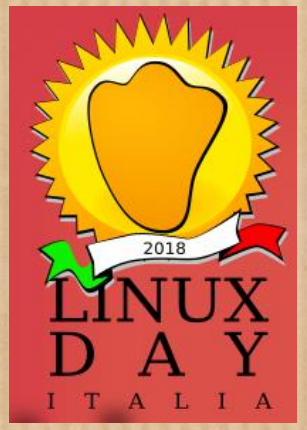
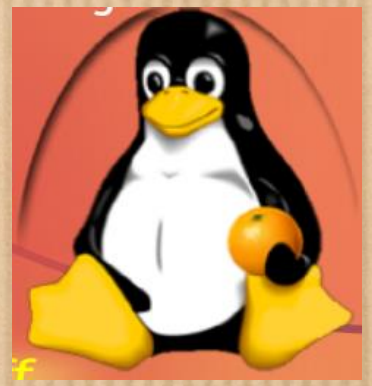


GDPR

Vademecum per le piccole imprese

Patrizia Isaija
info@lineapa.it

Linux day 27/10/2018 Ivrea



Regolamento UE 2016/679

- Entrato in vigore a maggio 2016 - Si applica dal 25/05/2018 in tutti i 28 paesi dell'Unione Europea. Non necessaria una legge nazionale di recepimento

- Contiene norme relative alla protezione delle persone fisiche, in particolare per quanto concerne i dati personali e la loro circolazione.

Applicazione

- Si applica al trattamento:

1. Di dati personali, automatizzato in tutto o in parte
2. Di dati personali contenuti in un archivio, non automatizzato

- Non si applica ai trattamenti :

1. Effettuati dalla persone fisiche per uso personale o domestico
2. Effettuati dalle autorità per i loro scopi

Principi

- Trattati in modo **lecito**, corretto e trasparente;
- Raccolti per **finalità determinate** ed esplicite;
- **Adeguati**, pertinenti e limitati; (minimizzazione dell'uso dei dati)
- **Esatti e aggiornati**;
- **Conservati** per un **tempo limitato**;
- Trattati con adeguate misure di **sicurezza**.

Consenso

Prima di trattare i dati degli utenti il titolare deve raccoglierne il consenso libero, specifico ed informato, ad esempio tramite checkbox come quella per il form di iscrizione alla newsletter

Per chi ha meno di 16 anni

- Per la vendita o forniture di beni e servizi a minori di 16 anni è obbligatorio il consenso esplicito dei genitori o di chi ne fa le veci.

Durata del consenso

- Non sarà più «per sempre» , ma avrà una data di scadenza, a seconda dell'uso specifico dei dati. Dopo quella data dovrà essere rinnovato.
- Le attività di verifica periodica sono da documentare con cadenza almeno annuale.

Diritti dell'interessato

- Trasparenza e informativa
- Accesso
- Rettifica
- Limitazione
- Cancellazione/Oblio
- Portabilità
- Opposizione

Informativa

- L’interessato deve essere informato dell’esistenza del trattamento e delle sue finalità.

Sono da indicare:

- dati titolare;
- dati responsabile trattamento;
- finalità;
- categorie di dati e destinatari dei dati;
- periodo di conservazione dei dati;
- esistenza processo decisionale automatizzato.

Informativa

- Il testo deve essere breve, semplice, comprensibile anche ai minori, senza riferimenti normativi. Dovrà essere facilitata la volontà di aderire al trattamento dei dati. Le informazioni possono essere rese abbinando il testo a icone standardizzate.
- Informativa a strati, in modo graduale (rimandando ad approfondimenti specifici)
- Deve contenere nuovi elementi come l'origine dei dati e il tempo di conservazione previsto.

Attenzione: titolare del trattamento, chi è?

- Titolare del trattamento è **la persona giuridica** e non il rappresentante o l'amministratore unico quale organo della società.

Responsabile del trattamento

- Il Responsabile del trattamento, generalmente una persona fisica o giuridica, è un soggetto che tratta dati personali per conto del titolare del trattamento.
- I rapporti tra titolare e responsabile sono di natura contrattuale-legale.

Come si individua il responsabile

La designazione del responsabile deve contenere:

- materia disciplinata;
- durata del trattamento;
- natura e finalità del trattamento;
- tipologia di dati personali trattati;
- categorie di interessati;
- obblighi e diritti del titolare.

Autorizzato al trattamento

- Figura già prevista nel Codice della privacy e definito come incaricato al trattamento.
- Il Regolamento fa riferimento a "persona fisica autorizzata a compiere operazioni di trattamento dal titolare o responsabile".
- Il titolare del trattamento ha l'obbligo di formare gli addetti autorizzati al trattamento.
- Chiunque agisce sotto l'autorità del titolare, che abbia accesso a dati personali, non può trattare tali dati se non debitamente istruito.

Cose da fare

- Prima di subire una violazione o un furto di dati le imprese devono chiedersi: quali sono i dati che sto custodendo? Quindi analisi dei dati: a cosa servono e come vengono utilizzati.
- Dopo ci si domanda: come vengono conservati i dati?
- In seguito: messa a punto della documentazione. Con la nuova normativa il consenso al trattamento dei dati personali e l'informativa non sono più eterni, vanno aggiornati periodicamente.
- Fare formazione ai dipendenti
- Implementare procedure di contenimento, avviso e informazione per esempio in caso di violazione.
- Adottare una procedura per gestire le richieste di informazione sui dati da parte degli interessati

Cosa contiene il registro dei trattamenti

Il registro deve contenere le seguenti informazioni:

- nome e dati di contatto del titolare;
- finalità del trattamento;
- descrizione di categorie di interessati e dati trattati;
- eventuali trasferimenti di dati verso l'estero;
- se possibile, termini ultimi previsti per la cancellazione dei dati;
- se possibile, descrizione delle misure di sicurezza adottate.

Q&A

Esempio dal mondo e-commerce: se un cliente lascia la propria email per ricevere informazioni sull'ordine, ma non spunta la casella per ricevere comunicazioni di carattere commerciale, come bisogna comportarsi?

Q&A

Esiste una differenza di trattamento tra ipotetici indirizzi info@azienda.it o amministrazione@azienda.it (non immediatamente associabili a persone fisiche) e rossi@azienda.it?

Q&A

Quali sono le autorità preposte a verificare che sia tutto in regola?

Q&A

Come comportarsi con i dati che le aziende divulgano pubblicamente, ad esempio reperibili online?

Q&A

È possibile che esistano dei “contitolari” dei dati?

Q&A

Come ci si comporta nei confronti della raccolta dati per strada, in caso di associazioni e simili?

Q&A

Se utilizzo Google Analytics in modo anonimo il cookie banner è necessario?

- Cookie tecnico: necessario al funzionamento del sito, ad esempio per tenere un prodotto nel carrello o per memorizzare la lingua di navigazione selezionata (funzionalità fondamentali)
- Cookie di profilazione: ad esempio Pixel di FB, per far comparire inserzioni mirate
- Cookie analitico o statistico: se adotto accorgimenti per limitare il potere identificativo di raccolta info del cookie e se mi assicuro che l'eventuale terza parte a cui i cookie analitici vengono erogati non fa incrocio dati con altri dati in suo possesso, allora il cookie analitico è assimilabile a quello tecnico.

Q&A

- I cookie tecnici vanno menzionati nella cookie policy, i cookie di profilazione vanno dettagliati (cookie banner più info estesa) e il trattamento non può iniziare se prima non ho il consenso dell'utente.

Q&A

Ho un DB dal sito con iscrizioni alla mailing list ante GDPR, cosa devo fare per usare questi dati con finalità di marketing?

Q&A

Il consenso effettuato con lo scorrimento della pagine è libero, informato e inequivocabile?

Q&A

- Mettendo la x sul banner non sto negando il consenso, ma sto continuando a navigare, quindi accetto la cookie policy.

- Ho una lista di partecipanti al mio corso con nome cognome e email, posso continuare il rapporto con loro mandando le mie newsletter? NO

Q&A

Quali dati devo registrare come prova del consenso?

Q&A

E’ possibile la raccolta del consenso cartacea?

Q&A

- Se ho sul sito un video youtube, il pulsante share per il like di facebook, delle statistiche anonime, lo spazio per i commenti nella sezione blog, la preferenza relativa alla lingua di navigazione: **sto già trattando dei dati**…
- Quindi devo avere la cookie policy

Per concludere …

Privacy policy

Contenuto, in tutte le lingue in cui è redatto il sito:

- Estremi identificativi titolare del trattamento
- Elenco dati trattati (nome, e mail, statistiche, etc…)
- Modalità a finalità del trattamento
- Diritti degli interessati
- Strumenti terzi utilizzati (es Analytics di Google)

Cookie policy

Contenuto, in tutte le lingue in cui è redatto il sito :

- Descrizione cookies utilizzati nel sito
- Riferimenti a terze parti che installano cookies attraverso il sito (ad es Facebook)
- I link alla informative e ai moduli di opt out delle terze parti

Cookie banner

- Visibile al primo accesso del sito
- Design discontinuo rispetto al sito
- Contiene informativa breve
- Contiene link a informativa estesa (cookie policy)

Blocco preventivo consenso e preferenze

- Gli script che installano cookie di profilazione devono essere preventivamente bloccati e riattivati solo dopo il consenso, che si intende prestato con il proseguimento della navigazione (un click sulla pagina)
- Le preferenze dell'utente possono esser registrate in modo da non erogare il cookie banner e il blocco preventivo dei codici ad ogni successiva visita

Cookies: esempio di disclaimer

La Cookie Law richiede il consenso informato degli utenti prima di installare cookie sui loro dispositivi e di iniziare il tracciamento.

- Questo sito usa i cookie per poterti offrire una migliore esperienza di navigazione. I cookie permettono di conteggiare le visite in modo anonimo e non permettono in alcun modo di identificarti direttamente. Clicca su OK per chiudere questa informativa, oppure approfondisci cliccando su "Privacy & Cookie policy completa".

- https://www.iubenda.com/privacy-policy/739746/legal

Privacy aziendale

I soggetti coinvolti nel trattamento dei dati (ad es i dipendenti) devono essere nominati addetti o responsabili.