SWITZERLAND GLOBAL ENTERPRISE

Regolamento europeo sulla protezione dei dati – foglio informativo

Contesto generale

Il 25 maggio 2018 è entrato in vigore il regolamento europeo sulla protezione dei dati (GDPR). Sebbene sia un regolamento adottato dall'Unione europea, in determinate circostanze il GDPR è applicabile anche alle aziende svizzere.

Attualmente la legge svizzera sulla protezione dei dati (LPD) si trova anch'essa in fase di revisione per essere adeguata al diritto europeo. L'entrata in vigore della LPD svizzera non è prevista prima del 2019.

Il presente foglio informativo intende fornire una panoramica generale sull'applicabilità del GDPR alle aziende svizzere e sulla necessità di intervento. Il foglio informativo vuole essere un ausilio operativo senza alcuna pretesa di esaustività. È sempre necessaria un'analisi individuale dell'azienda interessata.

A chi si applica il GDPR dell'Unione europea?

Il GDPR dell'Unione europea riguarda **qualsiasi operazione relativa a dati personali** (ivi compresi raccolta, conservazione, cancellazione, anonimizzazione, trasferimento, ecc.; in breve "trattamento") effettuata da aziende svizzere se l'azienda

- **ha uno stabilimento nell'UE**, come ad es. una succursale, un'agenzia, un ufficio di rappresentanza locale o una società affiliata, purché questa non agisca autonomamente ma per conto della casa madre svizzera, e tratta dati personali in relazione a detto stabilimento (ad es.: uno stabilimento in Francia vende prodotti o servizi per lo stabilimento principale in Svizzera e per farlo utilizza nome e indirizzo dei clienti finali o delle persone di contatto dell'acquirente francese);
- **non ha uno stabilimento nell'UE**: se l'azienda offre beni o servizi nell'Unione europea (ad es.: un'azienda in Svizzera vende attivamente beni o servizi in Germania attraverso un sito web oppure un fornitore di software come servizio (SaaS) in Svizzera ha clienti nell'UE) o osserva il comportamento di cittadini dell'UE (ad es.: un sito web svizzero utilizza cookie che consentono di tracciare il comportamento dei visitatori del sito stesso e di analizzare i dati così ricavati).

Quali sono i principi di protezione dei dati sanciti dal GDPR dell'Unione europea?

I principi di protezione dei dati da osservare e rispettare per qualsiasi trattamento di dati sono i seguenti:

- **Principio di liceità:**
  I dati personali devono essere trattati solo in modo lecito e corretto (ossia in base alla legge, a un contratto, a un consenso o a un legittimo interesse).

- **Principio di limitazione della finalità:**
  I dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in un modo che non sia incompatibile con tali finalità.

- **Principio di trasparenza:**
  La raccolta di dati personali e in particolare la finalità del trattamento devono risultare trasparenti nei confronti dell'interessato. Il titolare del trattamento deve informare attivamente gli interessati di come vengono trattati i dati personali. A loro volta, gli interessati hanno diritto di accesso.

- **Principio di esattezza dei dati:**
  Chiunque tratti dati personali deve costantemente accertarsi che tali dati siano esatti e aggiornati.

- **Principio di minimizzazione dei dati e di limitazione della conservazione:**
  Il trattamento deve essere adeguato e limitato a quanto necessario rispetto alla sua finalità. La durata della conservazione deve essere definita in modo tale che i dati siano conservati solo per il tempo necessario al conseguimento della finalità del trattamento (attuazione di processi di archiviazione e cancellazione).

- **Integrità e riservatezza:**
  I dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati stessi (ivi compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali).

- **Responsabilizzazione:**
  Il titolare del trattamento è responsabile per il rispetto dei suddetti principi e deve essere in grado di comprovarlo.

Quali misure organizzative e operative occorre adottare?

Le aziende svizzere che sono soggette al GDPR dell'Unione europea pur non avendo uno stabilimento sul suo territorio devono nominare un rappresentante locale in ognuno dei Paesi interessati[1]. In determinate circostanze[2] è inoltre necessario designare un responsabile della protezione dei dati.
Le aziende per cui si applica il GDPR sono chiamate a soddisfare numerosi requisiti. Per prima cosa devono adottare linee guida, modelli e altra documentazione a garanzia del rispetto dei seguenti obblighi (elenco non esaustivo):

- organizzazione e documentazione di attività volte all'adempimento degli obblighi (ad es. organizzazione della protezione dei dati, predisposizione di regolamenti e direttive inerenti alla protezione dei dati, formazione dei collaboratori);
- le aziende che trattano dati personali sono responsabili del rispetto dei principi stabiliti dal regolamento (responsabilizzazione) e devono tenere un registro delle attività di trattamento[3];
- gli interessati devono essere informati di determinati punti prima di iniziare il trattamento dei loro dati (in particolare mediante un'informativa sulla protezione dei dati);
- il periodo di conservazione dei dati personali deve essere prestabilito e i dati sono cancellati una volta che sia stata conseguita la finalità del trattamento, che il periodo di conservazione sia scaduto e , in determinate circostanze e fatti salvi gli obblighi di conservazione, anche su richiesta dell'interessato;
- in caso di violazione dei dati, il titolare del trattamento deve notificare la violazione all'autorità di controllo competente, senza ingiustificato ritardo ed entro 72 ore dal momento in cui ne è venuto a conoscenza, laddove la violazione presenti un rischio per i diritti e le libertà degli interessati. Se tale rischio è elevato, occorre informare anche l'interessato stesso;
- prima di procedere a trattamenti rischiosi dei dati, è opportuno effettuare una valutazione d'impatto sulla protezione dei dati ;
- gli interessati hanno vari diritti in relazione ai propri dati personali (ad es. diritto di accesso o alla cancellazione), ai quali si deve di norma dare seguito entro il termine di un mese attuando i relativi processi interni;
- con i fornitori di servizi a cui si affida il trattamento dei dati personali in qualità di responsabili del trattamento è necessario concludere appositi contratti scritti;

[1] Le deroghe a questa disposizione sono elencate all'art. 27, par. 2 GDPR.

[2] Cfr. art. 37 GDPR.
[3] Sono previste deroghe a questa disposizione per le aziende con meno di 250 collaboratori (art. 30, par. 5 GDPR).

- prima di trasferire dati personali verso Paesi al di fuori dell'Unione europea/del SEE o della Svizzera, occorre accertarsi che il Paese interessato disponga di un adeguato livello di protezione. In caso contrario, devono essere adottate misure adeguate (ad es. conclusione di contratti per la protezione dei dati).

Quali sono le conseguenze di una mancata osservanza del regolamento?

Una violazione del GDPR comporta le seguenti conseguenze:

- in caso di violazione, le autorità europee possono infliggere all'azienda inadempiente sanzioni amministrative pecuniarie fino a 20 milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale annuo.
- i contratti prevedono spesso l'obbligo di rispettare la legge applicabile in generale o la legge sulla protezione dei dati in particolare. In questi casi, l'inadempimento può avere come conseguenza l'obbligo di pagare una penale contrattuale, la risoluzione del contratto, richieste di risarcimento danni e perdita di diritti.
- oggigiorno la notizia di una violazione può diffondersi molto rapidamente, soprattutto nel caso di aziende che sono molto rinomate, che gestiscono dati sensibili, che si sono già rese responsabili di inadempimenti di legge o che operano in ambiti esposti. Ne derivano quindi anche rischi per la reputazione.

Regolamento europeo sulla protezione dei dati – foglio informativo 2: Misure adottate da S-GE – Nuove disposizioni

Gestione dei dati indicati su biglietti da visita:

Gestire la consegna dei biglietti da visita:

- esibizione in portabiglietti (in occasione di fiere/eventi nell'UE)
- consegna direttamente all'azienda (in mano a una persona)

Informazioni per la gestione dei dati indicati su biglietti da visita:

I dati indicati su biglietti da visita sono dati personali che devono essere conformemente al principio di liceità. In particolare, il trattamento è lecito se basato su una norma di legge, su un consenso espresso o su una causa di giustificazione (quale ad es. il legittimo interesse del titolare del trattamento).

Non esiste per ora una prassi consolidata per quanto riguarda il trattamento dei dati personali indicati su biglietti da visita, per cui il trattamento dipende sempre dalle circostanze del singolo caso.

In linea di principio, tuttavia, nella maggior parte dei casi si può presumere che l'azienda destinataria dei biglietti da visita distribuiti in fiera possa far valere un legittimo interesse al trattamento dei dati e che il partecipante alla fiera si aspetti dalle aziende l'utilizzo del suo biglietto da visita e dei dati ivi indicati.

È quindi sufficiente rilasciare un'informativa al momento di ricevere il biglietto da visita, ad es. sul lead sheet, oppure al primo contatto con la persona in questione, senza che sia necessario un consenso esplicito. L'informativa può avere il seguente testo:

> *Con la presente la informiamo che [nome della società / del destinatario del biglietto da visita] conserverà nel proprio sistema i suoi dati personali comunicati con il biglietto da visita ricevuto. I dati sono limitati a nome, posizione, indirizzo e-mail e numero di telefono.*
>
> *I dati saranno oggetto di conservazione, così da poter rimanere in contatto con lei e tenerla aggiornata sulle ultime novità. La preghiamo di comunicarci se non desidera ricevere informazioni, inviti o newsletter da parte nostra.*
>
> *I suoi dati non saranno trasmessi a terzi.*

Per ogni più ampio trattamento, come la trasmissione dei dati a terzi, è necessario richiedere il consenso. Il consenso è valido solo se basato su informazioni complete e specifiche per il caso concreto. Consigliamo pertanto di verificare a fondo ogni singolo caso.

Un esempio di consenso per la trasmissione dei dati a terzi potrebbe essere il seguente. Il consenso deve essere esplicitamente espresso dal titolare del biglietto da visita, ad es. barrando una casella (sul lead sheet con relativa firma o al momento del primo contatto; in ogni caso prima della trasmissione a terzi):

☐ *Esprimo il mio consenso affinché [nome della società / del destinatario del biglietto da visita] possa trasmettere a terzi i miei dati personali (nome, posizione, indirizzo e-mail, indirizzo e numero di telefono) per finalità di marketing nelle aree [elencare].*

È suo diritto revocare in qualsiasi momento il suddetto consenso e richiedere la cancellazione dei suoi dati personali. Per farlo ci contatti all'indirizzo [indirizzo e-mail].

Quali domande deve porsi una PMI in Svizzera?

- **Una PMI svizzera deve designare un responsabile della protezione dei dati?**

  Ai sensi dell'art. 37 GDPR un responsabile della protezione dei dati deve essere designato se

  a) l'**attività principale dell'azienda** consiste in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico** degli interessati su larga scala; oppure
  b) l'**attività principale dell'azienda** consiste nel **trattamento, su larga scala, di categorie particolari di dati** (ossia dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) o di dati personali relativi a condanne penali e a reati.

  I criteri per valutare l'obbligo di designare un responsabile della protezione dei dati non sono chiari e impongono un'analisi dell'effettiva attività svolta dalla PMI e delle attività di trattamento dati connesse.

- **Quali altri obblighi deve ottemperare una PMI svizzera per non incorrere in sanzioni?**

  Non è possibile fornire una risposta univoca a questa domanda, poiché la portata delle misure di protezione dei dati dipende dal trattamento specifico a cui sono sottoposti i dati personali. È quindi necessario valutare il caso concreto per ogni singola azienda.

  Vale comunque la pena di fare le seguenti riflessioni in merito agli obblighi di protezione dei dati:

  o Rispettate i seguenti principi di protezione dei dati per ciascuna attività di trattamento:
    - ✓ Principio di liceità e correttezza
    - ✓ Principio di limitazione della finalità
    - ✓ Principio di trasparenza
    - ✓ Principio di esattezza dei dati
    - ✓ Principio di minimizzazione dei dati e di limitazione della conservazione
    - ✓ Principi di integrità e riservatezza
    - ✓ Principio di responsabilizzazione

- Garantite una buona governance
  - ✓ Dovete conoscere i vostri processi interni e mantenere ordine nel trattamento dei dati in modo da poter adempiere in qualsiasi momento i vostri obblighi di accesso e informazione
  - ✓ Lavorate a stretto contatto con il vostro reparto IT
  - ✓ Prevedete autorizzazioni e restrizioni di accesso
  - ✓ Formate i vostri collaboratori e predisponete direttive interne
  - ✓ Definite le responsabilità relative alla protezione dei dati

- Redigete un'informativa sulla protezione dei dati
- Verificate la necessità di designare un rappresentante nell'UE ai sensi dell'art. 27 GDPR
- Assicuratevi che in caso di violazione delle norme sulla protezione dei dati personali venga rispettato il termine di 72 ore per la notifica all'autorità di controllo
- Tenete un elenco delle attività di trattamento ai sensi dell'art. 30 GDPR
- Adottate le misure tecniche e organizzative necessarie per rispettare i principi di protezione dei dati ("privacy by design" / "privacy by default")
- Verificate se siete obbligati a designare un responsabile della protezione dei dati

Per ulteriori domande potete consultare l'indirizzo www.s-ge-com/it/exporthelp, scrivere direttamente all'indirizzo exporthelp@s-ge.com oppure chiamare il numero di telefono 0844 811 812.