Commissione europea

Sette passi per le imprese

per prepararsi al Regolamento generale sulla protezione dei dati

Giustizia e consumatori

A chi interessa?

Questa guida ha lo scopo di aiutare le aziende che non gestiscono i dati personali come attività principale, come le PMI che trattano principalmente i dati personali dei loro dipendenti o conservano elenchi di clienti. Sono coinvolti anche i commercianti e i negozi, come le panetterie e i macellai, oppure i fornitori di servizi come gli architetti. Questa guida evidenzia i pochi passi da compiere per prepararsi al regolamento.

I dati personali sono tutte le informazioni che riguardano una persona vivente e reale (non entità giuridiche). Comprendono, ad esempio: nome, cognome, indirizzo di casa, indirizzo e-mail o dati sulla posizione dalla mappa sul tuo cellulare. Generalmente, sono i dati che potresti aver raccolto sui tuoi dipendenti, clienti o fornitori.

Minore è il coinvolgimento della tua attività con i dati personali, meno dovrai fare

Applica i principi chiave:

- **raccogli i dati personali per una finalità ben definita e non usarli per qualcos'altro** (se comunichi ai clienti di darti la loro e-mail in modo da poter ricevere le tue nuove offerte o promozioni, non puoi usare questa e-mail per nient'altro o vendere questa informazione a un'altra società);
- **non raccogliere più dati di quelli che ti servono** (se fai la consegna a domicilio, hai bisogno ad esempio di un indirizzo, un nome sul campanello, ma non hai bisogno di sapere se questa persona è sposata o single) e sii consapevole dei dati personali sotto il tuo controllo.

PASSO 1 — CONTROLLA I DATI PERSONALI CHE RACCOGLI E TRATTI, LO SCOPO PER CUI LO FAI E SU QUALE BASE GIURIDICA

Hai **dipendenti**; stai trattando i loro dati personali in base al contratto di lavoro e in base agli obblighi legali (es. segnalazione alle autorità fiscali / sistema previdenziale).

Puoi gestire un elenco di **clienti singoli**, ad esempio per inviare loro avvisi su offerte speciali / annunci se hai ottenuto il consenso da questi clienti.

Non hai sempre bisogno del consenso. Infatti, ci sono casi in cui le persone si aspettano che tu tratti i loro dati: ad esempio, un venditore di pizze può usare l'indirizzo di consegna per pubblicizzare uno dei suoi nuovi prodotti. Si tratta in questo caso di «interesse legittimo». Devi però informare le persone circa l'uso previsto e interrompere il trattamento di tali dati se ti dicono di farlo.

Se gestisci un elenco di **fornitori** o **clienti aziendali**, lo fai in base ai contratti che hai con loro. I contratti non sono necessariamente in forma scritta.

PASSO 2 — INFORMA I TUOI CLIENTI, DIPENDENTI E ALTRI SOGGETTI QUANDO RACCOGLI I LORO DATI PERSONALI

Le persone devono sapere che si stanno trattando i loro dati personali e per quale finalità.

Ma non c'è bisogno di informare le persone quando hanno già informazioni su come userete i dati, ad esempio quando un cliente ti chiede di effettuare una consegna a domicilio.

Se te lo chiedono, devi anche informare le persone dei dati personali che conservi su di loro e dare loro accesso ai dati. Mantieni i dati in ordine, in modo che quando ad esempio un tuo dipendente ti chiede quale tipo di suoi dati personali detieni, puoi fornirli facilmente senza alcun problema.

PASSO 3 — CONSERVA I DATI PERSONALI SOLTANTO PER IL TEMPO NECESSARIO

Dati sui dipendenti: fintanto che sussiste il rapporto di lavoro e gli obblighi legali connessi.

Dati sui clienti: finché dura il rapporto con il cliente e i relativi obblighi legali (ad esempio a fini fiscali).

Cancella i dati che non sono più necessari per le finalità per cui li hai raccolti.

PASSO 4 — PROTEGGI I DATI PERSONALI CHE STAI TRATTANDO

Se conservi questi dati su un **sistema IT**, limita l'accesso ai file contenenti i dati, ad esempio tramite una password. Aggiorna regolarmente le impostazioni di sicurezza del sistema.

(Nota: il regolamento non prescrive l'utilizzo di alcun sistema IT specifico)

Se archivi documenti fisici con dati personali, assicurati che non siano accessibili da persone non autorizzate; chiudili in cassaforte o in un armadio.

PASSO 5 — CONSERVA LA DOCUMENTAZIONE SULLE TUE ATTIVITÀ DI TRATTAMENTO DEI DATI

Prepara un breve documento che spiega quali dati personali conservi e per quali motivi. Potresti dover presentare la documentazione disponibile all'autorità nazionale per la protezione dei dati, se lo richiede.

Tali documenti devono includere le informazioni elencate di seguito.

INFORMAZIONI	ESEMPI
Le finalità del trattamento dei dati	Avvisare i clienti su offerte speciali / fornire consegne a domicilio, pagare i fornitori, paghe e previdenza sociale per i dipendenti
I tipi di dati personali	Dati di contatto dei clienti, dati di contatto dei fornitori, dati dei dipendenti
Le categorie di soggetti interessate	Dipendenti, clienti, fornitori
Le categorie di destinatari	Enti per l'impiego, enti fiscali
La durata dell'archiviazione	I dati personali dei dipendenti fino alla fine del contratto di lavoro (e relativi obblighi legali); i dati personali dei clienti fino alla fine del rapporto con il cliente / contrattuale
Le misure tecniche e organizzative di sicurezza per proteggere i dati personali	Soluzioni di sistema IT regolarmente aggiornate; armadio chiuso / cassaforte
Se i dati personali sono trasferiti a destinatari al di fuori dell'UE	Ricorrere a un responsabile del trattamento al di fuori dell'UE (ad esempio per la conservazione nel cloud)

PASSO 6 — ACCERTATI CHE IL TUO SUB-APPALTATORE RISPETTI IL REGOLAMENTO

Se subappalti il trattamento dei dati personali a un'altra società, utilizza solo un fornitore di servizi che garantisca il trattamento conformemente ai requisiti del regolamento (ad esempio per le misure di protezione). Prima di firmare un contratto, controlla se è già stato modificato e adattato al regolamento e inserisci questo elemento nel contratto.

PASSO 7 — VERIFICA SE LE SEGUENTI DISPOSIZIONI TI RIGUARDANO

> Per proteggere meglio i dati personali, le società potrebbero dover nominare un responsabile della protezione dei dati. **Tuttavia, non è necessario designare un responsabile della protezione dei dati** se il trattamento di dati personali non è una parte fondamentale della tua attività, non è un trattamento rischioso e la tua attività non opera su larga scala.

Ad esempio, se la tua impresa raccoglie solo dati sui clienti per la consegna a domicilio, non è necessario nominare un responsabile della protezione dei dati.

Anche se è necessario avvalersi di un responsabile della protezione dei dati, potrebbe essere un dipendente già assunto incaricato di questa mansione in aggiunta alle sue altre attività, oppure un consulente esterno, così come molte imprese usano contabili esterni.

> **Normalmente non è necessario eseguire una valutazione dell'impatto sulla protezione dei dati**

Tale valutazione d'impatto è riservata a coloro che presentano maggiori rischi per i dati personali, ad esempio chi effettua una sorveglianza su vasta scala di un'area accessibile al pubblico (ad esempio, la videosorveglianza).

Se sei una piccola azienda che gestisce gli stipendi dei dipendenti e un elenco di clienti, non è necessario eseguire una valutazione dell'impatto sulla protezione dei dati per tali operazioni.

Sanzioni

Le autorità di controllo della protezione dei dati hanno il potere di sanzionare le violazioni delle norme sulla protezione dei dati. Possono adottare misure correttive (come un'ordinanza o una sospensione temporanea del trattamento) e / o comminare una sanzione.

La loro decisione di comminare una sanzione deve essere proporzionata e basata su una valutazione di tutte le circostanze del singolo caso.

Se decidono di comminare una sanzione, l'importo dipenderà anche dalle circostanze del caso, compresa la gravità dell'infrazione o se l'infrazione era intenzionale o frutto di negligenza. Considereranno anche il tuo atteggiamento e le tue intenzioni.

Se desideri ottenere maggiori informazioni:

1. **Visita la guida online della Commissione europea sulla riforma della protezione dei dati, disponibile in tutte le lingue dell'UE:**

   europa.eu/dataprotection/it

2. **Consulta l'Autorità nazionale per la protezione dei dati:**

   edpb.europa.eu/about-edpb/board/members_it

AVVISO IMPORTANTE

Le informazioni contenute in questa guida hanno lo scopo di contribuire a una migliore comprensione delle norme dell'UE sulla protezione dei dati.

Esse sono intese esclusivamente come strumento di orientamento: solo il testo del regolamento generale sulla protezione dei dati ha forza legale, pertanto solo il regolamento può dare luogo a diritti e obblighi per le persone. Questa guida non dà luogo ad alcun diritto o aspettativa esecutiva.

L'interpretazione vincolante della legislazione dell'UE è di competenza esclusiva della Corte di giustizia dell'Unione europea. Le opinioni espresse in questa guida non possono pregiudicare la posizione che la Commissione potrebbe assumere dinanzi alla Corte di giustizia.

Né la Commissione europea né alcuna persona che agisca per conto della Commissione è responsabile per l'uso che può essere fatto delle informazioni presenti in questa guida.

Poiché questo documento riflette lo stato dell'arte al momento della sua stesura, dovrebbe essere considerato come uno «strumento vivente» aperto al miglioramento e il suo contenuto potrebbe essere soggetto a modifiche senza preavviso.

Ufficio delle pubblicazioni

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2018

Print	PDF
ISBN 978-92-79-85397-5	ISBN 978-92-79-85385-2
doi:10.2838/977340	doi:10.2838/61135
DS-02-18-544-IT-C	DS-02-18-544-IT-N