Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GUIDE TO THE SWISS-US PRIVACY SHIELD

SOURCE:

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

Content

Introduction

What is the SWISS-US Privacy Shield and why do we need it?

Switzerland and the United States (USA) have strong commercial ties. Transfers of personal data are an important and necessary part of the transatlantic relationship, especially in today's global digitalized economy. Many transactions involve the collection and use of personal data such as your name, phone number, date of birth, home and email addresses, credit card number, login name, gender and marital status, or any other kind of information that makes it possible to identify you. Personal data may be collected in Switzerland by the branch or business partner of an American company and then used in the USA.

This is the case when you buy goods or services online, when you use social media or cloud storage services as a private individual, or if you are an employee of a Swiss-based company and send data on people to a company in the USA (e.g. the parent company) for processing. Swiss law requires that when personal data is transferred to the USA, it continues to benefit from an adequate level of protection.

This is where the SWISS-US Privacy Shield comes in: thanks to this new legal framework, your personal data can be transferred from Switzerland to a company in the United States, provided that the US company complies with a set of data protection rules and safeguards. This protection that is given to personal data applies to everyone who is resident in Switzerland.

How does the Privacy Shield work?

When personal data are transferred from Switzerland to the USA, various tools are available to ensure an adequate level of data protection, such as contractual clauses, binding corporate rules and the Privacy Shield. In order to use the Privacy Shield, US companies must first register with the US Department of Commerce (DOC). The companies' obligations under the Privacy Shield are contained in the "Swiss-US Privacy Shield Principles" (cf. Swiss-US Privacy Shield Framework/ANNEX Principles and Arbitration). The DOC is responsible for managing and administering the Privacy Shield and ensuring that companies meet their obligations. Companies that wish to be certified must have a privacy policy in line with the Privacy Principles. They must renew their certificate, i.e. their "membership" of the Privacy Shield, on an annual basis. If they do not, they can no longer receive and use personal data from Swiss companies under that framework.

If you want to know whether a company in the USA is a member of the Privacy Shield, you can check the Privacy Shield List on the Department of Commerce website (https://www.privacyshield.gov/welcome). This list gives you details of all the companies certified for the Privacy Shield, the kind of personal data they use, and the kind of services they offer. You can also find a list of companies that are no longer part of the Privacy Shield and which are no longer allowed to receive personal data under the Privacy Shield. This means they are no longer allowed to receive your personal data under the Privacy Shield. Also, these companies may only keep your personal data if they commit to the Department of Commerce that they will continue to apply the Privacy Principles.

Privacy Shield companies' obligations and rights of persons whose personal data is used

Companies wishing to process personal data are obliged to comply with the Privacy Principles.

1. The right to be informed

A Privacy Shield company must provide you with information on the following:

- the types of personal data it processes;
- the reasons why it is processing your personal data;
- any plans it has to transfer your personal data to another company and the reasons why;
- your right to ask the company for access to your personal data;
- your right to choose whether you allow a company to disclose your personal data to another company or to use your personal data in a 'materially different' way. It is sufficient if the company gives you the right to refuse (to 'opt-out'). When the data is sensitive, (i.e. data that reveals, for example, your ethnic origin or the state of your health, see Article 3 of the Data Protection Act (FADP)), the Privacy Shield company must obtain your express consent (also known as your right to 'opt-in');
- how to contact the company if you have a complaint about the use of you personal data;
- the alternative dispute resolution (ADR) body, either in Switzerland or the USA, where you can bring your case;
- the government agency in the USA that is responsible for investigating and enforcing the company's obligations under the Privacy Shield framework;
- that there may be justification for disclosing information about you, when the US authorities make a lawful request.

The Privacy Shield company must provide you with a link to its privacy policy if it has a public website, or otherwise tell you where you can access its privacy policy. It must also provide you with a link to the Privacy Shield list on the DOC website so that you can check the company's Privacy Shield status.

2. Limiting the use of your data to a specific purpose

In principle, a Privacy Shield company can only use your personal data for the purpose for which it was originally collected or which you have subsequently authorised. If it wants to use your data for a different purpose, the question of whether this is permitted depends on how much the new purpose diverges from the original purpose:

• Using your data for a purpose that is incompatible with the original purpose is never allowed;

• If the new purpose is 'materially different' from, but still related to the original purpose, the Privacy Shield company may only use your data if you do not object (if youdo not 'opt out') or, in the case of sensitive data, if you give your express consent (if you 'opt-in').

• If the new purpose is not materially different from the original one, such use is permissible.

For example, if your employer has sent your personal data to the USA, the US company could use the data to offer you an insurance policy or pension scheme, as long as you do not object to this. On the other hand, it is not permitted to sell your data to a third party for commercial purposes that have no connection with your job.

You also have a right to choose whether you allow a Privacy Shield company to pass on your personal data to another company, whether in the USA or another country outside Switzerland. While you do not have such a choice when your data will be sent to another company (also known as an "agent") for processing on behalf, in the name and under the instructions of the Privacy Shield company, the Privacy Shield company will have to sign a contract with the agent that obliges the latter to provide the same data protection safeguards as contained in the Privacy Shield framework. And the Privacy Shield company can be held liable for its agent's actions if the agent does not respect the rules.

3. Obligation to act proportionately

The Privacy Shield company may only process personal data that is relevant for the purpose of processing. It must also ensure that the data used are accurate, reliable, complete and up to date. It is only allowed to keep personal data for as long as is necessary for the purpose of the processing. It may keep data for longer periods only if it needs them for certain specified purposes, such as archiving in the public interest, journalism, literature, art, scientific or historical research, or for statistical analysis. In such cases, the company must also comply with the Privacy Principles.

4. Data security

The company must ensure that your personal data is kept in a safe environment and secured against loss, misuse, unauthorised access, disclosure, alteration or destruction, taking due account of the nature of the data and the risks involved in the processing.

5. Transfer of data to a third party

As noted above under point 2, subject to certain conditions and taking account of the purpose for which it received your personal data, the Privacy Shield company may transfer it to another company. Irrespective of its location, within or outside the USA, the company that receives your data must give it the same level of protection as guaranteed under the Privacy Shield framework. This requires a contract between the two companies setting out the conditions under which the third party can use your personal data. In particular, the contract must require the third party to inform the Privacy Shield company if it can no longer continue to meet its obligations, in which case it must stop using the data. Stricter rules apply where a third party is acting as an agent on behalf of a Privacy Shield company. Here, the Privacy Shield company can be held liable for any actions of an agent that violate its obligations to protect your personal data.

6. Your right to access and correct your data

You have the right to ask the Privacy Shield company to give you access to your personal data. This means that you have a right to have your data communicated to you but also to get information about the purpose for which the data are pro¬cessed, the categories of personal data concerned and the recipients to whom the data are disclosed.

You are not obliged to give any reasons why you want information; however, the company is entitled to ask you to do so if your request is too broad or vague. The company has to respond to your request within a reasonable time. It may only limit your rights to have access in specific situations, e.g. if providing information would breach confidentiality or professional privilege or conflict with legal obligations..

7. Your right to file a complaint and obtain a remedy

If the company does not follow the rules of the Privacy Shield and violates its obligation to protect your personal data, you have the right to complain and obtain a remedy, free of any cost. Privacy Shield companies are obliged to provide an independent recourse mechanism. They can choose alternative dispute resolution (ADR) or submit to the oversight of the Federal Data Protection and Information Commissioner (FDPIC).

You can file a complaint with:

1. the USA Privacy Shield company itself;

2. an independent recourse mechanism, such as an ADR body or the FDPIC;

3. the US Department of Commerce, but only via the FDPIC;

4. the US Federal Trade Commission (or the USA Department of Transportation if complaint relates to an airline or ticket agent); or

5. an arbitration panel for Privacy Shield matters, but only if other remedies have failed

• Alternative Dispute Resolution body (ADR)

An Alternative Dispute Resolution (ADR) body is a private organization that deals with complaints filed against companies, including complaints related to data protection matters. When opting for ADR, the Privacy Shield company has to choose whether it submits to ADR in Switzerland or in the United States. The procedure by which the ADR handles your complaint depends on the specific body that has been selected.

• FDPIC

The Federal Data Protection and Information Commissioner is responsible at national level as the advisory and supervisory authority for data protection matters.

• U.S. Department of Commerce (DOC) and U.S. Federal Trade Commission (FTC)

Complaints to the DOC and/or the FTC must be filed with the FDPIC, which forwards them to the USA.

• Arbitration panel for Privacy Shield matters

The arbitration panel is made up of three neutral arbitrators, and offers an opportunity to settle disputes without going to court. Its decisions are binding and enforceable in the US courts. Subject to certain conditions, you can request arbitration before the competent arbitration panel (in particular, all other legal remedies must have been exhausted). Privacy Shield companies may not submit their complaints to arbitration, because the procedure is solely intended for natural persons.

8. Remedies in the event of US authorities accessing data

The privacy of your personal data may also be affected by US authorities accessing your data. The Privacy Shield ensures that this occurs only to the extent necessary to pursue an objective of significant public interest, such as national security or law enforcement. While existing USA law provides you with safeguards and remedies in relation to law enforcement matters, the Privacy Shield framework for the first time creates a special instrument to address issues related to data access on the grounds of national security, the ombudsperson mechanism (see part C).

How can I make a complaint against a Privacy Shield company?

The Privacy Shield offers you a number of ways to complain about a company, for example if you think that it is not using your personal data correctly or that it is not complying with the rules in any other way.

You are free to choose the remedy that is best suited to your complaint. Your complaint can be made to:

1. The US Privacy Shield company, directly: A company must always provide you with detailed information on how to make a complaint. The company must respond to you within 45 days of receiving your complaint. The response must state whether your complaint has merit and, if so, the remedy the company will provide. The company is obliged to look into each complaint it receives unless it is clearly groundless.

2. The Alternative Dispute Resolution body(ADR): If the Privacy Shield company has chosen the ADR body as its independent recourse mechanism. The company's website must provide you with information about ADR and a link to the website of the ADR body, including details of the services it offers and the procedures. The body must be able to impose effective remedies and sanctions to ensure that the Privacy Shield company complies with its obligation to protect your personal data. You can use this procedure free of any charge

3. The FDPIC: A Privacy Shield company can choose the FDPIC to act as its independent recourse machanism. As FDPIC oversight is mandatory for any company that handles human resources (personnel) data, as an employee you can always go to the FDPIC if you have any complaints with regard to employment-related data that has been sent to a Privacy Shield company. This is the case even if the company concerned has not opted to work with the FDPIC. The FDPIC will refer your complaint to the competent US authority.

The FDPIC will deliver advice to the company as quickly as possible, at the latest within 60 days of receiving the complaint. You will be informed about his advice, which is normally also made public. A company then has 25 days to comply with the FDPIC's advice; if it fails to do so, the FDPIC may refer the case to the US Federal Trade Commission for enforcement action. It may also notify the DOC of the company's refusal to comply, which may lead to the company's removal from the Privacy Shield List if the company persists in its non-compliance.

In addition, if your complaint reveals that the transfer of your personal data to the Privacy Shield company is a violation of Switzerland data protection law, the FDPIC can also act against Swiss company that sends the data, and prevent the data transfer.

4. The Department of Commerce (DOC). Although the FDPIC has no direct powers of oversight in relation to the US Privacy Shield company that is the object of your complaint, it can still refer your complaint to the US DOC. The DOC will review your complaint and respond to the FDPIC within 90 days. The DOC may also forward your complaint to the Federal Trade Commission (or the Department of Transportation).

5. The Federal Trade Commission (FTC). You can also make your complaint directly to the US Federal Trade Commission under the same complaint system used by US citizens: www.ftc.gov/complaint. The Federal Trade Commission will also review complaints it receives from the US Department of Commerce, EU DPAs and ADR bodies. Similarly to the Department of Commerce, the Federal Trade Commission has set up a dedicated point of contact to liaise directly with EU DPAs to facilitate referrals and increase cooperation to handle individual complaints

6. The arbitration panel for Privacy Shield matters: If your complaint is still wholly or partially unresolved after using all the foregoing procedures, or if you are not satisfied with the way your complaint has been handled, the final legal remedy available to you is the binding arbitration procedure.

Who is allowed to bring arbitration proceedings? Under which conditions?

You are the only person entitled to bring arbitration proceedings against a Privacy Shield company, and the panel's decision is binding on the company.

However, you may only apply to the arbitration panel after you have exhausted all other avenues of redress without success. Arbitration is not possible if your complaint has already been considered in arbitration proceedings, if a court has already ruled on the same complaint involving the same parties, if the parties have already reached a settlement, or if the FDPIC has resolved your complaint directly with the company. In addition, the FTC can also conduct investigations in parallel with the arbitration proceedings.

How do I apply for arbitration?

Before you initiate the arbitration process, you must formally notify the company of your intention to do so. Your notice must include a description of the alleged violation of the Privacy Shield provisions and a summary of the steps you have already taken to resolve your complaint. You may also provide supporting documents or legal texts relating to your complaint.

Where will the arbitration take place?

Arbitration takes place in the USA because all certified Privacy Shield companies are based there.

What are the benefits?

- You have the right to ask for the FDPIC's assistance to prepare your claim;
- You can take part in the proceedings by telephone link or video-conference, so there is no requirement to be physically present in the USA;
- You are entitled, free of charge, to interpretation services and to translations of documents from English into another language;
- The costs of arbitration (with the exception of lawyer's fees) are paid from a fund specially set up by the Department of Commerce and financed from the Privacy Shield companies' annual contributions

How long does the arbitration process take?

The arbitration process must be completed within 90 days of the day on which you gave notice to the company.

What remedies can arbitration provide?

The arbitration panel can grant you the right to access, correct or delete your personal data or to have your data returned to you. Although the panel cannot award you monetary damages, you can file a claim in court under the US Federal Arbitration Act if you are not satisfied with the outcome of arbitration.

The Ombudsperson Mechanism: how to bring a complaint against a US public authority

The Privacy Shield has set up a new independent redress mechanism on matters of national security: the Privacy Shield Ombudsperson.

The Ombudsperson is a senior official within the US Department of State who is independent from US intelligence agencies. Assisted by a number of staff, the Ombudsperson ensures that complaints are properly investigated and dealt with promptly. You will receive confirmation that the relevant US laws have been complied with, or, if the laws have been violated, that the situation has been remedied.

When dealing with your complaint, and in order to obtain all the information it needs on the legality of any surveillance measures, the Ombudsperson works closely with the independent oversight and investigation bodies that are responsible for overseeing the various US intelligence agencies.

The Ombudsperson's jurisdiction

The Ombudsperson deals with complaints relating to transfers of personal and commercial data from Switzerland to companies in the USA, including data transferred by US companies that are not Privacy Shield members and data transferred on the basis of alternative transfer tools such as standard contractual clauses or binding corporate rules.

How do I bring a complaint to the Ombudsperson?

Your written request must be submitted to the FDPIC. It should explain the grounds for your complaint and outline the type of answer or support you are looking for. It should also name the US government agencies that you think have been involved in the surveillance activities and provide details of the measures that you have already taken to pursue your request and any answer you may have received. However, your request need not provide any proof that your data have in fact been accessed by US intelligence agencies.

Before being submitted to the Ombudsperson, your request will be checked to confirm that it relates to a legitimate concern. The following points will be verified:

- your identity, to ensure that you are acting only for yourself and not on behalf of a government or intergovernmental organization;
- that your request contains all the relevant information,
- that it relates to personal data transferred to the USA,
- that your request is not frivolous, vexatious or made in bad faith.

What happens once my request is sent to the Ombudsperson?

The Ombudsperson will process your request and, if it has any questions or requires more information, it will contact the referring body.

Once the Ombudsperson has determined that your request is complete, it will pass it on to the appropriate US body. If the request relates to the legality of surveillance under US law, the Ombudsperson will be able to work with an independent oversight body that has investigatory powers. The information obtained will enable the Ombudsperson to respond to the complaint. It will confirm in its response that your request has been properly investigated and either that US law has been complied with or that any violation of US law has been remedied. The response will not confirm whether you have been the target of surveillance by USA national intelligence services.

Freedom of information

You can request access to records held by the US government under the Freedom of Information Act (FOIA). The official website of each US government department provides information on how you can make a request for access to documents. You can find more information on how to make such a request on www.FOIA.gov and http://www.justice.gov/oip/foia-resources.

However, no access is permitted to classified national security information, personal information relating to third parties, or information concerning law enforcement investigations. These restrictions apply irrespective of whether you are a US citizen or not.

In the event of any dispute about a FOIA request, you can file an appeal with the relevant administrative authority and thereafter with a federal court in the USA. The court can then decide whether the records you requested have been properly withheld, or it can order the government to grant you access to the documents. The courts can award legal costs but monetary damages are not available.