Nuova LPD - Riassunto

Dati

La sicurezza dei dati è da capirsi a 360 gradi

Il diritto svizzero si allinea a quello Europeo mentre la decisione da parte EU è in attesa e questo per un motivo di competitività della piazza svizzera

Principio degli effetti

- si applica a tutte le società, anche straniere, che operano in CH

Le società straniere devono nominare un rappresentante in CH se il trattamento dei dati:

- si basa sulla profilazione in base a merci o prestazioni
- avviene su larga scala
- deve essere periodico
- comporta un rischio elevato per la personalità

Dato personale –>art. 5 a,c

- Introduce anche la nuova normativa: DNA, dati biometrici, …

Profilazione a rischio elevato –> art. 5 g

- Comporta un rischio elevato per la persona
- Deve essere dato consenso espresso

Profilazione

- raccolta automatizzata di dati (tracciamento, marketing, …)

Titolare del trattamento –> art. 5 j

Obbligo di informare –> artt. 19, 20, 21

- Informativa di facile accesso e adeguato
- Es. QR-CODE per accesso all'informativa non sempre adeguata (persona anziana)
- È meglio dimostrare che si prende a cuore la materia di protezione dei dati –> trasparenza

Responsabile del trattamento –> art. 5k

- Se il titolare del trattamento dati nomina una società o persona esterna
- Deve sottoscrive un contratto di servizio che deve essere personalizzato
- Il titolare deve garantire che il responsabile garantisca la sicurezza dei dati
- Il titolare, se in contratto, dovrebbe eseguire audit e/o controlli sul responsabile nominato

In dati devo essere trattati in modo lecito –> artt. 6, 30, 31

- Il consenso della persona interessata deve essere espresso
- Obbligo di legge
- Interesse preponderante
- Deve essere conforme alla buona fede
- Deve essere proporzionale allo scopo (i.e. per la newsletter non serve la carta di identità)
- I dati devo essere cancellati quando richiesto
- I dati devo essere esatti e sono responsabilità dell'organizzazione (es. documenti scaduti)

Privacy by design e by default –> art. 7

Diritti delle persone interessate –> artt. 25, 26, 27, 28, 32

- La fornitura deve essere di norma gratuita ma si può richiedere un compenso
- Linguaggio chiaro e semplice
- Deve essere comunicato entro 30 giorni questo anche in caso di differimento
- Devo esserci delle **procedure** perché le richieste vanno evase in un tempo limite

Portabilità

- I dati devono essere RAW (presentati senza alterazioni)
- Sono esclusi dati elaborati e/o analizzati da titolare ma posso essere richieste delucidazioni sulla natura di dati sintetici

Consulente per la PDD –> art. 10

- Deve partecipare alla stesura della PDD in un'organizzazione
- Deve avere delle conoscenze multidisciplinari (IT, PR, Leggi)
- La nomina è facoltativa ma fortemente raccomandata e strategica

Provvedimenti e sanzioni

Incaricato Federale -> artt. 3, 49, 50, 51, 52, 55, 58

- Può avviare delle inchieste
- Può ordinare perizie, controlli, accessi ai dati, interrogatori, accesso ai locali
- Sospendere e/o vietare la trasmissione dei dati
- Può richiedere di distruggere i dati in possesso (es. i dati di tutti i clienti)

Disposizioni penali -> artt. 60,61,62,63,64

- Multa fino a 250k che andrà pagata dalle persone fisiche (CEO, Proprietario, Manager, …)
- La multa viene solo comminata alle persone fisiche a dolo conclamato
- Se la multa è fino a 50k di norma potrà essere pagata dall'azienda

Obblighi

Registro attività di trattamento -> art. 12

- Essenziale per avere una mappa di tutte le attività
- Obbligatorio con più di 250 dipendenti, con dati ad alto rischio e raccolta dati su vasta scala

Sicurezza dei dati -> artt. 7, 8

- Deve essere garantita la sicurezza dei dati da possibili violazioni

Linee guida OPDa -> artt. 1,2,3

- Integrità
- Tracciabilità
- Confidenzialità
- Disponibilità

La normativa NON è retroattiva.

La tracciabilità NON è necessaria se questa è automatizzata

Art. 7

- Privacy by design
- Best practices
- Proporzionalità
- Rischio
- Privacy by default
- Minimizzazione

Art. 8

- Requisiti Minimi

Valutazione d'impatto

- Se I dati posso comportare un rischio elevato
- Prodotti e sistemi certificati secondo **art. 13**
- Si avvale di un codice di condotta

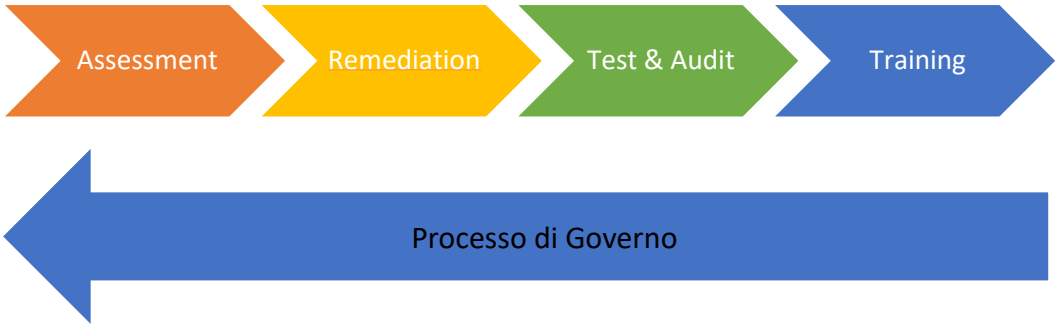
Notifica di violazione -> art. 24

- La notifica deve essere immediata (incaricato federale) se vi è il rischio di violazione dei dati
- Le **procedure** sono essenziali per non perdere tempo in caso di violazione
- Verrà istituita un portale online per la notifica delle violazioni

Paesi esteri

Al momento, verso I paesi che non garantiscono la protezione dei dati (USA, Cina, …) vanno presi delle misure preventive attendendo un accordo tra stati per garantire la trasparenza nelle nostre azioni.

Esempio Governance progetto di adeguamento



ISO/IEC 27001/2 2022

La revisione 2022 può essere un'ottima base per implementare e conformarsi alla nLPD

In particolare, i controlli negli annessi A e B prevedono una serie di controlli revisionati dalla versione 2013 e aggiunti che trattano molto da vicino GDPR e nLPD.

I nuovi controlli aggiunti in 27002:2022 si chinano in dettaglio su questo punto.