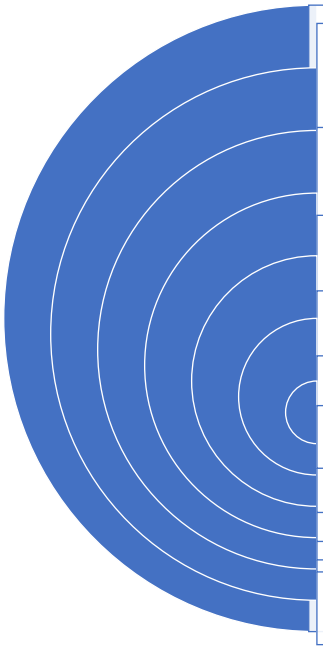
portata geografica dell'attività di trattamento)

Non si considera su larga scala il "trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato"

Studi Legali: cosa fare?







Sicurezza fisica dello studio prevenire accessi indesiderati: *prevenire azioni concretantesi nella lesione della riservatezza, della disponibilità, della integrità delle banche dati*

Registro dei trattamenti: *redigere registro come Titolare ed altro eventuale registri come Responsabile*

Privacy by design: *dare corso alle conseguenti attività, motivate e documentate*

Privacy by default: *dare corso alle conseguenti attività, motivate e documentate*

DPIA: *verificare la necessità di procedere agli adempimenti di legge e motivare per iscritto*

DPO: *verificare la necessità di procedere alla nomina e motivare per iscritto*


KEEP
CALM
AND
COMPLY WITH
GDPR