Sviluppi normativi

Recenti sviluppi normativi

Ultimo aggiornamento: maggio 2024

pwc

Contenuti

1 Altri sviluppi

1.1 Regolamento generale sulla protezione dei dati dell'UE (RGPD)

Il RGPD introduce un rigoroso quadro giuridico per la protezione dei dati e la privacy all'interno e all'esterno dell'Unione europea in materia di trattamento dei dati personali. Il regolamento è stato adottato dagli Stati SEE.

Stato:
- in vigore dal 25 maggio 2018

Applicabilità delle disposizioni UE più rigide in materia di protezione dei dati

Il Regolamento generale sulla protezione dei dati (RGPD-UE, anche noto con l'acronimo inglese GDPR per General Data Protection Regulation), in vigore dal 25 maggio 2018, ha delineato nei 28 Stati membri dell'Unione europea (UE) un nuovo quadro normativo per quanto concerne le leggi sulla protezione dei dati e sostituito la precedente direttiva dell'UE sulla protezione dei dati.

Il RGPD-UE implementa condizioni quadro giuridiche molto severe per la protezione dei dati e la sfera privata all'interno e all'esterno dell'Europa in relazione al trattamento dei dati personali. Con la delibera del Comitato misto SEE del 6 luglio 2018, il RGPD è stato recepito nell'accordo SEE e dal 20 luglio 2018 è valido anche in Islanda, Norvegia e nel Principato del Liechtenstein.

Il percorso di Compliance

Le nuove disposizioni del RGPD-UE richiedono alle imprese un'analisi della situazione nonché l'aggiornamento dei sistemi e dei processi operativi relativi alla protezione dei dati. Nel complesso, le regole stabiliscono un cosiddetto «percorso di compliance» che le organizzazioni devono intraprendere per garantire il rispetto delle disposizioni. Il RGPD-UE rappresenta una grande e molteplice sfida per molte imprese, soprattutto per quelle dotate di grandi archivi di dati, con numerose connessioni con società terze incaricate della gestione dei dati e per quelle con architetture IT complesse. Il recepimento dei requisiti comporta numerose sfide e si articola spesso su molteplici livelli. I rischi normativi e operativi sono notevoli, specialmente per le aziende che svolgono attività basate sull'utilizzo commerciale di dati personali. Violazioni gravi sono già state sanzionate con multe di oltre 200 milioni di euro, mentre sanzioni dell'ordine di diversi milioni non rappresentano una rarità per aziende più grandi.

Le violazioni del regolamento sono punibili con una sanzione che può arrivare a 20 milioni di euro o al 4% del fatturato annuo (che potrebbe essere quello di gruppo), a seconda di quale dei due importi sia maggiore. Il RGPD-UE disciplina anche il trasferimento internazionale dei dati. Al trasferimento transnazionale dei dati si applicano regole restrittive, che devono essere analizzate. Le società sono responsabili di garantire che il trasferimento transnazionale dei dati avvenga in modo appropriato. Questo vale sia per i trasferimenti di dati personali esistenti, sia per quelli nuovi, in particolare nei cosiddetti «paesi terzi» (paesi al di fuori dell'UE e dello SEE).

I principi di protezione dei dati secondo RGPD-UE devono essere rispettati in qualsiasi momento. Nell'ambito del trattamento dei dati personali, principi come «la limitazione della conservazione», «la minimizzazione dei dati» o «la liceità, correttezza e trasparenza» fanno parte della protezione dei dati odierna. Sussiste inoltre un cosiddetto «principio di responsabilità», che obbliga le aziende ad essere in grado di comprovare la conformità ai principi RGPD-UE alle autorità competenti da una parte e agli stakeholder chiave dall'altra. Devono altresì essere rispettati in modo tempestivo i diritti delle persone interessate («data

subjects»). In particolare, il diritto alla cancellazione («diritto all'oblio») pone grandi sfide alle aziende e alle organizzazioni dotate di un'architettura IT molto complessa.

Poiché il RGPD-UE rappresenta un'importante innovazione nel diritto della protezione dei dati, anche dopo la conclusione del periodo di transizione di due anni e della relativa implementazione all'interno dell'impresa, sarà necessario porre particolare attenzione agli ulteriori sviluppi. Le attività delle autorità di vigilanza e la giurisprudenza del diritto in materia di protezione dei dati impongono infatti un monitoraggio costante e istituzionalizzato da parte dell'azienda.

Chi è interessato?

La portata del RGPD-UE trascende la precedente direttiva dell'UE sulla protezione dei dati. Qualsiasi organizzazione attiva in Europa che tratta dati personali è tenuta a rispettare le disposizioni del RGPD-UE. Questo vale anche per quelle che, pur non avendo alcuna succursale nell'UE, offrono beni e servizi a persone nell'UE oppure osservano il comportamento di persone che si trovano nell'UE. Per cui, ad esempio, un commerciante svizzero senza alcuna filiale nell'UE, ma che svolge iniziative di marketing rivolte ad acquirenti nell'UE, dovrà comunque attenersi alle prescrizioni del RGPD-UE. Lo stesso vale per le imprese che offrono i propri prodotti o servizi nello SEE o che ivi osservano il comportamento delle persone.

Come procedere?

Considerato che il RGPD-UE è già entrato in vigore, si può supporre che abbiate già implementato gran parte delle nuove disposizioni presso la vostra impresa.

Raccomandiamo pertanto le seguenti ulteriori misure:

- identificazione delle lacune tra il vostro attuale programma di protezione dei dati e le disposizioni del RGPD-UE, anche considerando gli enti che trattano dati su mandato per conto vostro;
- adeguamento e miglioramento delle strutture operative per garantire il rispetto delle disposizioni; ciò implica una dettagliata documentazione dei vostri processi di protezione dei dati e dei relativi controlli;
- verifiche e certificazioni sulla protezione dei dati per poter comprovare internamente ed esternamente la relativa compliance.

Il vostro esperto PwC sulla protezione dei dati sarà lieto di assistervi nel migliorare il vostro livello di protezione dei dati e garantire la vostra affidabilità.

1.2 Versione riveduta della Legge federale sulla protezione dei dati (LPD)

Il diritto della protezione dei dati svizzero viene rivisto, in particolare la LPD e l'Ordinanza sulla LPD (OLPD). La LPD viene modellata sul regolamento generale sulla protezione dei dati dell'UE, sebbene con alcune importanti deroghe.

Stato:
- entrata in vigore il 1º settembre 2023

Revisione della legge sulla protezione dei dati

Il 15 settembre 2017 il Consiglio federale ha pubblicato il disegno di legge per la revisione della Legge federale sulla protezione dei dati. La revisione della legge intende rafforzare la protezione dei dati personali e adeguare le disposizioni esistenti all'era digitale. Essa punta altresì ad armonizzare la legge svizzera in materia di protezione dei dati con la legislazione europea, vale a dire con il Regolamento generale sulla protezione dei dati dell'UE (RGPD-UE). A quasi tre anni dalla pubblicazione della prima bozza, dopo una serie di divergenze e una conferenza di conciliazione tra il Consiglio nazionale e il Consiglio degli Stati, il disegno di legge è stato approvato da ambedue i consigli il 25 settembre 2020.

Uno dei fattori che hanno caratterizzato la revisione della LPD durante i tre anni di consultazione è stato l'impegno a garantire l'accesso illimitato al mercato interno dell'UE. A causa delle pressioni esercitate dalla Commissione europea su questa questione, alcune sezioni della legislazione UE in materia di protezione dei dati sono infatti state deliberatamente recepite nel diritto svizzero. Questo per assicurare che la Svizzera continui a essere considerata dall'UE come Stato terzo con una protezione dei dati adeguata e possa quindi beneficiare del trasferimento transfrontaliero dei dati senza ulteriori misure legislative di protezione.

Punti chiavi del disegno di legge e differenze rispetto al RGPD-UE

Come il RGPD-UE, il disegno di legge svizzero mira fondamentalmente ad aumentare la trasparenza nel trattamento dei dati e a inasprire le conseguenze penali in caso di violazioni della protezione dei dati. In effetti, il disegno riprende in molti ambiti la terminologia giuridica dell'UE.

Viene inoltre perseguito un approccio basato sul rischio per cui, ad esempio, i doveri relativi alla protezione dei dati per i responsabili degli stessi aumentano in rapporto ai rischi per la sfera privata delle persone interessate. Come il RGPD-UE, anche la revLPD prevede, in linea di massima, che tutti i titolari e i responsabili del trattamento dei dati debbano documentare le proprie attività tramite un registro delle attività di trattamento. In linea con l'evoluzione in ambito UE, la revisione della legge federale sulla protezione dei dati (revLPD) rafforza altresì il ruolo e la posizione dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

Tuttavia, in alcuni ambiti, il disegno di legge si differenzia sostanzialmente dal diritto dell'UE: infatti, esso non prevede che i responsabili dei dati debbano documentare il rispetto della revLPD in conformità con il principio di «responsabilità». Contrariamente al RGPD-UE, non si giunge quindi per la protezione dei dati a un'inversione dell'onere della prova. Il disegno di legge non prevede inoltre alcuna disposizione specifica circa la protezione dei minori.

Ulteriori differenze rispetto al RGPD-UE emergono nell'ambito della perseguibilità penale. L'importo massimo delle sanzioni è di 250'000 franchi ed è quindi significativamente più basso che nell'UE. Inoltre, ai sensi della revLPD, saranno i collaboratori responsabili (persone fisiche) a essere perseguiti penalmente e non le entità responsabili (imprese) come nel caso del RGPD-UE.

Conseguenze della revisione e entrata in vigore

Poiché l'adozione della revLPD rappresenta un passo importante verso l'adeguamento della legge svizzera in materia di protezione dei dati auspicato dalla Commissione europea, il rischio di un'eventuale revoca dell'equivalenza del diritto svizzero in materia di protezione dei dati da parte dell'UE è per il momento relativamente ridotto. La Svizzera dovrebbe quindi continuare a essere riconosciuta dall'UE come equivalente per quanto concerne il diritto in materia di protezione dei dati. Questo è particolarmente importante per l'economia svizzera.

Come procedere?

Raccomandiamo alle imprese di occuparsi delle novità introdotte dalla revLPD, in particolare se non hanno ancora preso provvedimenti in relazione al RGPD-UE.

Le società che operano in Svizzera necessitano di acquisire una comprensione completa del modo in cui elaborano i dati personali. Al termine di questa analisi, adottando un approccio orientato al rischio, devono essere prese le misure necessarie per garantire il rispetto della nuova legislazione sul trattamento dei dati. Il vostro esperto PwC sulla protezione dei dati sarà lieto di assistervi in questo processo.

2 International Standards on Auditing (ISA)

2.1 ISA 600 (revised) «Considerazioni speciali – Revisione di bilanci di gruppo (incluso il lavori dei revisori delle controllate)»

Questo standard rafforza e aumenta le responsabilità del revisore responsabile dell'incarico del gruppo relativamente alla gestione e al raggiungimento della qualità della revisione nell'incarico e le responsabilità del revisore del gruppo per le attività di gestione e supervisione generale della revisione del gruppo e il riesame del lavoro dei revisori delle società controllate.

Stato:
- standard applicabile per le revisioni contabili dei conti annuali relativi agli esercizi che iniziano il 15 dicembre 2023 o successivamente

Le modifiche più significative apportate allo standard comprendono:

- la responsabilità del revisore del gruppo per la revisione contabile del gruppo, oltre a una modifica della definizione di team di revisione;
- il revisore del gruppo determina le componenti oggetto di revisione (a tal fine, si è eliminato come tipologia di lavoro il concetto di «componenti significative» e «revisione delle informazioni finanziarie della componente») e la natura, la tempistica e la misura in cui i revisori delle controllate devono essere coinvolti.