CONFINDUSTRIA

FIGURE SOGGETTIVE NEL TRATTAMENTO DEI DATI PERSONALI GDPR 679/2016

AVV. FRANCESCA TRESANINI

FIGURE SOGGETTIVE NEL TRATTAMENTO DEI DATI PERSONALI

1) INTERESSATO
2) TITOLARE DEL TRATTAMENTO
3) CONTITOLARE DEL TRATTAMENTO
4) RESPONSABILE DEL TRATTAMENTO
5) PERSONA AUTORIZZATA AL TRATTAMENTO
6) DPO DATA PROTECTION OFFICER

IL TITOLARE DEL TRATTAMENTO- DATA CONTROLLER

E' il vero soggetto ***"RESPONSABILE" DEL TRATTAMENTO*** dei dati personali

Soggetto che (da solo o insieme ad altri)

- Determina le **FINALITA' del trattamento**
- Determina le **MODALITA**' del trattamento
- è' **RESPONSABILE** dell'osservanza degli obblighi previsti dalla normativa in materia di protezione dei dati personali

SETTORE PRIVATO : persona fisica o giuridica

SETTORE PUBBLICO : persona giuridica (ente /società)

GRUPPI DI SOCIETA' : es soc. madre e controllata avendo personalità giuridica diversa abbiamo più titolari del trattamento

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

① **METTERE IN ATTO MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE ADEGUATE PER :**

- **GARANTIRE**
- **COMPROVARE** (documentare)

che il **TRATTAMENTO** dei dati personali sia stato **EFFETTUATO CONFORMEMENTE AL REGOLAMENTO**

MISURE DI SICUREZZA

Sono tutte quelle misure tecniche ed organizzative che devono GARANTIRE UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO

Il GDPR NON fa riferimento alle MISURE MINIME DI SICUREZZA ma a MISURE ADEGUATE

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

L'**adeguatezza delle misure** viene valutata dal Titolare del trattamento considerando:

- lo **stato dell'arte** ed i **costi di attuazione**
- **natura e ambito di applicazione del trattamento**
- il **rischio** la **probabilità** e la **gravità della violazione**

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

Le misure di sicurezza sono enunciate a TITOLO ESEMPLIFICATIVO

A) MISURE TECNICHE:

- **PSEUDONIMIZZAZIONE** : i dati sono conservati in una FORMA che impedisce l'identificazione dell'utente senza l'utillizzo di ulteriori informazioni (TAG o MASCHERAMENTO)
- **CIFRATURA DEI DATI : dati INCOMPRENSIBILI a chi non è autorizzato all'accesso**

B) MISURE ORGANIZZATIVE

- **GARANZIE** di riservatezza integrità disponibilità e recupero dei dati
- **ACCESSO TEMPESTIVO AI DATI** in caso di incidenti
- **PROCESSO DI VERIFICA PERIODICA** per valutare l'efficacia delle misure

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

Titolare e Responsabile del trattamento **PER DIMOSTRARE**

- **la ADEGUATEZZA DELLE MISURE** e
- la **CONFORMITA**' al Regolamento

possono ADERIRE A **CODICI DI CONDOTTA** O A **MECCANISMI DI CERTIFICAZIONE**

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

CODICI DI CONDOTTA o DEONTOLOGICI

- Sono **PREDISPOSTI DALLE ASSOCIAZIONI DI CATEGORIA** di Titolari o Responsabili in un determinato settore.
- I codici **INDICANO GLI OBBLIGHI** di Titolare e Responsabile in relazione al RISCHIO in determinato settore.
- Sono sottoposti a controllo del Garante:
  - se il codice si applica in 1 solo Stato con parere positivo è PUBBLICATO
  - se il codice si applica in PIU' Stati necessario il parere del Comitato Europeo

Il CONTROLLO sul rispetto del codice da parte del Titolare o Responsabile spetta all'**AUTORITA' DI CONTROLLO o ORGANISMI ACCREDITATI**

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

CERTIFICAZIONI

- Servono a **VALUTARE IL LIVELLO DI PROTEZIONE DEI DATI** attraverso apposizione di Sigillli o Marchi che devono essere apposti da organismi accreditati
- Oggi non sono esistenti

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

② **NOMINARE CON CONTRATTI RESPONSABILI CONTITOLARI E DPO**

Il Titolare del trattamento è OBBLIGATO nominare il Responsabile

③ **ATTUARE POLITICHE ADEGUATE in materia di privacy**

La logica del Regolamento è di tipo ORGANIZZATIVO e prevede l'impostazione a monte della tutela dei dati con vari strumenti (registro Dpia nomina responsabili)

④ **GARANTIRE L'ESERCIZIO DEI DIRITTI AGLI INTERESSATI** (oblio, portabilità accesso ai dati..)
⑤ **DARE RISCONTRO AGLI INTERESSATI** in relazione al loro esercizio dei diritti
⑥ **DARE INFORMATIVA e ACQUISIRE CONSENSO**
⑦ **RISPETTARE I PRINCIPI DI PRIVACY BY DEFAULT AND BT DESIGN**

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

⑧ **EFFETTUARE VALUTAZIONE D'IMPATTO PREVENTIVA** in presenza di rischio elevato

La Valutazione d'impatto DPIA deve essere effettuata da parte del Titolare del trattamento prima di iniziare il trattamento dei dati quando tale TRATTAMENTO, soprattutto per l'utilizzo di NUOVE TECNOLOGIE , considerando la natura il contetesto e le finalità del trattamento, PRESENTA UN RISCHIO ELEVATO PER I DIRITTI E LE LIBERTA' DELLE PERSONE

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

⑨ CONSULTAZIONE PREVENTIVA GARANTE

in caso di trattamento di dati sensibili o dati relativi a condanne penali o reati , il Titolare del trattamento può chiedere una Consultazione preventiva al Garante che consiste in una sorta di consiglio sulla scelte delle misure di sicurezza implementate

⑩ ADOTTARE MISURE DI SICUREZZA (Dpia)

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

⑪REGISTRO DEI TRATTAMENTI

- Deve essere tenuto da Titolari e Responsabili
- Non è un adempimento formale ma strumento di comprova
- **OBBLIGATORIO** per aziende con PIU di 250 dipendenti , altrimenti ESCLUSO a meno che siano effettuati trattamenti a rischio

CONTENUTO DEL REGISTRO

- NOME e dati di contatti Titolare Responsabile Contitolare Dpo
- FINALITA' del trattamento
- descrizione di CATEGORIE INTERESSATI / DATI PERSONALI/ DESTINATARI
- indicazione PAESI TERZI o organizzazioni internazionali cui sono trasmessi i dati
- termini CANCELLAZIONE DATI
- MISURE SICUREZZA

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

- Il Registro del Responsabile deve indicare i trattamenti effettuati per conto del Titolare

- Il registro deve avere forma scritta anche elettronica

⑫ **NOTIFICAZIONE DELLE VIOLAZIONI DI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO**

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

VIOLAZIONE DEI DATI PERSONALI
DATA BREACH

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

LA VIOLAZIONE DEI DATI PERSONALI consiste nella **violazione di sicurezza** che comporta

- **ACCIDENTALMENTE**
- in **MODO ILLECITO**

DISTRUZIONE PERDITA MODIFICA DIVULGAZIONE ACCESSO NON CONSENTITO ai dati

La violazione dei dati comporta un danno alle persone

Il DATA BREACH deve essere impedito implementando corrette misure di sicurezza perché danneggia INTERESSATO ed il TITOLARE soggetto al controllo del Garante

Il Titolare del trattamento **DEVE NOTIFICARE LA VIOLAZIONE alla Autorita' di Controllo** quando ne è a conoscenza tempestivamente entro 72 ore e senza ingiustificato ritardo

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

La NOTIFICA E' SUBORDINATA alla VALUTAZIONE DEL RISCHIO da parte del titolare

CONTENUTO DELLA NOTIFICA:

- descrizione della **NATURA DELLA VIOLAZIONE** e dei **DATI coinvolti**
- **CATEGORIA E NUMERO DEGLI INTERESSATI**
- possibili **CONSEGUENZE della violazione**
- **MISURE** adottare per **PORRE RIMEDIO/ ATTENUARE GLI EFFETTI**
- **TEMPI DI RIPRISINO**
- **INDICAZIONE DEL DPO**

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

Il **RESPONSABILE DEL TRATTAMENTO** deve **INFORMARE** IL titolare quando è a conoscenza di un data breach

COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE

- quando la violazione presenta un **RISCHIO ELEVATO** per i diritti e le libertà fondamentali
- Si consente all'interessato di provvedere.
- La comunicazione meno tecnica deve indicare conseguenze della violazione e Misure adottate
- **NON** è necessaria se :
  - il titolare ha **CIFRATO I DATI**
  - sono adottate **MISURE PER RIDURRE I RISCHI**
  - la comunicazione richiederebbe uno **SFORZO SPROPOSITATO**

IL TITOLARE DEL TRATTAMENTO - OBBLIGHI

DOCUMENTAZIONE INTERNA DELLE VIOLAZIONI

- Anche se non è notificata o comunicata la violazione deve essere documentata indicando circostanze e rimedi adottati.

Nel codice della privacy è previsto il data breach per i fornitori di servizi di comunicazione elettronica.

Esiste il **REGISTRO INFORMATICO DELLE VIOLAZIONI** che consiste in una specie di **INVENTARIO** con indicazione delle circostanze della violazione e dei provvedimenti adottati per porvi rimedio

IL TITOLARE DEL TRATTAMENTO – RESPONSABILITA’

PRINCIPIO DI RESPONSABILIZZAZIONE ACCOUNTABILITY

IL TITOLARE DEL TRATTAMENTO – RESPONSABILITA'

In applicazione del principio di accountability il TITOLARE DEL TRATTAMENTO DEVE METTERE IN ATTO MISURE TECNICHE ED ORGANIZZATIVE ADEGUATE per GARANTIRE E DOCUMENTARE LA CONFORMITA' del TRATTAMENTO AL REGOLAMENTO

Il Titolare ed il Responsabile del trattamento **DEVONO DIMOSTRARE di AVER EFFETTUATO IL TRATTAMENTO ADEMPIENDO A TUTTI GLI OBBLIGHI**
Hanno pertanto loro l'ONERE DELLA PROVA.

Sono abrogati:

- PRIOR CHECKING
- ISTANZA DI RICONOSCIMENTO DI NTERESSE LEGITTIMO

IL TITOLARE DEL TRATTAMENTO – RESPONSABILITA’

Titolare e Responsabile **DECIDONO AUTONOMAMENTE**

MODALITA’ GARANZIE E LIMITI DEL TRATTAMENTO

- rispettando **LE NORME**
- rispettando **CRITERI SPECIFICI** fra cui :
    1. **DATA PROTECTION BY DEFAULT AND BY DESIGN**
    2. **VALUTAZIONE DEL RISCHIO (DPIA)**

Il Titolare del trattamento **HA RESPONSABILITA’ DIRETTA IN CASO DI RISARCIMENTO DANNI**

IL TITOLARE DEL TRATTAMENTO – RESPONSABILITA'

1. DATA PROTECTION BY DEFAULT AND BY DESIGN

Il trattamento dei dati personali deve essere effettuato **PREVEDENDO FIN DALL'INIZIO LE GARANZIE INDISPENSABILI per:**

- sodisfare i requisiti del Regolamento
- tutelare i diritti degli interessati

considerando il contesto complessivo dove si colloca il trattamento e i rischi per i diritti e le libertà degli interessati.

- **PRIBACY BY DESIGN**: PROTEZIONE DEL DATO FIN DALLA PROGETTAZIONE DEI SISTEMI INFORMATICI che ne prevedono l'utilizzo
  tutela della privacy fin dalla progettazione di app software database

- **PRIVACY BY DEFAUTL**: consiste nella ADOZIONE DI MISURE per garantire che SIANO TRATTATI DI DEFAULT solo i dati personali necessari per la finalità(minimizzazione / limitazione)

I CONTITOLARI DEL TRATTAMENTO

Figura espressamente regolata nel GDPR

Sono **CONTITOLARI DEL TRATTAMENTO i soggetti che CONGIUNTAMENTE DETERMINANO LE FINALITA' ED I MEZZI DEL TRATTAMENTO.**

Sono **OBBLIGATI** a sottoscrivere un **ACCORDO DI RIPARTO** ossia un contratto che determina i rispettivi COMPITI e le rispettive RESPONSABILITA' conosciuto dall'interessato nel suo CONTENUTO ESSENZIALE

Ogni contitolare risponde esclusivamente di quanto previsto nell'accordo di riparto.

NON si ha FUSIONE DELLE ORGANIZZAZIONI DI TRATTAMENTO

Gli INTERESSATI possono rivolgersi indifferentemente all'uno o all'altro dei contitolari

IL RESPONSABILE DEL TRATTAMENTO – DATA PROCESSOR

IL RESPONSABILE DEL TRATTAMENTO è la persona fisica , persona giuridica , amministrazione ente organismo o servizio che **TRATTA ED ELABORA I DATI PERSONALI PER CONTO DEL TITOLARE DEL TRATTAMENTO** secondo le sue **ISTRUZIONI**

- la **NOMINA** del responsabile con il GDPR è divenuta **OBBLIGATORIA** e quest'ultimo NON può rifiutare.
- la nomina del o dei responsabili è prevista sempre nell'ottica di EFFICIENZA ORGANIZZATIVA
- La NOMINA avviene con **CONTRATTO** o altro atto scritto giuridicamente analogo e deve indicare:

IL RESPONSABILE DEL TRATTAMENTO – DATA PROCESSOR

La NOMINA deve indicare:

- la **materia disciplinata**
- la **durata** la **natura** e le **finalità** del trattamento
- il tipo di **dati trattati** e la **categoria degli interessati**
- gli **obblighi ed i diritti del titolare** del trattamento

Il Responsabile del trattamento **NON** può mai determinare le **FINALITA'** del trattamento ma **SOLO I MEZZI**

IL RESPONSABILE DEL TRATTAMENTO – DATA PROCESSOR

Il Titolare del trattamento deve scegliere un responsabile che presenti **GARANZIE SUFFICIENTI** per mettere in atto **MISURE** tecniche ed organizzative adeguate a consentire il RISPETTO DELLE ISTRUZIONI ricevute dal titolare.

Le **GARANZIE** consistono in **CONOSCENZA SPECIALISTICA** e **AFFIDABILITA'**

Se il Titolare del trattamento NON sceglie un responsabile che presenti tali garanzie può essere sanzionato.

Con IL CONTRATTO DI NOMINA il Titolare del trattamento **DELEGA al Responsabile LA CONCRETA GESTIONE DEL TRATTAMENTO**

IL RESPONSABILE DEL TRATTAMENTO – DATA PROCESSOR- OBBLIGHI

OBBLIGHI DEL RESPONSABILE

1. **TRATTARE I DATI PERSONALI SECONDO LE ISTRUZIONI** impartire dal Titolare del trattamento.

   Se NON rispetta le istruzioni diviene egli stesso Titolare del trattamento

2. **GARANTIRE** che le **PERSONE AUTORIZZATE AL TRATTAMENTO si impegnino alla RISERVATEZZA**
3. **ADOTTARE LE MISURE TECNICHE ED ORGANIZZATIVE** individuate dal Titolare del trattamento a seguito della Impact Analisy
4. **ESSERE DISPONIBILE AD AUDIT DI VERIFICA** da parte del Titolare del trattamento

IL RESPONSABILE DEL TRATTAMENTO – DATA PROCESSOR- OBBLIGHI

5. **ASSISTERE il TITOLARE DEL TRATTAMENTO IN TUTTE LE ATTIVITA'**
6. **CANCELLARE E RESTITUIRE I DATI PERSONALI** al termine del trattamento su richiesta del Titolare
7. **DIMOSTRARE** al titolare del Trattamento di **AVERE RISPETTATO OBBLIGHI ED ISTRUZIONI IMPARTITE**

IL RESPONSABILE DEL TRATTAMENTO – DATA PROCESSOR- OBBLIGHI

⑧ NOMINARE SUB- RESPONSABILI DEL TRATTAMENTO

- Tale nomina è facoltativa
- Subordinata ad AUTORIZZAZIONE SCRITTA del Titolare del trattamento
- Il contratto fra Responsabile e Sub-Responsabile deve essere identico a quello fra Titolare e Responsabile
- Il Responsabile nominato dal Titolare risponde dell'operato del sub-responsabile salvo esercizio del diritto di rivalsa
- Il Responsabile del trattamento può nominare il sub-responsabile RESPONSABILE ESTERNO

IL RESPONSABILE DEL TRATTAMENTO – DATA PROCESSOR- OBBLIGHI

⑨ **REGISTRO DEL TRATTAMENTO**

Il Responsabile deve tenere un proprio registro del trattamento nel quale illustra i trattamenti effettuati PER CONTO del Titolare

⑨ **AVVERTIRE** il Titolare del trattamento di un **DATA BREACH**

⑩ **COOPERARE con AUTORITA' DI VIGILANZA**

⑪ **DESIGNARE DPO**

PERSONE AUTORIZZATE AL TRATTAMENTO - INCARICATI

Il Codice della Privacy OBBLIGA il Titolare del Trattamento a NOMINARE PER ISCRITTO gli INCARICATI pena sanzione penale

Con Il GDPR gli incaricati sono definiti **PERSONE AUTORIZZATE AL TRATTAMENTO** coloro che svolgono il trattamento **SOTTO L'AUTORITA' DIRETTA** del Titolare o del Responsabile

Il Regolamento NON prevede espressamente l'obbligo di nomina scritta

Anche se tali figure NON sono espressamente previste NON SONO INCOMPATIBILI con il principio di organizzazione interna e responsabilizzazione

Il Responsabile DEVE garantire che tali persone rispettino il vincolo di RISERVATEZZA

DATA PROTECTION OFFICER

- Il **DPO** è il **RESPONSABILE PROTEZIONE DATI PERSONALI**
- Nuova figura professionale introdotta con il GDPR il quale sostituisce il RESPONSABILE DELLA SICUREZZA DEI DATI
- Risponde ai principi di organizzazione interna e responsabilizzazione di Titolare e Responsabile del trattamento

Puo' essere NOMINATO:

- DPO INTERNO : un dipendente del Titolare o del Responsabile
- DPO ESTERNO : persona fisica o società di consulenza con apposito CONTRATTO DI SERVIZI
- TEAM DPO

DATA PROTECTION OFFICER

OBBLIGO DI NOMINA DEL DPO quando il **TRATTAMENTO DEI DATI PERSONALI** è effettuato da :

1. **AUTORITA' PUBBLICA O ORGANISMO PUBBLICO** ad eccezione degli Organismi Giurisdizionali
2. **SOCIETA' con PIU DI 250 DIPENDENTI**
3. **ATTIVITA' PRINCIPALE** del Titolare o del Responsabile del trattamento consiste nel trattamento di dati personali che **RICHIEDE UN MONITORAGGIO REGOLARE E SISTEMATICO SU LARGA SCALA DEGLI INTERESSATI**

   (es attività di core businees)

DATA PROTECTION OFFICER

4. **ATTIVITA' PRINCIPALE** del Titolare o del Responsabile consiste nel **TRATTAMENTO SU LARGA SCALA DI DATI SENSIBILI O DATI RELATIVI A CONDANNE PENALI O REATI**

   I DATI SENSIBILI sono quei dati che se rivelati provocano un grave danno alla persona. Sono dati che indicano origine razziale etnica religiosa, l'appartenenza a partiti politici , associazioni sindacali. Oggi definiti **DATI DI PARTICOLARE NATURA** che comprendono anche dati genetici biometrici relativi alla salute e al sesso.

Al di fuori di queste ipotesi la nomina NON è obbligatoria

DATA PROTECTION OFFICER

CARATTERISTICHE DEL DPO:

1. **SOGGETTO INDIPENDENTE E AUTONOMO**
2. **NON IN CONFLITTO DI INTERESSI**
3. **NON RICEVE ISTRUZIONI**
4. **NON PUO' ESSERE RIMOSSO**
5. **DEVE AVERE RISORSE FINANZIARIE e STAFF**
6. **NON E' SOGGETTO AL POTERE DISCIPLINARE**
7. **DEVE AVERE CONOSCENZA GIURIDICA ed in SICUREZZA INFORMATICA**
8. **RIFERISCE al CEO** vertice gerarchico di Titolare e Responsabile

DATA PROTECTION OFFICER

9. **TENUTO A SEGRETEZZA E RISERVATEZZA**
10. Deve **REDIGERE UNA RELAZIONE ANNUALE** da sottoporre al Cda
11. può **ESSERE CONTATTATO DALL'INTERESSATO**
12. Può **ESSERE CONTATTATO DAL GARANTE**

- Soggetto quasi permanentemente presente in azienda
- Non sono richieste qualifiche specifiche se non una ottima conoscenza in materia giuridica e di sicurezza informatica
- NON sono rilasciate ATTESTAZIONI PROFESSIONALI

DATA PROTECTION OFFICER

COMPITI DEL DPO:

1. Dare **CONSULENZA** sulla normativa del GDPR a Titolare e Responsabile
2. **VERIFICARE E VIGILARE sul RISPETTO DELE NORME** del Regolamento
3. **SENSIBILIZZARE e FORMARE IL PERSONALE**
4. **DARE PARERI** se richiesto sulla **VALUTAZIONE D'IMPATTO** e sorvegliare sugli adempimenti
5. **PUNTO DI CONTATO CON INTERESSATI E AUTORITA' DI CONTROLLO**
6. **MONITORARE IL DATA BREACH**

GRAZIE DELL'ATTENZIONE!!!

- *AVV. FRANCESCA TRESANINI*