



ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI

M I L A N O



La Primavera del Non Profit

Buone pratiche degli enti non profit – Tutela dei dati personali
alla luce del Regolamento Europeo

**LA "NUOVA" PRIVACY DEL GDPR - COSA SUCCEDERÀ IL
25 MAGGIO 2018?**

*I pilastri del GDPR, spunti di riflessione per una verifica
preventiva*

Avv. Giada Svanzioli

28 marzo 2018, corso Europa 11 – Milano

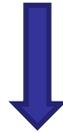
TERMINI

Regolamento Europeo 2016/679



25 maggio 2018

Legge delega 163/2017



Decreto legislativo entro 21 aprile 2018
(approvato schema di decreto)

AMBITO DI APPLICAZIONE DEL GDPR (art. 3)

- Trattamenti effettuati nell'ambito delle attività di uno **stabilimento** di un titolare o responsabile del trattamento **nel territorio dell'Unione**;
- Trattamenti di dati personali di **Interessati che si TROVANO nell'Unione**, effettuato da un titolare o da un responsabile che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
 - Beni o servizi a Interessati nell'Unione;
 - Monitoraggio del comportamento di interessati nell'Unione;
- Titolare del trattamento non stabilito nell'Unione ma in un **luogo soggetto al diritto di uno Stato membro** in virtù del diritto internazionale pubblico

ADEGUATEZZA DELLE MISURE TECNICHE E ORGANIZZATIVE

(art. 32 e artt. 24, 28)

SCOPO

Garantire e dimostrare un livello di sicurezza adeguato al rischio

(ACCOUNTABILITY)

APPROCCIO RISK-BASED:

- assessment privacy per individuare i rischi esistenti e potenziali
- adottare misure per minimizzare i rischi

ASSESSMENT PRIVACY

FOCUS

- Tipologia dei dati trattati
- Finalità
- Tipologia dei trattamenti
- Nomine (incaricati/responsabili)
- Durata dei trattamenti
- Rischi alla confidenzialità, integrità, disponibilità (distruzione, perdita, modifica, divulgazione non autorizzata, accesso, in modo accidentale o illegale)
- Sicurezza organizzativa, logica, fisica
- Modulistica

MISURE TECNICHE E ORGANIZZATIVE

Da valutare sulla base dell'assessment privacy, tenendo conto dello stato dell'arte e dei costi di attuazione.

Esempi:

Pseudonimizzazione, cifratura

Procedure di backup, business continuity, vulnerability test, penetration test

SOGGETTI

Titolare e responsabile del trattamento

Assessment privacy



Misure tecniche e organizzative adeguate

Privacy by design

Privacy by default

Registro delle attività di trattamento

DPIA

Consultazione preventiva

Nomine (incaricati, responsabili, DPO)



Data breach notification

PRIVACY BY DESIGN (ART. 25)

PUNTO DI PARTENZA

Analisi su: natura, ambito di applicazione, contesto, finalità del trattamento, rischi con probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

+

Valutazione stato dell'arte e dei costi di attuazione

QUANDO

Prima: quando vengono determinati i mezzi del trattamento

Durante: all'atto del trattamento

PRIVACY BY DESIGN

(ART. 25)

AZIONE

Adottare **misure tecniche e organizzative adeguate** (es. pseudonimizzazione)

SCOPO

Attuare efficacemente i principi di protezione dei dati (es. minimizzazione art. 5)

+

Integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del GDPR e tutelare i diritti degli interessati

PRIVACY BY DEFAULT

(ART. 25)

AZIONE

Adottare misure tecniche e organizzative adeguate

COME

Per **impostazione predefinita**

SCOPO

Garantire che siano trattati **SOLO** i dati personali **NECESSARI** per ogni specifica finalità del trattamento

Garantire che **non** siano resi accessibili dati personali ad un **NUMERO INDEFINITO** di persone fisiche senza l'intervento della persona fisica

AMBITO

Quantità dei dati raccolti, portata del trattamento, periodo di conservazione, accessibilità

Maggiore è la quantità di dati trattati, maggiore è la superficie esposta a rischi provenienti dall'interno e dall'esterno

In fase di **sviluppo, progettazione, selezione e utilizzo** di applicazioni, servizi e prodotti, i produttori dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati quando sviluppano e progettano tali prodotti, applicazioni e servizi e far sì che i titolari e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.

I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere considerati anche negli appalti pubblici.

(considerando 78)

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (art. 30)

L'obbligo NON si applica alle imprese o organizzazioni con meno di 250 dipendenti

A MENO CHE

il trattamento che esse effettuano possa presentare un **rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati o i dati personali relativi a condanne penali e a reati**

RICORDIAMO POI

Il principio dell'accountability (cfr. anche considerando 82)



Valutazione risk-based sull'obbligo/opportunità

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (art. 30)

FORMA

Scritta, anche in formato elettronico

SOGGETTI

Titolare e responsabile del trattamento

CONTENUTO = MAPPA DEL TRATTAMENTO

1) se tenuto dal **titolare del trattamento**

- nome, dati di contatto del titolare del trattamento (+ event. contitolare, rappresentante del titolare del trattamento) e del responsabile della protezione dei dati;
- le finalità del trattamento;
- descrizione delle categorie di interessati e delle categorie di dati personali;

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (art. 30)

- categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati (cfr. artt. 5 lett. e), 13 c2 lett. a, 14 c2 lett.a);
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative .

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (art. 30)

2) se tenuto dal **responsabile del trattamento**

- nome, dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI – DPIA (art. 35)

OGGETTO

valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

SOGGETTO

titolare del trattamento

PRESUPPOSTO

tipo di trattamento che:

- 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

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI – DPIA (art. 35)

QUANDO

prima di procedere al trattamento + consultazione con il DPO.

La DPIA **DEVE** essere svolta in caso di:

- **valutazione sistematica e globale** di aspetti personali relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- **trattamento, su larga scala, di categorie particolari** di dati personali o di **dati relativi a condanne penali e a reati** di cui all'articolo 10;
- **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI – DPIA (art. 35)

CONTENUTO MINIMO:

- descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- valutazione dei rischi per i diritti e le libertà degli interessati;
- 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.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI – DPIA (art. 35)

INDICAZIONI E CHIARIMENTI

Article 29 WP

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679

Politecnico di Milano

https://www.osservatori.net/it_it/linea-guida-per-la-data-protection-impact-assessment

CONSULTAZIONE PREVENTIVA (Art. 36)

OGGETTO

Consultazione dell'autorità di controllo

PRESUPPOSTO

qualora la DPIA indichi che il trattamento presenterebbe un **rischio elevato in assenza di misure** adottate dal titolare del trattamento per attenuare il rischio

QUANDO

prima di procedere al trattamento



CONSULTAZIONE PREVENTIVA (Art. 36)

CONTENUTO

- ove applicabile, le rispettive **responsabilità** del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
- le **finalità e i mezzi** del trattamento previsto;
- le **misure e le garanzie** previste per proteggere i diritti e le libertà degli interessati;
- ove applicabile, i **dati di contatto** del titolare della protezione dei dati;
- la **DPIA**;
- ogni altra informazione richiesta dall'autorità di controllo.

CONSULTAZIONE PREVENTIVA (Art. 36)

POTERI DELL'AUTORITA' DI CONTROLLO

Se ritiene che il trattamento previsto violi il GDPR, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, 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 e può avvalersi dei poteri di cui all'articolo 58.

Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

SOGGETTI / NOMINE

titolare del trattamento



incaricati
responsabili (int.? – esterni)
DPO
rappresentante
amministratore di sistema

responsabile del trattamento



incaricati
responsabili (int.?-esterni)
DPO
rappresentante
amministratore di sistema

Verificare alla luce dell'emanando decreto legislativo

RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO (artt. 37-38-39)

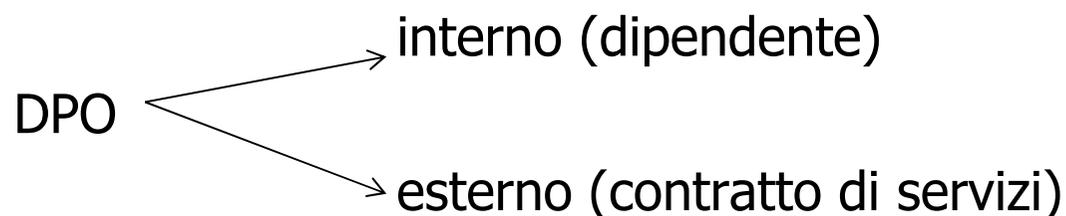
Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un DPO quando:

- il trattamento è effettuato da **un'autorità pubblica o da un organismo pubblico** (no autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali);
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati**

RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO (artt. 37-38-39)

Unico DPO per:

- **gruppo imprenditoriale** (deve essere facilmente raggiungibile da ciascuno stabilimento)
- **più autorità pubbliche o organismi pubblici** (tenuto conto della loro struttura organizzativa e dimensione)



Il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento **possono** o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un DPO. Il DPO può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO (artt. 37-38-39)

REQUISITI

- **qualità professionali**, in particolare conoscenza specialistica della normativa e prassi in materia di protezione dei dati
- capacità di **assolvere i compiti** di cui all'articolo 39

INDICAZIONI E CHIARIMENTI

Article 29 WP Guidelines on Data Protection Officers ('DPOs')

Norma UNI 11697:2017

Nuove Faq Garante Privacy

RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO (artt. 37-38-39)

COMPITI MINIMI DEL DPO

- **informare** e fornire **consulenza** in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni relative alla protezione dei dati
- **sorvegliare** l'osservanza del presente regolamento, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo (sono doveri del titolare e del responsabile)

RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO (artt. 37-38-39)

COMPITI MINIMI DEL DPO

- fornire, se richiesto, un **parere** in merito alla DPIA e sorvegliarne lo svolgimento;
- **cooperare** con l'autorità di controllo;
- fungere da **punto di contatto** per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo

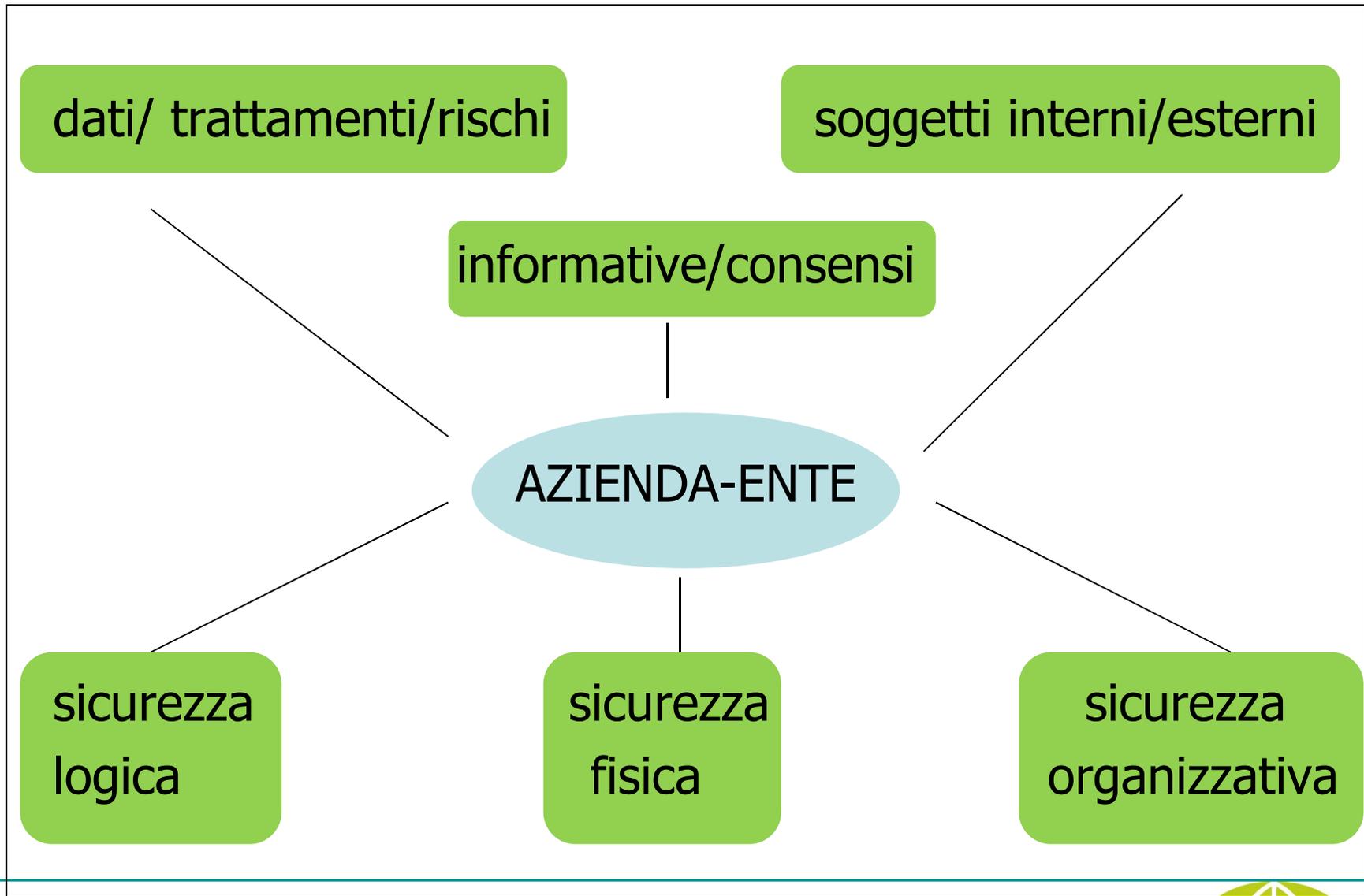


ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI

M I L A N O



TEMI DI UNA VERIFICA PREVENTIVA – GAP ANALYSIS



- **Dati, trattamenti (finalità, durata, base giuridica, modulistica),rischi**
- **sistema di nomine**
- **policy / istruzioni**
- **la formazione**
- **piano di audit**
- **registro dei trattamenti**
- **Chi e come risponde alle istanze di accesso, rettifica, cancellazione, opposizione degli Interessati**
- **misure di protezione fisica dell'edificio**
- **accesso all'edificio (come e chi)**
- **videosorveglianza -geolocalizzazione**
- **dove e come vengono conservati i documenti cartacei?**
- **CED, contratto server farm, cloud**
- **antivirus, firewall**
- **procedure di backup, disaster recovery, business continuity, penetration test**
- **provider (sito e mail)**
- **Wi-Fi**
- **dispositivi mobili, BYOx**
- **software**
- **Data breach**

GRAZIE PER L'ATTENZIONE

Avv. Giada Svanziroli

FUMAGALLI
GRANDO
E ASSOCIATI
STUDIO LEGALE

Via San Vittore, 40 – MILANO

giada.svanziroli@fglex.it

© 2018 Studio Fumagalli Grando e Associati