Stato della revisione della legge svizzera sulla protezione dei dati (LPD) – Entrata in vigore del regolamento generale europeo sulla protezione dei dati (RGPD UE)

Nella prima parte del presente scritto vi informiamo sullo stato attuale di questa revisione della legge svizzera. Contemporaneamente, nella seconda parte richiamiamo la vostra attenzione sul regolamento generale sulla protezione dei dati dell'Unione Europea che entrerà in vigore il 25 maggio 2018 e che in parte sarà valido anche per le imprese svizzere. Le relative conclusioni e raccomandazioni sono reperibili a pagina 3.

Stato della revisione della legge svizzera sulla protezione dei dati (LPD)

Come ha reso noto la Commissione delle istituzioni politiche del Consiglio nazionale il 13 aprile 2018 (comunicato stampa accessibile all'indirizzo: https://www.parlament.ch/press-releases/Pages/mm-spk-n-2018-04-13.aspx), quest'ultima ha deciso di affrontare la revisione della legge sulla protezione dei dati in due fasi. In una prima fase verranno intrapresi i necessari adeguamenti alla direttiva Schengen relativa al trattamento dei dati personali nell'ambito del diritto penale. Solo nella seconda fase verrà inclusa la revisione totale della legge sulla protezione dei dati che riguarderà tutti i trattamenti di dati da parte di privati e organi della Confederazione. Nel corso della sessione estiva, il Consiglio nazionale si occuperà degli adeguamenti previsti dalla 1ª tappa (direttiva Schengen) e deciderà nel contempo se accettare la suddivisione della revisione della legge sulla protezione dei dati.

Il Consiglio nazionale è la camera prioritaria: ciò significa che successivamente il disegno di legge verrà discusso anche dal Consiglio degli Stati.

Di conseguenza, attualmente un'entrata in vigore in Svizzera delle disposizioni rilevanti per i nostri soci della revisione totale della legge sulla protezione dei dati non è prevista prima della metà o, più probabilmente, della fine del 2019.

Entrata in vigore del regolamento generale europeo sulla protezione dei dati (RGPD UE)

Il RGPD UE diventerà legge valida in tutti gli stati membri dell'UE in data **25 maggio 2018**. La seguente panoramica illustra cosa questo significhi per le imprese svizzere, chiarendo se esse sono soggette a obblighi, e nel caso a quali.

A. Campo di applicazione del RGPD UE

Il campo di applicazione del RGPD UE è molto ampio e si estende anche al di fuori dei confini dell'UE. Giusta l'art. 3 RGPD UE, il regolamento è applicabile a un'impresa svizzera se questa si occupa di trattare i dati personali di persone fisiche residenti nell'Unione Europea, quando le attività di trattamento dell'impresa svizzera riguardano:

1. l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
2. il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

AGVS/UPSA
Wölflistrasse 5, Postfach 64, 3000 Bern 22
Telefon 031 307 15 15, Fax 031 307 15 16
info@agvs-upsa.ch, www.agvs-upsa.ch

Per stabilire se sussiste **un'offerta di beni o una prestazione di servizi**, è sufficiente che l'impresa (svizzera) *manifesti un'intenzione evidente* di offrire beni o prestare servizi alle persone interessate nell'UE.

Indizi di una simile intenzione risultano da fattori come ad es. l'utilizzo di una lingua o di una valuta che è in uso nello stato membro dell'UE ma non in Svizzera, in combinazione con la possibilità di ordinare beni e servizi in questa altra lingua, oppure l'accenno ad altri clienti o utenti che si trovano nell'Unione. La semplice accessibilità del sito web di un'impresa svizzera dall'UE non è invece ancora considerato un indizio che confermi l'intenzione di questa impresa di voler offrire beni o servizi nell'Unione.

L'intenzione di voler **monitorare il comportamento delle persone interessate all'interno dell'Unione** attraverso il trattamento dei dati viene ad es. confermata dal fatto che le attività internet di queste persone venano tracciate (ad es. Google Analytics) e/o che vengano utilizzate tecniche per la profilazione di persone fisiche che analizzano o prevedono ad es. preferenze personali, comportamenti o abitudini delle stesse.

È chiaro dunque che il campo di applicazione del RGPD UE è molto ampio e che anche le imprese svizzere sono tenute a verificare se sono soggette a queste nuove regole. I seguenti esempi selezionati relativi agli obblighi delle imprese derivanti dal RGPD UE mirano a fornire solo una prima impressione e non devono assolutamente essere considerati come una lista di controllo completa.

B. Obblighi per le imprese

Informazione e consenso della persona interessata

Contrariamente a quello svizzero, nel diritto della protezione dei dati dell'UE vale il cosiddetto "divieto con riserva di consenso". Ciò significa che il trattamento dei dati è sostanzialmente vietato, a meno che non sia espressamente consentito da una legge o che la persona interessata abbia dato il suo consenso al trattamento. La persona interessata può in qualsiasi momento revocare il proprio consenso. Occorre garantire che tale revoca possa essere effettuata con la stessa facilità del consenso stesso.

"Privacy by design" e "privacy by default"

Il principio "privacy by design" (protezione dei dati fin dalla progettazione) significa che già all'atto della progettazione il responsabile deve prevedere un sistema di trattamento dei dati volto a minimizzare e a prevenire una violazione della protezione dei dati. Ad es. occorre prevedere una regolare cancellazione dei dati o una loro pseudonimizzazione per impostazione predefinita.

Il principio "privacy by default" (protezione dei dati per impostazione predefinita) significa che per impostazione predefinita devono essere trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Ad es. un sito web deve sostanzialmente consentire la possibilità di fare acquisti senza bisogno di creare un account utente.

Nomina di un rappresentante nell'UE

Sostanzialmente, le imprese svizzere che rientrano nel campo di applicazione del RGPD UE sono tenute a nominare un rappresentante nell'UE. Questo obbligo decade se il trattamento è occasionale, quando non vengono trattate categorie particolari di dati e quando è improbabile che il trattamento presenti un rischio per i diritti e le libertà delle persone fisiche.

Registro delle attività di trattamento

Il responsabile deve tenere un registro delle attività di trattamento svolte presso l'impresa. In particolare, si tratta di una documentazione o panoramica relativa a tutti i processi aziendali utilizzati per il trattamento dei dati personali. Il registro deve contenere tutte le principali informazioni sul trattamento dei dati, come ad es. le categorie di dati, la cerchia delle persone interessate, la finalità del trattamento ed eventuali destinatari dei dati.

Obbligo di denuncia: notifica di una violazione dei dati personali

Eventuali violazioni dei dati personali devono essere denunciate all'autorità di controllo, se possibile entro 72 ore. L'obbligo di denuncia non sussiste quando è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Spesso è necessario informare anche le persone interessate.

Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è necessario effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di adeguate misure per attenuare il rischio, è necessario consultare l'autorità di controllo.

Conseguenze della violazione dei dati personali

La massima sanzione amministrativa pecuniaria può arrivare fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. In questo caso vale in fatturato annuo dell'intero gruppo, non quello di una singola persona giuridica. Il RGPD UE prevede inoltre la possibilità di un'azione legale di categoria, grazie alla quale in futuro le associazioni dei consumatori potranno far valere i diritti delle persone interessate.

C. Conclusioni e raccomandazioni

Il campo di applicazione del RGPD UE è molto ampio e anche le imprese svizzere sono tenute a verificare se devono rispettare queste nuove regole. Gli esempi di obblighi per le imprese derivanti dal RGPD illustrati brevemente in alto UE forniscono una prima impressione sulle conseguenze di questo regolamento dell'Unione. Considerando l'ammontare non irrilevante delle sanzioni, si invitano le imprese svizzere a prendere sul serio il rispetto di questo nuovo regolamento.

Nel frattempo sono già disponibili strumenti gratuiti e molto utili per verificare se il RGPD UE è applicabile alla propria impresa, che forniscono anche un sostegno sulle eventuali misure necessarie:

- per un primo breve test (circa 6 min): protezione dei dati "Online Check" di economiesuisse, accessibile all'indirizzo: https://www.economiesuisse.ch/it/datenschutz-online-check.
- più dettagliato e preciso: il Self Assessment Tool sulla protezione dei dati, accessibile all'indirizzo: www.dsat.ch. DSAT è stato sviluppato da David Rosenthal dello studio Homburger, che si occupa della parte redazionale insieme a David Vasella dello studio Walder Wyss.