



IL REGOLAMENTO UE (679/2016) SULLA PRIVACY APPLICATO AL SINDACATO

Avv. Marco Giuri
marcogiuri@studiogiuri.it

DATA PROTECTION OFFICER

Responsabile della protezione dei dati

FIGURA NUOVA art 37

ARTICOLO 37 Regolamento

Prevede 3 casi in cui occorre la nomina di questa figura

Dipendente

Consulente

Tutela il Titolare verso i terzi e Autorità Garante Privacy

Data Protection Officer

a) Trattamento effettuato da un'autorità pubblica o da un organismo pubblico

b) Le attività principali sono trattamenti che per loro natura, campo di applicazione e/o finalità, richiedono il CONTROLLO REGOLARE E SISTEMATICO degli interessati su larga scala

c) Le attività principali del responsabile o dell'incaricato consistono nel trattamento SU LARGA SCALA (?) di categorie particolari di dati: sensibili, giudiziari.

d) Negli altri casi è facoltativo.

Data Protection Officer

Caratteristiche:

Qualità professionali, conoscenza specialistica della norma e delle misure di protezione dei dati, capacità di adempiere ai propri compiti.

Può essere dipendente o libero professionista.

Coinvolto in tutte le scelte che hanno a che fare con l'azienda/struttura.

Deve avere ampia autonomia, non riceve istruzioni sui suoi compiti (art 36).

Riferisce al CDA o ai massimi vertici non al Responsabile.

Compiti DPO: Data Protection Officer

1) Informare e **consigliare il titolare** e/o Responsabile nonché i dipendenti/incaricati sugli obblighi del Regolamento

2) **Sorvegliare l'osservanza** del Regolamento e delle politiche del titolare/Responsabile o dell'incaricato, compresi l'attribuzione di responsabilità, la sensibilizzazione e la formazione del personale, attività di audit.

3) **Fornire, SE RICHIESTO, pareri** in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento

Compiti DPO: Data Protection Officer

- 4) **Cooperare con Autorità di controllo**
- 5) Coordinare attività con Autorità di controllo, anche per consultazione preventiva e su altri aspetti

Data Protection Officer

Approfondimento

LINEE GUIDA GRUPPO ART 29
13 DICEMBRE 2016

NEWSLETTER N. 432 del 15 settembre 2017

Tutela della Privacy

DATO PERSONALE

- **Sono dati personali** le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..
- Particolarmente importanti sono: i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

TIPI DATI PERSONALI

Regolamento

Dati sensibili e dati giudiziari

Divieto del trattamento dei dati sensibili:

dati che rivelino **origine razziale**, etnica, **opinioni politiche**, **convinzioni religiose** o filosofiche, appartenenza **sindacale**, **dati genetici**, **biometrici**, **dati su salute e vita sessuale** e **orientamento sessuale**.

Tutela della Privacy

DATO PERSONALE

DATO PERSONALE

***DATO SENSIBILE -
PARTICOLARE***

Tutela della Privacy

Introduzione alla disciplina

Riservatezza come diritto plurifunzionale:

DIRITTI DELL'INTERESSATO

DIRITTO ALLA TUTELA DELLA RISERVATEZZA E
DIGNITA' (DATI PARTICOLARI – EX SENSIBILI)

DIRITTO PROTEZIONE DATI PERSONALI

FONTI NORMATIVE

- **DIRETTIVA 95/46/CE: ABROGATO!**
- **REGOLAMENTO UE 679/2016**
- **CODICE PRIVACY**
- **LINEE GUIDA GARANTE PRIVACY**
- **PROVVEDIMENTI GARANTE**
- **CODICE CIVILE**
- **CODICE PENALE**

Diritto della Protezione dei dati - Regolamento

il Regolamento prevede la privacy delle **persone fisiche** come un **DIRITTO FONDAMENTALE** così come era previsto dalla Direttiva 95/46/EU

Obiettivi del Regolamento UE GDPR

Garantire la certezza del diritto

La Trasparenza agli operatori economici

Garantire a tutti i cittadini UE gli stessi diritti

**Definire stessi obblighi e responsabilità dei
Titolari / Responsabili del trattamento**

Stabilire sanzioni uguali in tutti i Paesi EU

Cooperazione fra Autorità di controllo



Regolamento EUROPEO

Regolamento UE 679/2016

Entrato in vigore il **25 maggio 2018**

Perché Nuovo Regolamento?

- a) Continua evoluzione dei concetti di privacy e protezione dati
- b) Diffusione del progresso tecnologico
- c) Massima diffusione di dati: condivisione dei dati ai massimi livelli

ALCUNE NOVITA' RILEVANTI

Diritto Portabilità

Data Breach

Valutazione d'impatto sulla protezione dei dati

Registri delle attività di trattamento

Consultazione preventiva

Certificazione

Diritto portabilità – articolo 20

L'interessato **ha diritto di ricevere** in un formato strutturato, di uso comune e leggibile a macchina i suoi dati personali forniti ad un Titolare ed **ha il diritto di trasmettere** tali dati ad un altro Titolare del trattamento senza impedimenti qualora:

- a) Il trattamento si basi sul **consenso** **o** su un **contratto** e il trattamento sia effettuato con mezzi automatizzati

Diritto Portabilità

L'interessato può anche richiedere che la trasmissione sia diretta da un titolare ad un altro.

Se alla base non c'è un consenso o un contratto non è ammessa la portabilità: es .
Esercizio funzioni pubbliche.

I RISCHI PER I DATI DEGLI ASSOCIATI

**PERDITA DATI
SOTTRAZIONE
COMUNICAZIONE A SOGGETTI NON
AUTORIZZATI
DISTRUZIONE
MODIFICA NON AUTORIZZATA**

I RISCHI PER I DATI DEGLI ASSOCIATI

Data Breach - Articolo 33

Novità rilevante

In caso di **violazione dei dati personali**, il Titolare del trattamento **notifica** la violazione **all'autorità di controllo competente** senza ingiustificato ritardo, ove possibile **entro 72 ore dal momento della conoscenza**, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.

Se non viene effettuata entro 72 ore, la notifica è corredata di una giustificazione motivata

Contenuto Minimo Notifica Data Breach

- a) DESCRIZIONE natura della violazione, le categorie violate, il numero di interessati
- b) Il nome e le coordinate di contatto del DPO
- c) Descrivere le probabili conseguenze della violazione
- d) Descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione

Obbligo

Il Titolare **documenta** qualsiasi violazione dei dati personali incluse le circostanze in cui si è verificata, le sue conseguenze ed i provvedimenti adottati per porvi rimedio.

ACCOUNTABILITY

Comunicazione all'interessato

Comunicazione di una violazione all'interessato: quando la violazione dei dati è suscettibile di presentare un rischio elevato per i diritti delle persone, il titolare del trattamento comunica la violazione all'interessato **SENZA INGIUSTIFICATO RITARDO. Va usato linguaggio semplice e chiaro per spiegare la violazione.**

Comunicazione all'interessato

Non è richiesta la comunicazione se:

- 1) Il titolare aveva utilizzato le misure tecniche ed organizzative adeguate alla protezione e tali misure hanno difeso i dati oggetto di violazione: es. cifratura - **OPPURE**
- 2) Il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti degli interessati, **O**
- 3) Detta comunicazione comporterebbe sforzi sproporzionati: **si fa comunicazione pubblica**

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Articolo 35: La fa il Titolare del Trattamento.

Regola generale

Quando? (Prima di procedere al trattamento)

Quando un tipo di trattamento, allorchè prevede uso di nuove tecnologie, considerati la natura, il campo di applicazione, il contesto e le finalità del trattamento **può presentare un RISCHIO ELEVATO per i diritti e le libertà delle persone. Chiede un parere a DPO.**

Casi specifici di Valutazione d'Impatto

Regola specifica

Va fatta la valutazione d'impatto in questi casi:

- a) Una valutazione **SISTEMATICA E GLOBALE** di aspetti personali relativi a persone fisiche, basata su trattamento automatizzato, compresa profilazione,
- b) Il trattamento su **larga scala** di dati sensibili o dati giudiziari
- c) La sorveglianza sistematica di una zona accessibile al pubblico su larga scala

Contenuto **Minimo** Valutazione Impatto

- a) Descrizione sintetica dei trattamenti e delle finalità e l'interesse legittimo perseguito dal responsabile del trattamento
- b) Una valutazione della necessità e proporzionalità dei trattamenti rispetto alle finalità
- c) Una valutazione dei rischi per i diritti degli interessati
- d) Le misure previste contro questi rischi

Le misure di sicurezza da adottare sui dati degli iscritti

ESEMPI

Misure fisiche

PROTEZIONE FISICA
ARMADI CHIUSI
CONTROLLO ACCESSI

Misure informatiche

PASSWORD
BACK UP
FIREWALL

Misure organizzative

NOMINE INTERNE
FORMAZIONE

Registri delle attività di trattamento

Articolo 30

Ogni titolare del trattamento e il suo eventuale rappresentante tengono un **registro delle attività di trattamento** svolte sotto la propria responsabilità.

Contenuto Registro

- a) Nome e coordinate contatto del titolare e di ogni corresponsabile, del rappresentante e del DPO (Data Protection Officer)
- b) Le finalità del trattamento
- c) Categoria interessati e categoria dati
- d) Le categorie di destinatari cui saranno comunicati i dati
- e) I trasferimenti dei dati ai Paesi Terzi o organizzazione internazionale
- f) I termini ultimi per la cancellazione dei dati
- g) Una descrizione generale delle misure di sicurezza tecniche ed organizzative

Altro Registro: responsabile

Anche ogni responsabile del trattamento e il suo eventuale rappresentante devono tenere un registro di tutte le categorie di trattamento svolte ***per conto di un titolare del trattamento***

Contenuto registro responsabile

- a) Nome e coordinate di contatto del titolare del trattamento per conto del quale agisce, del rappresentante, del DPO
- b) Le categorie dei trattamenti
- c) I trasferimenti dati all'estero verso Paesi terzi o Organizzazioni internazionali
- d) Descrizione generale delle misure di sicurezza tecniche ed organizzative
- e) **REGISTRI SONO TENUTI PER ISCRITTO**

Trattamento dati particolari

Possibile solo quando ci sono determinati casi:

Consenso esplicito dell'interessato per finalità specifiche

Assolvimento obblighi ed esercitare i diritti specifici del Responsabile o dell'interessato in materia di DIRITTO DEL LAVORO e sicurezza sociale

Necessario per tutelare un interesse vitale dell'interessato o di un terzo se l'interessato si trova in condizione di incapacità fisica o giuridica di esprimere un consenso

Trattamento dati sensibili

- d) **Trattamento effettuato da una fondazione/associazione/organismo SENZA SCOPO di LUCRO che persegua finalità politiche, filosofiche, religiose, sindacali solo per il trattamento sui membri aderenti, ex membri e persone che hanno regolari contatti con essi enti e a condizione che NON siano comunicati a terzi senza consenso dell'interessato**
- e) Trattamento riguarda dati personali resi manifestatamente pubblici dall'interessato
- f) Per la difesa in giudizio o attività svolte da autorità giurisdizionali

Trattamento dati sensibili

- g) Trattamento necessario per motivi di interesse pubblico
- h) Trattamento necessario per finalità prevenzione medica, medicina lavoro, valutazione capacità lavorativa del lavoratore, diagnosi, assistenza sanitaria o sociale, gestione servizi sanitari/sociali
- i) Trattamento necessario per motivi di interesse pubblico nel settore sanità pubblica come minacce gravi per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici
- l) Trattamento per finalità archiviazione nel pubblico interesse e finalità ricerca scientifica

Dati Giudiziari

Trattamento relativo ai dati personali delle CONDANNE PENALI e dei reati o a connesse misure di sicurezza: può avvenire solo sotto il controllo dei pubblici poteri o se il trattamento è autorizzato dal diritto degli Stati membri che preveda adeguate garanzie per i diritti e le libertà degli interessati.

ADEMPIMENTI IN SINTESI NEL SINDACATO

**INFORMATIVE +
CONSENSO**

**NOMINE INTERNE
RESPONSABILI
AUTORIZZATI**

DATA BREACH

DATA PROTECTION OFFICER

**MISURE
DI
SICUREZZA**

ACCOUNTABILITY

REGISTRO DEI TRATTAMENTI