ATTUAZIONE DEL NUOVO REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

NNTT

ESCURA

Cos'è il RGPD?

Perché è obbligatorio per le?

Sanzioni

La figura del Delegato di Protezione dei Dati

Metodologia

Conclusioni

Quali regolamenti sono?

1. **Il Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio, di 27 aprile 2016, sulla protezione de le persone físiche per quanto riguarda al trattamento dei dati personali e alla libera circolazione di questi dati e per il quale viene abrogata la Directiva 95/46/CE (**Regolamento Generale sulla Protezione dei Dati**).

2. **Ptogetto preliminare della Lege Orgánica sulla Protezione dei Dati di Carattere Personale.**

Cos'è il Regolamento Generale sulla protezione dei Dati?

1. Regolamento Generale sulla Protezione dei Dati (RGPD)

- Il Regolamento Europeo sulla Protezione dei Dati unifica e modernizza la normativa europea sulla protezione dei dati, permettendo ai citadini di abbere un miglore controllo dei suoi dati e alle società approfittare al massimo le opportunità di un mercato digitale unico.

- "Sarà obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno Stato membro.

- **Entrerà in vigore il 25 maggio 2018.**

Cos'è il Regolamento Generale sulla protezione dei Dati?

1. **Ptogetto preliminare della Lege Orgánica sulla Protezione dei Dati di Carattere Personale :**

   È stato presentato a Giugno 2017 e dovrebbe essere approvato prima del Marzo 2018.

   Rispetta sempre il Regolamento Generale sulla Protezione dei Dati e chiarisce il suo contenuto.

   Sostituirà l'attuale Legge Organica sulla Protezione dei Dati.

Cosa cambia legalmente?

- La precedente Direttiva Europea 95/46 / CE è abrogata.
- La Legge Organica 15/99 sulla protezione dei dati è abrogata.
- Il Regio Decreto 1720/2007 è abrogato.
- Il Regolamento Generale sulla Protezione dei Dati UE 2016/679 entra in vigore: 25 Maggio 2018.
- Non è necessario trasporre (sarà lo stesso in tutti i paesi dell'UE).

Cosa cambia conceptualmente?

LOPD

-Consenso tacito

-3 livelli: base, medio, alto.

-Registrazione pubblica di file.

-Regolamento esterno

-Misure di sicurezza stabilite nel RD.

-4 Diritti: ARCO

RGPD

-Consenso espresso

-2 livelli: speciale e non speciale.

-Registro interno delle attività

-Autoregolazione.

-Misure di sicurezza definite dalla società.

-6 diritti: ARCO + oblio + portabilità

Come viene dato il consenso?

LOPD

- Manifestazione di volontà
- Tacito, Contrario o negativo, implicito
- Diversi consensi in uno
- Silenzio positivo

RGPD

- Manifestazione di volontà espressa (inequivocabile)
- Non c'è spazio per taciti o presunti consensi
- Ogni consenso separatamente (Privacy by Design).
- Silenzio negativo (Privacy by Default)

Perché è obbligato per le società?

L'articolo 24 RGPD e l'articolo 30. del progetto preliminare:

- **Tutte le società devono nominare un responsabile della protezione dei dati,** che, dopo aver valutato i rischi che il trattamento può generare nei diritti delle persone colpite e, in particolare, nel loro diritto alla protezione, sarà responsabile di stabilire le organizzazioni per garantire ed essere in grado di dimostrare che il trattamento dei dati è conforme ai regolamenti comunitari**.**

¿Qué requisitos tiene que tener el Delegado de Protección Datos?

Art. 45 LOPD

1.- Le infrazioni minori saranno sanzionate con una multa da 900 a 40.000 euro.

2.- Le infrazioni gravi saranno sanzionate con una multa da 40.001 a 300.000 euro.

3.- Le infrazioni molto gravi saranno sanzionate con una multa da 300.001 a 600.000 euro

Art. 83 RGPD

1.- Sanzioni amministrative pecuniarie fino a 10.000.000 €- o, per le imprese, fino al 2% del fatturato totale annuo dell'esercizio precedente, - se superiore.

2.- Sanzioni amministrative pecuniarie fino a un massimo di 20.000.000 €- o, per le imprese, fino al 4% del fatturato totale annuo dell'esercizio precedente, - se superiore..

Quali dati appaiono nel nuovo RGPD?

Nell'articolo 9.1 del RGPD appare la figura della categoria dei dati speciali che la definisce nel seguente modo:

“È vietato trattare dati personali che rivelano l’origine razziali o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o vita sessuale o all'orientamento sessuale della persona"

Quali obblighe appaioo in base al tipo di dati?

Per la categoria di **dati speciali** appaiono gli obblighi di:

- Realizzazione di una **Valutazione d'Impatto** (EIPD).
- **Registro** di Attività.
- Nomina del **Delegato di Protezione dei Dati.**

In cosa consiste la Valutazione d'Impatto?

Raccolto nell'articolo 35 del RGPD, i responsabili devono eseguire una EIPD prima di mettere in pratica quei trattamenti che riguardano dati speciali e che possono comportare un rischio elevato per gli interessati. Dovrebbe essere fatto quando:

1. In base ai dati, sono generati i profili in base al quale vengono prese decisioni che producono effetti legali.

2. Quando si eseguono trattamenti su amplia scala di dati sensibili.

3. Quando esista un'osservazione sistematica su amplia scala di un'area di accesso pubblico.

4. Le autorità per la protezione dei dati vengono obbligate a redigere elenchi aggiuntivi di trattamenti che richiedono un EIPD.

Cos’è il Registro di Attività?

Lo troviamo nell'**articolo 30 del RGPD**:

- Sostituisce la precedente registrazione di file pubblici con l'Agenzia Spagnola per la Protezione dei Dati.

- È registrato internamente nella società: **"Principio di Responsabilità Proattiva"**

Cosa contiene il Registro di Attività?

Deve contenere:

- Nome e informazioni di contatto della società responsabile
- Nome e informazioni di contatto dei gestori dei trattamenti
- Nome e dati del DPO
- Scopi per i quali i dati sono raccolti
- Categorie di parti interessate (elenco dei proprietari con la società)
- Tipi di dati (menzionando se sono speciali)
- Dove applicabile, trasferimenti internazionali
- Base giuridica (motivo per cui ho i dati)
- Se si tratta di dati speciali, documentare valutazione dell'impatto per il proprietario.

Quali misure di sicurezza dovrebbe svolgere la società?

Lo schema delle misure di sicurezza fornite in RD 1720/2007 **NON rimarrà valido automaticamente.**

- Le misure sono decise in base al risultato dell'analisi del rischio.
- Devono essere applicati PRIMA dell'inizio del trattamento.
- Basato sul miglioramento continuo.
- Le misure tecniche e organizzative dovrebbero essere stabilite tenendo conto:
  1. Il costo e lo stato dell'arte
  2. I costi dell'applicazione
  3. La natura, la portata, il contesto e gli scopi del trattamento.
  4. Rischi per i diritti e le libertà delle persone interessate.
- È configurato come un Sistema di Gestione della Privacy basato sull'autoapprendimento e sul miglioramento, che richiede l'autoanalisi del sistema (audit).

Cos’è il Delegato di Protezione dei Dati?

Si trova nell'**articolo 37 del RGPD**:

"Il titolare del trattamento e il responsabile del trattamento designanoo sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giuristizionali;

b) le attività del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicatizione e/o finalit’a, richiedono il monotoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui dell'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

Quali funzioni ha il Delegato per la protezione dei dati?

a) Informare e consigliare il titolare del trattamento o il responsabile del trattamento e i dipendenti che si occupano del trattamento dei dati personali degli obblighi che incombono loro ai sensi del regolamento e di altre disposizioni sulla protezione dei dati dell'Unione o degli Stati membri;

b) Vigila sul rispetto delle disposizioni del regolamento, di altre disposizioni sulla protezione dei dati dell'Unione o degli Stati membri e delle politiche del titolare del trattamento o il responsabile del trattamento, compresa l'assegnazione delle responsabilità, la consapevolezza e la formazione del personale coinvolto nelle operazioni di trattamento e gli audit corrispondenti;

Quali funzioni ha il Delegato per la protezione dei dati?

c) Offrire il consiglio che viene chiesto sulla valutazione dell'impatto relativo alla protezione dei dati e supervisionarne la realizzazione;

d) Cooperare con l'autorità di controllo;

e) Agire come punto di contatto dell'autorità di controllo per questioni relative al trattamento di dati personali inclusa la previa consultazione e consultare, se del caso, su qualsiasi altra questione.

Quali requisiti deve avere il Delegato per la Protezione dei Dati??

a) Vasta esperienza e conoscenza della materia e della interpretazione e adattamento pratico per applicare le norme sulla protezione dei dati, comprese le misure di sicurezza in tutti i processi tecnici e amministrativi e lo sviluppo della società.

b) Conoscenza concreta della materia applicata ai diversi settori.

c) Esperienza e capacità di consigliare alla società di fronte alle ispezioni, ai requisiti delle autorità competenti e davanti qualsiasi tipo di consultazione di terzi interessati dal trattamento dei dati della ragione sociale.

d) Capacità di negoziazione, formazione ed empatia per lavorare con i rappresentanti dei lavoratori e, naturalmente, con i lavoratori della società.

Metodología

1- Nomina del RPD o del DPD.

- La società deve nominare a un Responsabile per la protezione dei dati (RPD) o titolare per la protezione dei dati (TPD), sulla base dall'articolo 37 RGPD.

2- Valutazione del rischio

- L'RPD o una DPD effettueranno una valutazione del rischio e, se del caso (dati appositamente protetti), un'evoluzione dell'impatto sui rischi che potrebbero avere ripercussioni sulla società.

Metodología

3- Registro di attività

- L'RPD o un DPD crea un registro di file interni, insieme alle necessarie misure di sicurezza per proteggere la società dai rischi rilevati.

4- Misure di sicurezza

- Una volta eseguite le procedure di cui sopra, tutto è compilato in un unico documento, che dovrebbe governare il comportamento dei membri dell'organizzazione in termini di protezione dei dati.

Esempi di rischi

Accesso illecito alle informazioni riservate
Furto fisico di informazioni digitali o su supporto cartaceo
Invio di informazioni riservate a terzi senza autorizzazione
Design insufficiente delle misure di sicurezza
Scarsa catena di password di custodia
Fughe accidentale d'informazioni
Intercettazione della documentazione
Intercettazione, accidentale o no, di conversazioni
Non chiudere un'applicazione per computer dopo il suo uso
Divulgazione di dati personali di clienti, lavoratori, fornitori ...

Conclusioni

Tutte le società devono rispettare la normativa comunitaria

Qualsiasi azienda deve sviluppare e conformarsi alle politiche adattate sulla protezione dei dati

Il servizio offerto deve essere adattato alle esigenze richieste dalla legge

I processi sensibili devono essere analizzati e devono crearsi i programmi organizzativi adattati a ogni situazione

Le fasi per l'implementazione delle politiche di protezione dei dati sono basate su una metodologia e sulla partecipazione della società

Le sanzioni che possono essere imposte in caso di non conformità possono raggiungere fino al 4% del fatturato della società