

A man and a woman are standing in a server room, looking at a tablet together. The man is wearing a light blue shirt and the woman is wearing a dark blazer over a white turtleneck. They are both looking at the tablet with interest. In the background, there are server racks with glowing lights and another person is sitting at a desk with multiple monitors.

TPinfinity

# GENERAL DATA PROTECTION REGULATION

GDPR - Regolamento 2016/679

IL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI DELL'UNIONE EUROPEA (GDPR) È UN INSIEME DI REGOLE SU COME LE AZIENDE DEBBANO TRATTARE I DATI PERSONALI DEGLI INTERESSATI.

IL GDPR DEFINISCE LE RESPONSABILITÀ DELLE ORGANIZZAZIONI PER GARANTIRE LA PRIVACY E LA PROTEZIONE DEI DATI PERSONALI, FORNISCE AGLI INTERESSATI DETERMINATI DIRITTI E ASSEGNA POTERI AI REGOLATORI PER CHIEDERE DIMOSTRAZIONI DI RESPONSABILITÀ O PERSINO IMPORRE SANZIONI NEI CASI IN CUI UN'ORGANIZZAZIONE NON RISPETTI I REQUISITI DEL GDPR.

# I Requisiti chiave del GDPR

## 1) Trattamento

### LECITO

- Tutti i trattamenti devono essere basati su uno scopo legittimo

### EQUO

- Le aziende si assumono la responsabilità e non trattano i dati per scopi diversi da quelli legittimi

### TRASPARENTE

- Le società devono informare gli interessati delle attività di trattamento dei loro dati personali

## 2) Limitazione di scopo, dati e archiviazione

### LIMITAZIONE DI SCOPO

- Le aziende non possono trattare dati personali al di fuori degli scopi legittimi per i quali tali dati personali sono stati raccolti

### DATI

- Le aziende non possono richiedere dati personali diversi da quelli necessari

### ARCHIVIAZIONE

- Le aziende devono cancellare i dati personali una volta raggiunto lo scopo legittimo per il quale sono stati raccolti

# I Requisiti chiave del GDPR

## 3) I Diritti degli interessati

Agli interessati è stato dato il diritto di chiedere all'azienda quali informazioni questa abbia su di loro e cosa faccia con queste informazioni. Inoltre, l'interessato ha il diritto di chiederne la rettifica, opporsi al trattamento, presentare un reclamo o anche chiedere la cancellazione o il trasferimento dei propri dati personali

## 4) Il Consenso

Se e quando la società intende trattare i dati personali oltre allo scopo legittimo per cui sono stati raccolti tali dati, è necessario che sia richiesto un consenso chiaro ed esplicito all'interessato. Una volta raccolto, questo consenso deve essere documentato e l'interessato è autorizzato a ritirare il proprio consenso in qualsiasi momento.

Inoltre, per il trattamento dei dati dei minori, il GDPR richiede il consenso esplicito dei genitori (o tutori) se l'età del minore è inferiore ai 16 anni.

## 5) Violazioni dei dati personali

Le organizzazioni devono mantenere un Registro delle Violazioni dei Dati Personali e, in base alla gravità, il regolatore e l'interessato devono essere informati entro 72 ore dall'identificazione della violazione.

## 6) Privacy by design

Le aziende devono incorporare meccanismi organizzativi e tecnici per proteggere i dati personali nella progettazione di nuovi sistemi e processi; cioè, gli aspetti relativi alla privacy e alla protezione dei dati devono essere garantiti per default.

# I Requisiti chiave del GDPR

## 7) La valutazione dell'impatto sulla Protezione dei Dati

Per valutare l'impatto di cambiamenti o azioni nuove, è necessario condurre una Valutazione dell'Impatto sulla Protezione dei Dati quando si avvia un nuovo progetto, cambiamento o prodotto. La Valutazione dell'Impatto sulla Protezione dei Dati è una procedura che deve essere eseguita quando viene introdotta una modifica significativa nel trattamento dei dati personali. Questa modifica potrebbe essere un nuovo processo o una modifica a un processo esistente che altera il modo in cui i dati personali vengono trattati

## 8) Trasferimenti di dati

Il controllore<sup>1)</sup> dei dati personali ha la responsabilità di garantire che i dati personali siano protetti e che i requisiti GDPR siano rispettati, anche se il trattamento viene eseguito da una terza parte. Ciò significa che i controllori hanno l'obbligo di garantire la protezione e la riservatezza dei dati personali quando tali dati vengono trasferiti all'esterno della società, a una terza parte e / o un'altra funzione all'interno della stessa società.

## 9) Il Responsabile della Protezione dei Dati

In caso di trattamento significativo di dati personali all'interno di un'organizzazione, l'organizzazione deve nominare un Responsabile della Protezione dei Dati. Una volta nominato, il Responsabile della Protezione dei Dati ha la responsabilità di consultare la società sulla conformità ai requisiti del GDPR dell'UE

## 10) Consapevolezza e formazione

Per concludere, esiste un numero significativo di requisiti relativi al GDPR dell'UE. È importante comprendere tali requisiti e le loro implicazioni per la tua azienda e implementarli nel contesto della tua azienda. Tale implementazione richiede uno sforzo dedicato, equivalente a quello necessario per sviluppare un progetto.

# Le Figure coinvolte

TITOLARE DEL TRATTAMENTO	RESPONSABILE DEL TRATTAMENTO	INCARICATO DEL TRATTAMENTO	INTERESSATO
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che singolarmente o insieme ad altri, determina le <b>finalità o i mezzi</b> del trattamento dei «dati personali» (art.4 par.1, n.7 GDPR). In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide «perché» e «come» devono essere trattati i dati	E' la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del <u>titolare del trattamento</u> , (art.4 par.1, n.8 GDPR).	E' il <b>sogetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali</b> , sotto l'autorità diretta del <u>titolare</u> o del <u>responsabile</u>	L'interessato (data subject) al <u>trattamento</u> è la <b>persona fisica</b> a cui si riferiscono i <u>dati personali</u> . L'interessato, inoltre, <u>può essere solo una persona fisica e non giuridica, un ente o un' associazione.</u>
Deve rispettare gli obblighi e i principi previsti dalla normativa in materia di protezione dei dati personali	Deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato	Il Regolamento europeo non prevede l'obbligo di nomina o designazione espressa, ma è fondamentale <b>fornire agli autorizzati le istruzioni operative</b> (art.29 GDPR), compreso gli obblighi inerenti le misure di sicurezza, e che sia fornita loro <b>la necessaria formazione</b>	La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al titolare del trattamento. L'interessato può esercitare i suoi diritti anche in un momento successivo in quello in cui ha prestato il consenso, potendo così revocare il consenso già prestato
Decide i trattamenti, le modalità e le finalità	Tratta i dati attenendosi alle istruzioni del titolare, assume responsabilità proprie e ne risponde alle autorità di controllo e alla magistratura	L'autorizzato deve, ovviamente, attenersi strettamente alle istruzioni ricevute, e non deve avere alcuna autonomia	
↓	↓	↓	↓
CLIENTE/TP Infinity	CLIENTE/TP Infinity	INTERVISTATORE	INTERVISTATO

# Le Istruzioni per l'incaricato

## DATO PERSONALE

- Qualsiasi informazione riguardante una persona fisica identificata o identificabile: nome, cognome, data di nascita, numero di telefono, codice fiscale, il numero di conto corrente; e quelle informazioni che permettono di sapere quando, con chi e per quanto tempo ci si è collegati in rete: indirizzo mail, i c.d. file di log.

## DATI SENSIBILI

- Quelli che rivelano origine razziale o etnica, opinioni politiche, convinzioni religiose/filosofiche, appartenenza sindacale, dati relativi alla salute, dati relativi alla vita sessuale e all'orientamento sessuale. Dal 2017 i dati relativi alle **persone giuridiche** non sono più considerati dati personali e non occorre quindi più rendere informativa ed ottenere il consenso nel rapporto fra le aziende

- Effettuare operazioni di trattamento di dati personali soltanto per le finalità e con le modalità strettamente correlate allo svolgimento dell'attività affidata così da istruzioni riportate nei documenti messi a disposizione da TP Infinity nonché alle istruzioni impartite tramite i responsabili della struttura/ufficio a cui è assegnato.
- Accedere solo ai dati strettamente necessari;
- mantenere e garantire la riservatezza sui dati personali conosciuti e trattati per lo svolgimento delle suddette attività, astenendosi dal comunicarli a terzi se non nei casi previsti dalle prassi aziendali od indicati dal responsabile della struttura/ufficio di riferimento;
- astenersi, in caso di cessazione dell'attività, dall'effettuare operazioni di trattamento dei dati personali conosciuti durante lo svolgimento dell'incarico ed, in particolare, dal conservarli, duplicarli, comunicarli, o cederli a terzi;
- informare prontamente la nostra Società su ogni questione rilevante in relazione al trattamento di dati personali effettuato o su eventuali richieste ricevute dalle persone cui si riferiscono i dati;
- attenersi alle istruzioni e misure di sicurezza presenti in regolamenti/linee guida predisposti in ambito aziendale, in modo da evitare i rischi di perdita o distruzione (anche accidentale) dei dati, di trattamento non consentito o non conforme alla finalità per cui i dati sono raccolti, anche nel rispetto degli standard di sicurezza seguiti in ambito societario.
- Controllare e custodire gli strumenti elettronici utilizzati per il trattamento dei dati e i documenti contenenti i dati personali
- Curare la gestione delle credenziali d'autenticazione custodendole diligentemente garantendone la segretezza e l'accesso a terzi

# Thank You

FOR YOUR ATTENTION

[tpinfinity.com](http://tpinfinity.com)