POLIGRAFICO E ZECCA DELLO STATO ITALIANO

A cura dello STUDIO LEGALE LISI

DATI PERSONALI: UN PATRIMONIO DA CUSTODIRE CON ATTENZIONE

Secondo il Regolamento UE 679/2016 (General Data Protection Regulation) la protezione dei dati personali deve animare qualsiasi scelta nella nostra struttura. Questo concetto si esprime nella

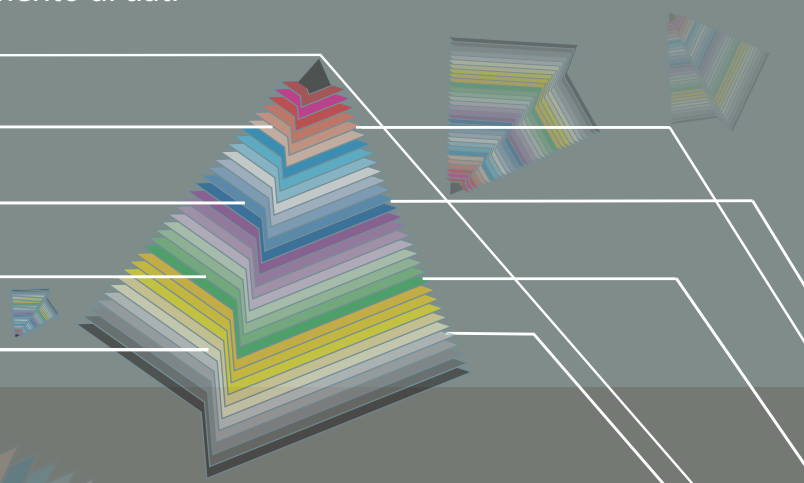
PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE (PRIVACY BY DESIGN) E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA (PRIVACY BY DEFAULT)

Privacy by design: è un approccio che consiste nel prevenire le criticità e i rischi legati alla protezione dei dati personali, che devono essere valutati sin dalla fase di progettazione di qualsiasi progetto innovativo

Privacy by default: è un approccio in base al quale per impostazione predefinita si dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario all'espletamento delle finalità di trattamento.

Questi principi devono animare qualsiasi trattamento di dati personali e vanno valutati in relazione:

- alla quantità dei dati personali raccolti
- alla portata del trattamento
- al periodo di conservazione
- all'accessibilità



"Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro".

Stefano Rodotà

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

A cura dello STUDIO LEGALE LISI

DATI PERSONALI: UN PATRIMONIO DA CUSTODIRE CON ATTENZIONE

ALCUNI ASPETTI DA VERIFICARE IN RELAZIONE ALL'UTILIZZO O ALLA FORNITURA DI UN SERVIZIO IT

- Che attività di trattamento sono consentite dal software?
- È consentita la separazione dei dati?
- È consentita la portabilità in formato interoperabile/riutilizzabile dei dati?
- È consentita la «limitazione» nel trattamento del dato in caso di richiesta?
- È prevista l'automatica cancellazione dei dati dopo un tempo stabilito?
- Ci sono strumenti di anonimizzazione/pseudoanonimizzazione?
- In caso di soluzione in cloud i server sono dislocati in Europa?
- È previsto un accesso selettivo ai dati previo inserimento di id e password?
- Le password sono robuste? Il sistema ne prevede in automatico il cambio?
- Sono previste politiche di autorizzazione differenziata per profilo utente nella gestione dei database?
- È prevista una gestione dei log?
- È previsto una gestione dei report in caso di data breach?
- Chi opererà sviluppo e manutenzione? Sono previsti dei subfornitori?

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

A cura dello STUDIO LEGALE LISI

DATI PERSONALI: UN PATRIMONIO DA CUSTODIRE CON ATTENZIONE

I CONSIGLI PER LA PROTEZIONE DEI DATI PERSONALI NEI SERVIZI CLOUD

- Individuare correttamente le misure di sicurezza che ha adottato il cloud provider per proteggere i dati
- Identificare il reale fornitore del servizio in cloud (singola società o più società consorziate che collaborano?)
- Verificare i piani di business continuity (verificare nel dettaglio i tempi di ripristino del sistema) e disaster recovery (esistono piani di emergenza per i servizi essenziali forniti dal cloud provider?)
- Viene garantita una accessibilità a tutto il sistema o parte di esso in caso di problemi di connettività ad Internet?
- Controllare la separazione (e quindi il grado di riservatezza) dei data base rispetto all'utilizzo comune con altre società dei server forniti nel servizio cloud
- Determinare in quale Stato sono conservati i dati conservati nella "nuvola"
- Accertare l'esportabilità del database in caso di cessazione del servizio fornito
- Concordare con il cloud provider forme di risarcimento in caso di perdita di dati e precisare i livelli di servizio forniti
- Ricordarsi che risponde sempre il titolare del dato in caso di violazioni privacy commesse dal cloud provider!
- Nominare il cloud provider come responsabile del trattamento
- Verificare il livello di professionalità del personale del cloud provider
- Verificare i livelli di accountability forniti dal cloud provider

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

A cura dello STUDIO LEGALE LISI

DATI PERSONALI: UN PATRIMONIO DA CUSTODIRE CON ATTENZIONE

Il Data Protection Officer deve essere il Vostro punto di riferimento in caso di dubbi sulla protezione dei dati personali!

QUINDI DEVE ESSERE COINVOLTO TEMPESTIVAMENTE IN OGNI QUESTIONE ATTINENTE ALLA PROTEZIONE DEI DATI

Quando è opportuno coinvolgere il DPO:

- Istituzione e tenuta del Registro delle attività di trattamento per il Titolare o il Responsabile (art. 30 GDPR)
- Scelta e adozione delle misure di sicurezza tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio di trattamento (art. 32 GDPR)
- In caso di data breach, per la valutazione circa la necessaria notifica all'Autorità di controllo o la comunicazione agli interessati (artt. 33 e 34 GDPR)
- Scelta di aderire a Codici di condotta o a processi per il conseguimento di certificazioni (artt. 40 e 42 GDPR)
- Valutazione degli adempimenti per il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, ad es. per trattamenti realizzati attraverso servizi IT che utilizzano sistemi cloud (artt. 44 e ss. GDPR)

Occorrerà garantire:

- che il DPO sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello
- la presenza del DPO ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il DPO deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea
- che il parere del DPO riceva sempre la dovuta considerazione
- che il DPO sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente

Grafica: Marcello Moscara