Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GUIDA ALLO SWISS-US PRIVACY SHIELD

FONTE:

GUIDE TO THE EU-U.S. PRIVACY SHIELD
European Commission
Directorate-General for Justice and Consumers

Contenuto

Introduzione

Che cosa è lo Swiss-US Privacy Shield e perché ne abbiamo bisogno?

La Svizzera e gli Stati Uniti d'America (Stati Uniti) intrattengono solide relazioni commerciali. Il trasferimento di dati personali è una componente importante e irrinunciabile delle relazioni transatlantiche, in particolare nell'odierna economia mondiale digitalizzata. Molte transazioni implicano la raccolta e l'uso di dati personali quali nome, numero di telefono, data di nascita, domicilio, e-mail, numero di carta di credito, nome utente, sesso e stato civile o altre informazioni che consentano di identificare una persona. Si tratta di dati che possono essere raccolti in Svizzera da una succursale o da un partner commerciale di un'azienda statunitense e trattati negli Stati Uniti.

Ciò avviene quando si acquistano beni o servizi via Internet, si usano i social media o servizi di archiviazione su cloud, oppure quando un'azienda che ha sede in Svizzera si avvale di un'azienda con sede negli Stati Uniti (p.es. la società madre) per il trattamento dei dati personali dei propri collaboratori o clienti.

Secondo il diritto svizzero, i dati personali che vengono trasferiti negli Stati Uniti (p.es. alla società madre) devono beneficiare di un adeguato livello di protezione. Lo Swiss-US Privacy Shield è destinato a questo scopo: esso permette di trasferire dati personali dalla Svizzera a un'azienda negli Stati Uniti, a condizione che quest'ultima osservi una serie di norme e garanzie a tutela dei dati. La protezione si applica a tutte le persone domiciliate in Svizzera.

Come funziona lo Swiss-US Privacy Shield?

Al fine di garantire un livello di protezione adeguato per il trasferimento di dati personali dalla Svizzera agli Stati Uniti sono disponibili diversi strumenti, tra cui clausole contrattuali, norme vincolanti dell'azienda (le cosiddette «Binding Corporate Rules», BCR) ed il Privacy Shield. Per poterlo utilizzare, le imprese statunitensi devono prima di tutto registrarsi presso il Dipartimento del commercio degli Stati Uniti («Department of Commerce», DOC). Gli obblighi che si applicano alle aziende nell'ambito del Privacy Shield sono elencati nei principi applicabili alla protezione dei dati degli «Swiss-U.S. Privacy Shield Principles» (cfr. Swiss-US Privacy Shield Framework/ANNEX Principles and Arbitration). Il DOC è responsabile della gestione e dell'amministrazione del Privacy Shield, nonché di garantire che le aziende rispettino gli impegni presi. Per ottenere la certificazione, queste devono disporre di una politica sulla tutela dei dati personali in linea con i principi del Privacy Shield. Devono rinnovare il loro certificato, ovvero la loro «adesione» al Privacy Shield, ogni anno.

Per verificare se un'azienda statunitense è iscritta al Privacy Shield, occorre consultare l'elenco che figura sul sito Internet del DOC (https://www.privacyshield.gov/welcome). L'elenco riporta le informazioni relative a tutte le aziende certificate, al tipo di dati personali utilizzati e ai servizi offerti. Sul sito si ritrova anche un elenco di quelle che non aderiscono più al Privacy Shield, ovvero che non possono più ricevere dati personali nell'ambito del Privacy Shield. Queste ultime sono autorizzate a conservare i dati personali ottenuti durante il periodo di validità della certificazione soltanto dopo avere dichiarato al DOC che per quei dati continueranno a rispettare i principi in materia di protezione dei dati.

Obblighi delle aziende certificate per il Privacy Shield e diritti delle persone interessate

Le aziende sono tenute a trattare i dati personali nel rispetto dei principi della protezione dei dati del Privacy Shield.

1. Obbligo di informare

Un'impresa certificata deve informare le persone interessate su:

- i tipi di dati personali trattati;
- gli scopi del trattamento dei dati;
- l'eventuale intenzione di trasferire i dati personali a un'altra azienda e le ragioni del trasferimento;
- il diritto delle persone interessate di richiedere l'accesso ai propri dati personali;
- il diritto delle persone interessate di decidere se un'azienda può divulgare i loro dati personali a terzi o utilizzarli in modo «sostanzialmente diverso» da quello originalmente definito. In questo caso è sufficiente che l'azienda garantisca alla persona interessata un «diritto di opposizione» (diritto di «opt-out»). Nel caso di dati personali degni di particolare protezione (p.es. dati relativi all'origine etnica o allo stato di salute, cfr. art. 3 della legge sulla protezione dei dati, LPD), l'azienda deve richiedere il consenso esplicito della persona interessata (diritto di «opt-in»);
- il modo in cui le persone interessate possono contattare l'azienda per presentare un reclamo relativo all'uso dei loro dati personali;
- l'organo di mediazione svizzero o statunitense al quale presentare un reclamo;
- l'autorità governativa statunitense competente per indagare sugli obblighi dell'azienda nell'ambito del Privacy Shield e per garantirne il rispetto;
- la possibilità che l'azienda debba divulgare informazioni sul conto di persone interessate su legittima richiesta delle autorità statunitensi.

L'azienda che aderisce del Privacy Shield deve fornire un link verso le proprie disposizioni in materia di tutela dei dati personali nel caso in cui abbia un sito Internet oppure indicare dove reperire queste informazioni. Inoltre, è tenuta a fornire un link verso l'elenco gestito dal DOC in modo che le persone interessate possano verificare la validità della certificazione.

2. Destinazione vincolata

Di regola un'azienda certificata per il Privacy Shield può utilizzare i dati personali soltanto per gli scopi originariamente definiti o per uno scopo successivamente autorizzato. Se si intende usare i dati per uno scopo diverso, occorre valutare in che misura differisca da quello originale:

• l'uso di dati personali per uno scopo incompatibile con quello originale non è mai ammesso;

• se il nuovo scopo è «sostanzialmente diverso», ma attinente a quello originario, l'azienda può utilizzare i dati soltanto se non vi è opposizione («opt-out») oppure, in caso di datidegni di particolare protezione, se vi è un consenso esplicito («opt-in»);

• se il nuovo scopo non è sostanzialmente diverso da quello originario, il corrispondente uso è ammesso.

Se per esempio un datore di lavoro trasferisce dati personali negli Stati Uniti per trattarli, la filiale statunitense può utilizzarli per offrire ai collaboratori una polizza assicurativa o un piano pensionistico, a condizione che essi non si oppongano a tale uso. Per contro, la stessa non può vendere i dati per scopi commerciali a terzi che intendano offrire beni o servizi non attinenti direttamente al rapporto d'impiego.

Le persone interessate hanno altresì il diritto di decidere se un'azienda certificata per il Privacy Shield possa trasmettere i loro dati a un'altra azienda negli Stati Uniti o in un Paese terzo. Se l'azienda trasmette dati per trattamento a un'azienda mandataria, entrambe sono tenute a concludere un contratto scritto che contenga le stesse garanzie in materia di protezione dei dati di quelle previste nel Privacy Shield. L'azienda certificata può essere ritenuta responsabile delle azioni di quella mandataria se questa non rispetta le pertinenti disposizioni.

3. Proporzionalità

L'azienda certificata può trattare soltanto i dati personali che sono rilevanti a un determinato fine. Deve inoltre garantire che i dati utilizzati siano esatti, completi e aggiornati. I dati personali possono essere inoltre conservati soltanto per il tempo necessario ai fini del trattamento. Possono essere conservati più a lungo soltanto se servono a scopi specifici, per esempio archiviazione, letteratura, arte, giornalismo, ricerca scientifica o storica, oppure per analisi statistiche. Anche in questo caso i principi in materia di protezione dei dati vanno rispettati.

4. Sicurezza dei dati

L'azienda è tenuta a garantire che i dati personali siano conservati in un ambiente sicuro e protetti contro perdita, uso abusivo, accesso non autorizzato, divulgazione illecita, alterazione o distruzione, tenendo conto in modo adeguato della natura dei dati e dei rischi connessi al loro trattamento.

5. Trasferimento di dati a terzi

Come già accennato al punto 2, l'azienda certificata può trasferire dati personali a un'altra azienda a talune condizioni e tenendo conto dello scopo per il quale li ha originariamente ricevuti. Indipendentemente dalla sua sede, all'interno o all'esterno dal territorio degli Stati Uniti, l'azienda che riceve i dati deve garantire lo stesso livello di protezione dei dati personali di quello previsto dal Privacy Shield. Ciò implica che tra le due entità venga stipulato un contratto nel quale si stabiliscono le condizioni alle quali il trattamento dei dati personali è consentito. In particolare l'azienda mandataria deve essere tenuta a informare l'azienda certificata in merito a eventuali situazioni in cui non possa più adempiere ai propri obblighi; essa deve allora sospendere il trattamento dei dati. Regole più severe si applicano nel caso di terzi che agiscono in quanto mandatari di un'azienda certificata. Quest'ultima può essere ritenuta responsabile delle azioni compiute dal mandatario in violazione dei suoi obblighi in materia di tutela dei dati personali.

6. Diritto di informazione e di rettifica

Ogni persona interessata ha il diritto di chiedere all'azienda certificata di essere informata sui propri dati.

Può chiedere informazioni sugli scopi per i quali i dati sono trattati, sulle categorie di dati personali trattati e sui destinatari (o categorie di destinatari) ai quali i dati vengono trasferiti. Può anche richiedere di rettificarli o cancellarli se sono inesatti o non più attuali, oppure se sono stati trattati in violazione delle disposizioni del Privacy Shield.

Non si è tenuti a specificare il motivo per cui si vuole essere informati in merito ai propri dati; tuttavia è possibile che l'azienda lo richieda nel caso in cui la domanda appaia troppo ampia o generica. L'azienda è tenuta a rispondere alla richiesta entro un lasso di tempo ragionevole. Può limitare il diritto di informazione soltanto in casi determinati, per esempio quando ciò potrebbe compromettere la riservatezza, violare il segreto professionale o essere in conflitto con altri obblighi legali.

7. Diritto di reclamo e rimedi giuridici

Se l'azienda non si attiene alle disposizioni del Privacy Shield e viola i propri obblighi di protezione dei dati personali, le persone interessate possono presentare un reclamo e richiedere il gratuito patrocinio. Le aziende certificate sono tenute a prevedere una procedura di ricorso indipendente. Possono optare per l'organo di mediazione delle controversie statunitense (Alternative Dispute Resolution body, ADR), o scegliere di sottoporsi alla vigilanza dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

Le persone interessate possono presentare il reclamo presso:

1. l'azienda statunitense certificata per il Privacy Shield;

2. un organo di ricorso indipendente, ad esempio un organo di mediazione delle controversie statunitense (ADR) o l'IFPDT svizzero;

3. il DOC, attraverso l'IFPDT;

4. la Commissione federale del commercio («Federal Trade Commission», FTC) statunitense (oppure il Dipartimento dei trasporti statunitense, «Department of Transportation», se il reclamo è presentato nei confronti di una compagnia aerea o una biglietteria);

5. il collegio arbitrale competente per il Privacy Shield , una volta esaurite tutte le altre opzioni.

• Organo di mediazione delle controversie (ADR)

Un organo di mediazione delle controversie è un'organizzazione privata che si occupa tra l'altro dei reclami presentati nei confronti delle aziende. Se si opta per la mediazione delle controversie, l'azienda certificata per il Privacy Shield può scegliere se sottoporsi alla procedura di mediazione in Svizzera o negli Stati Uniti. La procedura è definita dall'organo che è stato scelto.

• IFPDT

L'Incaricato federale della protezione dei dati e della trasparenza è l'organo di consulenza e di vigilanza competente a livello nazionale per le questioni in materia di protezione dei dati.

• Dipartimento del commercio («Department of Commerce», DOC) e Commissione federale del commercio («Federal Trade Commission», FTC) statunitensi

I ricorsi destinati al DOC e/o alla FTC vanno presentati all'IFPDT.

• Collegio arbitrale del Privacy Shield

Il collegio arbitrale, composto di tre arbitri indipendenti, consente di comporre eventuali controversie senza la necessità di ricorrere in giudizio. Le sue decisioni sono vincolanti ed esecutive presso i tribunali statunitensi. La persona interessata può valersi dell'arbitrato presso il collegio arbitrale a talune condizioni (in particolare, tutti gli altri rimedi giuridici devono essere stati esauriti). Le aziende certificate non hanno invece questo diritto, in quanto il procedimento arbitrale è previsto soltanto per le persone interessate.

8. Protezione giuridica in caso di accesso ai dati da parte di autorità statunitensi

La protezione dei dati personali può essere pregiudicata anche in caso di accesso agli stessi da parte di autorità statunitensi. Il Privacy Shield garantisce che ciò avvenga unicamente nella misura necessaria per raggiungere uno scopo di interesse pubblico preponderante, per esempio per motivi di sicurezza nazionale o legati all'esecuzione delle pene. Sebbene la legislazione statunitense preveda già meccanismi di salvaguardia e rimedi giuridici nell'ambito del perseguimento penale, il Privacy Shield offre per la prima volta uno strumento speciale, ossia l'organo di mediazione, che si occupa della questione dell'accesso ai dati motivato dalla sicurezza nazionale (cfr. sezione C).

In che modo si può presentare un reclamo nei confronti di un'azienda certificata per il Privacy Shield?

Il Privacy Shield prevede una serie di modalità per la presentazione di un reclamo, per esempio nel caso in cui l'azienda non tratti in modo corretto i dati personali o non operi nel rispetto di altre disposizioni.

Il meccanismo di ricorso può essere scelto liberamente in base alle esigenze individuali.

Il reclamo può essere presentato presso:

1. L'azienda statunitense certificata per il Privacy Shield. Un'azienda deve sempre fornire informazioni dettagliate su come procedere in caso di reclamo. Essa è inoltre tenuta a rispondere entro 45 giorni dal ricevimento del reclamo. La risposta deve indicare se il reclamo è fondato e il modo in cui si intende porre rimedio al problema. L'azienda è tenuta a esaminare ogni reclamo che non sia manifestamente infondato.

2. L'organo di mediazione delle controversie (ADR), nel caso in cui l'azienda certificata abbia scelto questo tipo di composizione delle controversie. Il sito Internet deve indicare l'organo di mediazione delle controversie e il link al suo sito Internet, che deve contenere informazioni dettagliate sui servizi offerti e sulla procedura da seguire. L'organo deve essere in grado di imporre misure correttive e sanzioni efficaci per garantire che l'azienda certificata rispetti l'obbligo di proteggere i dati personali. La procedura arbitrale è gratuita per le persone interessate.

3. L'IFPDT. Un'azienda certificata per il Privacy Shield può scegliere l'IFPDT come organismo di ricorso indipendente. Siccome nel caso del trattamento di dati concernenti i dipendenti il controllo da parte dell'IFPDT è obbligatorio, questi possono sempre rivolgersi all'IFPDT per i reclami relativi a dati concernenti il rapporto d'impiego trasferiti a un'azienda certificata. Questo vale anche nel caso in cui l'azienda abbia deciso di non collaborare con l'IFPDT. Quest'ultimo trasmette il reclamo all'autorità statunitense competente.

L'IFPDT trasmette la sua raccomandazione all'azienda il più rapidamente possibile e comunque entro 60 giorni dalla data in cui riceve il reclamo. La persona che ha presentato il reclamo è informata della raccomandazione, che di norma è resa pubblica. L'azienda ha in seguito 25 giorni di tempo per conformarsi alla raccomandazione dell'IFPDT. Qualora non lo faccia, l'IFPDT può sottoporre la questione alla Commissione federale del commercio (FTC) statunitense affinché prenda provvedimenti esecutivi. Può però anche informare il Dipartimento del commercio (DOC) statunitense e richiedere la sua cancellazione dall'elenco delle aziende certificate per il Privacy Shield qualora continui a essere inadempiente.

Inoltre, se il reclamo dimostra che i dati personali sono stati trasferiti all'azienda certificata in violazione del diritto svizzero in materia di protezione dei dati, l'IFPDT può procedere anche nei confronti dell'azienda in Svizzera e disporre la sospensione del trasferimento.

4. Il Dipartimento del commercio (DOC). Anche se non ha poteri di controllo diretti sulle aziende statunitensi certificate nei confronti delle quali è stato presentato un reclamo, l'IFPDT può sottoporre il reclamo al Dipartimento del commercio statunitense (DOC). Il DOC provvede a verificare il reclamo e a inviare una risposta all'IFPDT entro 90 giorni. Può parimenti trasmettere i reclami alla Commissione federale del commercio (o al Dipartimento dei trasporti).

5. La Commissione federale del commercio (FTC). Vi è anche la possibilità di presentare reclamo direttamente alla Commissione federale del commercio statunitense utilizzando lo stesso sistema a disposizione dei cittadini statunitensi: www.ftc.gov/complaint.

6. Il collegio arbitrale del Privacy Shield. Qualora il reclamo sia ancora interamente o parzialmente irrisolto dopo aver seguito le altre procedure di ricorso, o l'autore dello stesso non sia soddisfatto del modo in cui è stato gestito, si può ricorrere all'arbitrato vincolante.

Chi può domandare un arbitrato vincolante e sotto quali condizioni?

Questa procedura può essere avviata personalmente soltanto da una persona interessata ed è vincolante per l'impresa certificata.

È possibile scegliere questa opzione soltanto dopo che tutte le altre modalità di ricorso non siano giunte a buon fine. Inoltre questa opzione è preclusa se il reclamo è già stato oggetto in precedenza di un procedimento arbitrale, se un giudice si è già espresso in merito e le parti in causa nella procedura erano le stesse, se le parti sono già giunte a un accordo o se l'IFPDT è in grado di risolvere il reclamo direttamente con l'azienda. La Commissione federale del commercio può effettuare indagini parallele.

Modalità per avviare la procedura arbitrale

Prima di avviare la procedura arbitrale, occorre anzitutto notificare formalmente all'azienda interessata la propria intenzione. La notifica deve includere una descrizione della presunta violazione delle prescrizioni del Privacy Shield e una sintesi delle misure già adottate. Si possono allegare anche una documentazione di supporto o i relativi documenti giuridici.

Luogo dell'arbitrato

Il procedimento arbitrale si svolge negli Stati Uniti poiché la sede dell'azienda certificata per il Privacy Shield è in questo Paese.

Vantaggi della procedura arbitrale

- il diritto di chiedere il supporto dell'IFPDT nella preparazione del reclamo;

- la possibilità di partecipare al procedimento telefonicamente o in videoconferenza, senza alcun obbligo di essere fisicamente presenti negli Stati Uniti;

- la possibilità di usufruire gratuitamente dei servizi di interpretariato e di far tradurre la documentazione dall'inglese in una lingua ufficiale svizzera;

- la presa a carico dei costi del procedimento arbitrale (fatta eccezione per gli onorari degli avvocati) da parte di un fondo appositamente costituito dal Dipartimento del commercio e finanziato con i contributi annui delle aziende certificate.

Durata della procedura arbitrale

La procedura arbitrale si conclude entro 90 giorni dal giorno in cui l'azienda interessata è stata informata dell'avvio della procedura.

Rimedi giuridici nell'ambito della procedura arbitrale

Il collegio arbitrale può concedere all'autore del reclamo diritti quali l'accesso, la rettifica, la cancellazione o la restituzione dei propri dati. Anche se il collegio arbitrale non può concedere un risarcimento, gli autori del reclamo hanno tuttavia la possibilità di far valere i loro diritti dinanzi al giudice conformemente alla legge statunitense in materia di arbitrato (Federal Arbitration Act), qualora l'esito del procedimento non sia soddisfacente.

L'organo di mediazione: punto di contatto per i reclami del trattamento di dati da parte di autorità statunitensi

Il Privacy Shield prevede un nuovo meccanismo di ricorso indipendente nell'ambito della sicurezza nazionale: l'organo di mediazione.

Si tratta di un funzionario di alto livello (mediatore per il Privacy Shield) del Dipartimento di Stato statunitense che opera in modo indipendente dalle agenzie federali di intelligence. Insieme ai suoi collaboratori garantisce che i reclami siano trattati in modo adeguato e tempestivo. Gli autori del reclamo ricevono conferma del fatto che le norme di diritto statunitense pertinenti sono state rispettate oppure, in caso siano state violate, che sono state applicate misure correttive.

Per esaminare i reclami, l'organo di mediazione collabora strettamente con altri organi di controllo indipendenti dotati di poteri d'inchiesta, al fine di disporre di tutte le informazioni necessarie per stabilire la conformità delle misure di vigilanza con il diritto statunitense. Gli organi con i quali collabora sono responsabili della vigilanza sulle diverse agenzie di intelligence statunitensi.

Competenze

L'organo di mediazione si occupa di tutti i reclami in relazione a dati personali e di tutti i tipi di trasferimenti commerciali dalla Svizzera a aziende negli Stati Uniti, anche se l'azienda statunitense che trasmette i dati non aderisce al Privacy Shield e i dati sono trasferiti attraverso strumenti di trasferimento alternativi, quali clausole contrattuali standard e norme aziendali vincolanti.

Procedura di presentazione di un reclamo

La domanda va inoltrata all'IFPDT per iscritto. Deve contenere una motivazione, nonché il tipo di risposta desiderata o di assistenza auspicata. Deve contenere inoltre informazioni relative agli organi governativi statunitensi che potrebbero essere coinvolti nelle attività di vigilanza e a ogni altra misura eventualmente già intrapresa e ogni risposta eventualmente già ricevuta. La domanda non deve tuttavia dimostrare che le agenzie di intelligence statunitensi abbiano effettivamente avuto accesso ai dati personali.

Prima della trasmissione all'organo di mediazione l'IFPDT esamina se la domanda poggia su una richiesta legittima. In particolare verifica:

- l'identità dell'autore del reclamo, al fine di determinare se agisce esclusivamente per conto proprio e non in rappresentanza di un governo o di un'organizzazione intergovernativa;
- la completezza delle informazioni contenute,
- che si tratti di dati personali trasferiti negli Stati Uniti;
- che la domanda non sia vessatoria o abusiva.

Svolgimento della procedura:

L'organo di mediazione provvede a trattare la domanda e contatta l'IFPDT qualora abbia altre domande o gli occorrano altre informazioni.

Una volta completa, la domanda è trasmessa all'organo statunitense competente. Se la domanda riguarda la compatibilità della vigilanza con le norme del diritto statunitense, l'organo di mediazione può collaborare con uno degli organi di controllo indipendenti dotati di poteri d'inchiesta. Per poter rispondere ai reclami, deve disporre di tutte le informazioni necessarie; confermerà poi che la domanda è stata esaminata adeguatamente e che le norme del diritto statunitense sono state rispettate, oppure, in caso di violazione, che sono stati adottati provvedimenti correttivi. La risposta non indica se la persona che ha presentato il reclamo è stata oggetto di attività di sorveglianza da parte dei servizi di intelligence degli Stati Uniti.

Principio di trasparenza

Conformemente alla legge statunitense sulla libertà di informazione («Freedom of Information Act», FOIA) chiunque può richiedere di accedere a documenti in possesso del Governo degli Stati Uniti. Informazioni su come procedere per inoltrare la domanda sono disponibili sui siti ufficiali di ciascun ministero. Ulteriori informazioni sono disponibili agli indirizzi www.FOIA.gov e http://www.justice.gov/oip/foia-resources.

Non è tuttavia possibile accedere a informazioni classificate nell'ambito della sicurezza nazionale, a informazioni personali di terzi e a informazioni relative a indagini giudiziarie. Queste limitazioni si applicano sia ai cittadini statunitensi e che a quelli stranieri.

In caso di controversie riguardanti l'accesso a documenti richiesto nell'ambito della legge sulla libertà di informazione è possibile inoltrare dapprima un ricorso amministrativo e poi un ricorso dinanzi a un tribunale federale. Il giudice stabilisce se l'accesso ai documenti sia stato negato legittimamente; in caso contrario, può imporre al governo di concedere l'accesso ai documenti. Il giudice può disporre il rimborso delle spese legali; un risarcimento non è tuttavia possibile